



Preside Multiservice Data Manager

# Fault Management

User Guide

241-6001-011



---

Preside Multiservice Data Manager

# **Fault Management**

## User Guide

---

Publication: 241-6001-011

Document status: Standard

Document version: 14.3RSUP

Document date: December 2003

---

Copyright © 2003 Nortel Networks.

All Rights Reserved.

Printed in Canada

NORTEL, NORTEL NETWORKS, the globemark design, the NORTEL NETWORKS corporate logo, PRESIDE, DPN, and PASSPORT, are trademarks of Nortel Networks. SUN and SUNLINK are trademarks of Sun Microsystems Inc. SPARCSTATION is a trademark of Sparc International Inc. UNIX is a trademark licensed exclusively through X/OpenCompany Ltd.

---



## Publication history

---

### December 2003

14.3RSUP Standard  
Commercial availability



---

# Contents

---

## **About this document** **21**

Who should read this document and why 21

What you need to know 21

How this document is organized 22

What's new in this document 23

Text conventions 24

Year representation 25

26

Related documents 26

---

## **Chapter 1**

### **Surveillance overview** **27**

Fault management 27

    Accessing fault management tools 29

Surveillance architecture 30

Functional overview 32

    Network Viewer 33

    Alarm Display 34

    Alarm Help 35

    Network Status Bar 35

    Component Information Viewer 36

    Component Status Display 37

    Command Console 38

Context 38

Start Tool 39

Common surveillance tasks 40

---

---

Finding troubled components	41
Monitoring a selected set of components	43
Responding to troubled or out-of-service states	44
Determining a problem	45
Putting a component into maintenance state	46
Putting a component in acknowledged state	47
Clearing an alarm	48
Acknowledging/Unacknowledging an alarm	48
Fixing a problem	49
Changing the Network Viewer display	49

---

## **Chapter 2**

### **Network Viewer**

51

Network Viewer overview	51
Network Viewer capabilities	51
Network Viewer modes	52
Using the Network Viewer tool	53
Starting Network Viewer	53
Using the Network Viewer Icon Bar	54
Interacting with other tools	56
Context	56
Start Tool menus	56
Exiting the Network Viewer	59
Understanding the network display	61
Displaying the Network Viewer legend	62
Displaying nodes	63
Node types in the Network Viewer and the network model	64
Displaying the node labels	66
Positioning the nodes	67
Displaying links	69
Displaying nodes and links owned by a site or region	71
Displaying shelf views	72
Displaying subcomponents in a textual list	74
Displaying component states	78
Navigating the network display	81

---

Using the Component Finder	81
Using organization navigation	85
Using background navigation	91
Using double-clicking actions	92
Controlling the network display	93
Using the NV Filter Settings Dialog	93
Using the Preferences dialog	97
Using Views of the network	99
Customizing the Network Viewer display	100
Selecting the background pixmap image	100
Changing node icon pixmap images	101
Selecting the default view	102
Modifying the Start Tool menus and icon bars	102
Customizing Network Viewer resources	103
Customizing color and display attributes	112
Troubleshooting	113

---

## **Chapter 3**

### **Passport Shelf View**

**117**

Overview	117
MDM state color conventions	118
Passport Shelf View window	119
Menu bar	121
State Summary	121
Logical Processor Summary pane	123
Processor Card Summary pane	124
Supplementary component pane	125
Physical Shelf	126
Card faceplates	128
Supplementary component bar	128
Component Information	129
Component Navigator pane	131
Related component pane	131
Component details pane	132
Application status bar	133

- Procedures 134
  - Starting Passport Shelf View from the MDM toolset 136
  - Starting Passport Shelf View from the UNIX command line 138
  - Starting Passport Shelf View from other MDM tools 140
  - Quitting Passport Shelf View 142
  - Displaying Passport Shelf View online help 143
  - Moving tabbed pages onto the desktop 144
  - Displaying tool tips 145
  - Opening pop-up menus 146
  - Adjusting the image size of the Physical Shelf 147
  - Adjusting pane sizes 148
  - Adjusting column widths 149
  - Navigating the Passport component tree structure 150
  - Setting the maintenance state for a component 152
  - Locking a logical port 153
  - Unlocking a logical port 154
  - Displaying related components 155
  - Sorting related components 156
  - Setting filters for related components 157
  - Setting an automatic refresh interval for related components 158
  - Displaying component attributes 159
  - Displaying alarms 160
  - Sorting alarms 161
  - Setting an automatic refresh interval for alarms 162
  - Acknowledging an alarm 163
  - Acknowledging all active alarms on a component 164
  - Unacknowledging an alarm 165
  - Unacknowledging all active alarms on a component 166
  - Clearing local alarms 167
  - Clearing global alarms 168
  - Making provisioning changes to components and services 169
  - Starting other MDM tools from Passport Shelf View 170
  - Errors and warnings 172
    - Non-Passport Context 172
    - Unknown Passport 172

---

- Cannot connect to psvagent 173
- Cannot Connect To Server 173
- Cannot Connect To mnsdagent 173
- Invalid or Missing Definition File 174

---

## **Chapter 4**

### **VPN Monitor**

**175**

- Overview 175
- Service views 176
- VPN Monitor architecture 177
- RFC 2764 178
  - RFC 2764 basic services 178
  - RFC 2764 service clusters 183
  - RFC 2764 provider edge network service views 184
- RFC 2547 187
  - RFC 2547 basic services 187
  - RFC 2547 service clusters 189
  - RFC 2547 provider edge network service views 191
- Direct virtual router to virtual router 193
  - Direct VR-VR basic services 193
  - Direct VR-VR service clusters 196
  - Direct VR-VR VPN views 197
- VPN state color conventions 198
  - Basic service states 199
  - Service cluster states 199
  - Core networks and view states 200
- VPN Monitor window 201
  - Menu bar 202
  - Tool bar 203
  - Navigation pane 203
  - Status pane 205
  - Recent event pane 205
- VPN Monitor dialogs 205
  - Find 205
  - Component 206

- 
- Procedures 207
  - Starting VPN Monitor from the MDM toolset 208
  - Starting VPN Monitor from the command line 209
  - Quitting VPN Monitor 210
  - Displaying VPN Monitor online help 211
  - Opening pop-up menus 212
  - Adjusting pane sizes 213
  - Displaying or hiding the tool bar 214
    - Procedure steps 214
  - Navigating the VPN 215
  - Displaying service view components 216
  - Displaying basic service components 217
  - Finding basic services or service clusters in the provider edge network 218
  - Starting other MDM tools from VPN Monitor 219

---

## **Chapter 5**

### **Alarm Display**

**221**

- Alarm Display overview 222
- Alarm Display formats 222
- Common alarm format 222
  - Syntax styles 223
- Alias substitution for component names 225
- Viewing alarms in the Active mode 226
  - Viewing alarms in the Active Alarm mode 226
- Clearing active alarms for DPN 229
- Clearing active alarms for Passport 230
  - Clearing a Passport alarm using Local Clear 231
  - Clearing a Passport alarm using Global Clear 232
  - Clearing a Passport alarm using the Global Clear tool 233
- Viewing alarms in the Log mode 236
  - Viewing alarms in Log mode 236
  - Acknowledging and Unacknowledging Alarms 238
  - Setting the Auto-Refresh interval 241
  - Sorting by time and by component id 241
- Displaying Customer Database Information 242

- 
- Setting customer database preferences 242
  - Keyboard shortcuts 244
  - Filtering alarms 245
    - Defining filters 245
    - Applying filters 251
    - Saving filters 253
  - Setting alarms by effects 254
    - Setting alarm effects for visual and audible monitoring 254
  - Starting another tool 256
  - Customizing Alarm Display Start Tool submenus 256
    - Passing component information from Alarm Display to Component Information Viewer 258
  - Saving and viewing Alarm Display files 259
    - Saving Alarm Display information to a file 260
    - Viewing an Alarm Display log file in active mode 260
    - Viewing an Alarm Display log file in log mode 261
  - Customizing resources 262
  - Command line arguments 264
- 

## **Chapter 6**

### **Alarm Help**

**267**

- About Alarm Help 267
- Alarm help window 268
- Starting Alarm Help 269
- Stopping Alarm Help 269
- Searching for an alarm code 270
- Searching for a text string 270
- Viewing alarm codes from Alarm Display or Component Information Viewer 271
- Adding and editing alarm codes 271
  - Adding a description for a new alarm code 271
  - Adding a description using an existing alarm code 272
  - Editing an alarm code description 273
  - Deleting an alarm code description 273

---

<b>Chapter 7</b>	
<b>Alarm acknowledgement and unacknowledgement</b>	<b>275</b>
Alarm Acknowledgement and Unacknowledgement overview	275
Acknowledging and unacknowledging single or multiple alarms	276
Changing state by acknowledging all active alarms on a component	277
Displaying Alarm Acknowledgment and Unacknowledgement information	277
Acknowledge Alarm(s) Dialog	278
Unacknowledge Alarm(s) Dialog	279
Alarm acknowledgement/unacknowledgement procedures	281
Starting Alarm Acknowledgment	281
Acknowledging selected active alarms	282
Acknowledging active alarms for selected components	282
Acknowledging active alarms on selected components	283
Unacknowledging selected active alarms	284
Unacknowledging active alarms on selected components	284
Customizing the Alarm Acknowledgment Dialog	286
Resource Files	286

---

<b>Chapter 8</b>	
<b>Network Status Bar</b>	<b>289</b>
Network Status Bar overview	289
Network Status Bar main window	290
Menu bar	291
Component information	291
Alarm information	292
Command buttons	293
Keyboard shortcuts	294
NSB Dialogs	294
Troubled Components Dialog	294
Error Dialogs	296
Warning Dialogs	296
NSB procedures	296

---

- 
- Starting the Network Status Bar 296
  - Acknowledging the current indicator values 297
  - Using the Troubled Components Dialog 297
  - Customizing the Network Status Bar 299
    - Customizing the Troubled Components pop-up menu 299
    - Customizing resources in the Network Status Bar 299
- 

## **Chapter 9**

### **Component Information Viewer**

**301**

- Component Information Viewer overview 301
- Component Information Viewer data 302
  - Management data 302
  - Diagnostic information 302
- Component Information Viewer window 303
  - Menu bar 306
  - Message area 307
  - Related components panel 307
  - Sash 310
  - Information panel 310
  - Preference boxes 318
  - Refresh button 318
- Customizing the Component Information Viewer display 318
  - Alarm list 319
  - Related components list menu 320
  - Information for field pop-up menu 320
  - Component Information Viewer Diagnostic Command menu 321
  - Other resources 321
- Diagnostic commands 325
  - Select Command Route 326
  - Command Console 326
  - Query Historical Alarms 326
  - Help 326
  - Passport Commands 326
  - Passport Tests 328
  - Passport Inventory 330

DPN Commands	331
DPN Inventory	333
NRS Commands	334
Passport Port Test Console	335
Procedures	342
Starting Component Information Viewer without context	344
Starting Component Information Viewer with context	345
Exiting Component Information Viewer	346
Displaying Component Information Viewer online help	347
Setting component filters	348
Setting Preferences	350
Using previously saved preference settings	354
Setting a target in the related components panel	355
Setting the acknowledge state for a component	356
Setting the maintenance state for a component	357
Starting other MDM tools from Component Information Viewer	358
Setting a target in the information panel	359
Displaying additional component information	360
Clearing active alarms for DPN	361
Clearing a Passport alarm using Local Clear	362
Clearing a Passport alarm using Global Clear	363
Clearing a Passport alarm using the Global Clear tool	365
Clearing active alarms for Passport	368
Acknowledging active alarms	369
Unacknowledging active alarms	370
Displaying diagnostic information	371
Selecting a new command route	373
Querying historical alarms from Component Information Viewer	375
Errors and warnings	381
Service Selection Warning Dialog	381
Save Settings Error Dialog	381
Restore Settings Error Dialog	381
Manual Alarm Clearing Error Dialog	382

---

**Chapter 10****Query Historical Alarms****383**

Overview 383

Query Historical Alarms dialog 384

Procedures 386

Querying historical alarms tool from the Preside MDM tool set  
window 387

Querying historical alarms from the command line interface 392

---

**Chapter 11****Component Status Display****397**

Component Status Display overview 397

Component status 399

Raw state values 399

Propagated state values 399

Component Status Display main window 401

Menu Bar 402

Message area 404

Components Panel 404

Control panel 409

Keyboard shortcuts 409

Component Status Display dialogs 409

Component Filter Settings Dialog 410

Preference Settings Dialog 411

Exit CSD Dialog 414

Warning and error dialogs 415

Component Status Display procedures 417

Starting the Component Status Display 418

Refreshing the Components Panel 418

Choosing a new organization 419

Putting a component into Acknowledged state 420

Putting a component into Maintenance state 420

Changing the Component Filter Settings 421

Exiting the Component Status Display 422

Setting Component Status Display preferences 423

- 
- Setting the sort key for the components list 423
  - Customizing the Component Status Display 425
    - Customizing the Components List Start Tool menu 425
    - Customizing other resources 425
- 

## **Chapter 12**

### **IP Discovery**

**429**

- Starting IP Discovery 431
- Setting a password for IP Discovery 432
- Starting IP Discovery with password protection 433
- Changing a password for IP Discovery 434
- Disabling password protection for IP Discovery 435
- Discovering devices using direct discovery 436
- Discovering devices using route-based discovery 437
  - Procedure steps 437
- Deleting devices 438
- Updating devices 440
- Finding devices 441
- Adding an address 442
- Creating a network setting 443
- Changing network settings 444
- Deleting network settings 445
- Moving rows in network settings 446
- IP Device Discovery window 447
  - Devices 450
  - Network Settings 452
- Discovery window 456
  - Route-based discovery 459
  - Direct discovery 459
  - Why a discovery may fail 460
- Logging 461
  - Changing the IP Discovery log location 461
- Error messages 462
- Warning messages 465

---

## Chapter 13

### Circuit Viewer

467

- Circuit Viewer overview 467
- Circuit Viewer server configuration 469
- Circuit management log files 469
- Circuit Viewer window 470
- Menu bar 472
  - File menu 472
  - Edit menu 472
  - Options menu 472
  - Tools menu 473
  - Help menu 474
- Circuit retrieval criteria panel 474
- Circuit(s) found panel 477
- Circuit details panel 478
  - Circuit state 478
  - Circuit information 478
  - Customer information 480
  - Circuit components 481
  - Connection states 485
- Sashes 487
- Online help 487
- Procedures 488
  - Starting the Circuit Viewer tool without component context 490
  - Starting the Circuit Viewer tool with component context 491
  - Displaying Circuit Viewer online help 492
  - Setting the server configuration options 493
  - Setting log file information levels 494
  - Setting authentication information 495
  - Retrieving a list of circuits from the Administration Database 496
  - Using the Component Selection Dialog 498
  - Sorting a list in the Circuit(s) found panel 499
  - Displaying circuit component information 500
  - Displaying provisioned or operational attributes of a component 502

---

Displaying a connection trace	505
Setting the polling configuration options	506
Starting state polling	508
Stopping state polling	509
Viewing circuit component statistics	510
Putting a component or circuit into context	513
Getting a component or circuit from context	514
Starting a service provisioning tool without context	515
Starting a service provisioning tool with context	516
Starting the MDM Database Administration tool from Circuit Viewer	517

---

<b>Chapter 14</b>	
<b>HP OpenView NNM desktop</b>	<b>519</b>
HP OpenView NNM overview	519
Root map	520
How HP OpenView NNM desktop displays device names	520
Procedures	523
Starting HP OpenView NNM from the MDM toolset	524
Starting HP OpenView NNM from the UNIX command line	525
Quitting HP OpenView NNM	526
Displaying online documentation	527
Displaying alarm help	528
Starting MDM Passport tools from the menu bar	529
Starting MDM Passport tools from the node pop-up menu	532
Starting MDM DPN tools from the menu bar	533
Starting MDM DPN tools from the node pop-up menu	535

---

<b>Appendix A</b>	
<b>LPDA-2 modem management</b>	<b>537</b>

---

<b>Appendix B</b>	
<b>Common alarm format</b>	<b>541</b>

---

<b>Index</b>	<b>543</b>
--------------	------------

---

## About this document

---

The following topics are discussed in this section:

- “Who should read this document and why” (page 21)
- “What you need to know” (page 21)
- “How this document is organized” (page 22)
- “What’s new in this document” (page 23)
- “Text conventions” (page 24)
- “Year representation” (page 25)
- “Related documents” (page 26)

### Who should read this document and why

This document is for system administrators and network operators who are responsible for network management. This document describes how to use the Preside Multiservice Data Manager (MDM) Fault Management toolset.

### What you need to know

This document assumes an understanding of network management. Also, you need to be familiar with

- the Sun workstation
- the UNIX operating system
- a UNIX text editor, for example, vi
- elements in your network, for example, DPN and Passport devices

To access the MDM Fault Management tools, you need to have a valid capability ID and a password.

## How this document is organized

- “Surveillance overview” (page 27) gives an overview of Preside Multiservice Data Manager (MDM) fault management tools.
- “Network Viewer” (page 51) describes the Network Viewer tool for monitoring a network and provides procedures for using this tool.
- “Passport Shelf View” (page 117) describes the Passport Surveillance Shelf View tool for displaying the physical and logical views of Passport multiservice devices and for performing a subset of surveillance and provisioning tasks.
- “VPN Monitor” (page 175) describes the VPN Monitor tool for managing faults in Passport IP VPN networks.
- “Alarm Display” (page 221) describes the Alarm Display tool for monitoring network alarms and provides procedures for using this tool.
- “Alarm Help” (page 267) describes the Alarm Help utility for viewing alarm code descriptions
- “Alarm acknowledgement and unacknowledgement” (page 275) describes the Acknowledge Alarm and Unacknowledge Alarms tools for informing other operators that you are currently investigating an Active alarm problem. This section also provides procedures for using these tools.
- “Network Status Bar” (page 289) describes the Network Status Bar tool for displaying a high-level view of the current network status and provides procedures for using this tool.
- “Component Information Viewer” (page 301) provides an overview and window description of the Component Information Viewer tool and procedures for using this tool.
- “Query Historical Alarms” (page 383) describes the short-term historical alarm search tool for displaying short-term historical alarms and provides procedures for using this tool.

- “Component Status Display” (page 397) describes the Component Status Display tool for displaying information about the network status in textual (rather than graphical) format and provides procedures for using this tool.
- “IP Discovery” (page 429) describes the Internet Protocol (IP) Discovery tool for discovering Simple Network Management Protocol (SNMP) devices and provides procedures for using this tool.
- “Circuit Viewer” (page 467) provides an overview and description of the Circuit Viewer tool and procedures for using the Circuit Viewer tool.
- “HP OpenView NNM desktop” (page 519) describes the HP OpenView Network Node Manager (NNM) tool for accessing the HP OpenView platform and starting MDM fault management tools. This section also provides procedures for using this tool.
- “LPDA-2 modem management” (page 537) appendix describes how to use LPDA-2 macros and how to update the LPDA-2 macro configuration file.
- “Common alarm format” (page 541) details the command alarm format parameters.

## What’s new in this document

The following features were added to this document:

- “Shelf View Enhancements” (page 23)
- “IP Discovery Enhancements” (page 23)
- “Support for IP VPN Access” (page 24)
- “VPN Monitor” (page 24)

### Shelf View Enhancements

Enhancements to Shelf View include new sparing relationship indicators; the ability to set maintenance state; and the ability to lock and unlock ports.

### IP Discovery Enhancements

This feature provides the ability to locate a device directly using a device name or IP address when using the IP Discovery graphical user interface.

## Support for IP VPN Access

The Circuit Viewer tool is enhanced to support the search and display of IP VPN Access Circuits.

## VPN Monitor

The VPN Monitor chapter was added to provide conceptual and procedural information for monitoring Passport IP Virtual Private Network services. VPN Monitor supports Passport VPNs based on FRC 2764, RFC 2547 and direct virtual router to virtual router configurations. “VPN Monitor” (page 175).

## Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`

Nonproportional spaced plain type represents system generated text or text that appears on your screen.

- **nonproportional spaced bold type**

Nonproportional spaced bold type represents words that you should type or that you should select on the screen.

- *italics*

Statements that appear in italics in a procedure explain the results of a particular step and appear immediately following the step.

Words that appear in italics in text are for naming.

- `[optional_parameter]`

Words in square brackets represent optional parameters. The command can be entered with or without the words in the square brackets.

- `<general_term>`

Words in angle brackets represent variables which are to be replaced with specific values.

- UPPERCASE, lowercase

In MDM, uppercase and lowercase letters that appear in UNIX commands and parameters must be matched exactly. The system matches upper and lowercase characters differently.

- ->

A right-pointing arrow in a procedure indicates that a menu item has submenus from which you must choose. The appropriate submenu selection is shown immediately after the arrow.

- |

This symbol separates items from which you may select one; for example, ON|OFF indicates that you may specify ON or OFF. If you do not make a choice, a default ON is assumed.

- ...

Three dots in a command indicate that the parameter may be repeated more than once in succession.

The term absolute pathname refers to the full specification of a path starting from the root directory. Absolute pathnames always begin with the slash (/) symbol. A relative pathname takes the current directory as its starting point, and starts with any alphanumeric character (other than /).

## Year representation

There are occurrences in this document where years are expressed as two digits rather than four, for example, 97 rather than 1997. To avoid ambiguity with the use of two-digit years, the following convention is used in this document. Years 91 to 99 (inclusive) represent the twentieth century, for example, 97 represents 1997; years 00 to 90 (inclusive) represent the twenty-first century, for example, 01 represents 2001.

## Related documents

See the following documents for related information:

- 241-1001-303 *DPN-100 Operator Commands and Responses*
- 241-2001-351 *DPN-100 Network Control System Operations and Maintenance*
- 241-5701-060 *Passport 7400, 15000, 20000 Components*
- 241-6001-012 *Preside MDM Configuration Management for DPN User Guide*
- 241-6001-015 *Preside MDM Network Model Administrator Guide*
- 241-6001-023 *Preside MDM Configuration Management for Passport User Guide*
- 241-6001-203 *Preside MDM Alarm and Status API Reference Guide*
- 241-6001-301 *Preside MDM Customization Administrator Guide*
- 241-6001-303 *Preside MDM Administrator Guide*
- 241-6001-804 *Preside MDM Workstation Utilities User Guide*
- 241-5701-050 *Passport 7400, 15000, 20000 Commands*
- 241-5701-060 *Passport 7400, 15000, 20000 Components*

# Chapter 1

## Surveillance overview

---

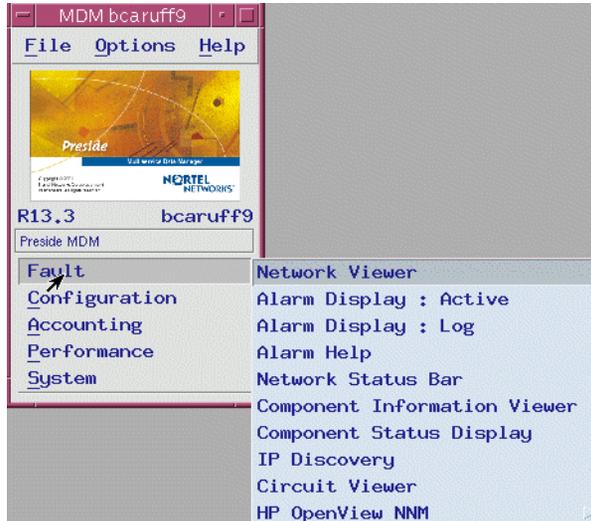
This section describes the Preside Multiservice Data Manager (MDM) tools for fault management and provides instructions on how to use these tools. You can view the following topics in this section:

- “Fault management” (page 27)
- “Surveillance architecture” (page 30)
- “Functional overview” (page 32)
- “Context” (page 38)
- “Start Tool” (page 39)
- “Common surveillance tasks” (page 40)

### Fault management

The Preside MDM tools for managing faults are available from the Fault toolset in the Preside MDM window. The figure “Preside MDM fault management tools” (page 28) shows the Preside MDM window and the available fault management toolset. Depending on the setup at your organization, the toolsets may differ from that shown in the figure.

### Preside MDM fault management tools



The following list provides a brief description of the fault management tools:

- **Network Viewer**  
Network Viewer provides a graphical view of network elements and monitors states for first-alert surveillance.
- **Alarm Display (Active and Log)**  
Alarm Display alerts to fault conditions in network components, indicating the severity of the fault, the type of fault, and additional information on the cause or current situation. The Alarm Display supports two startup options: Active Alarms or Logs.
- **Alarm Help**  
Alarm Help provides alarm code descriptions for DPN, Passport, integrated SNMP device, and MDM proxy alarms.
- **Network Status Bar**  
Network Status Bar provides a high-level view of the state of the network. As well, it monitors network health by means of global statistics.

- **Component Information Viewer**  
Component Information Viewer performs diagnostic analysis of components identified by the first-alert surveillance tools.
- **Component Status Display**  
Component Status Display performs first-alert surveillance on the network, indicating the current state or criticality of the network model components.
- **IP Discovery**  
The IP Discovery application lets you discover Simple Network Management Protocol (SNMP) devices by hostname or IP address using direct discovery or route-based discovery. Direct discovery accepts a list of devices and attempts to discover each device as an SNMP-managed device. Route-based discovery accepts seed devices, filters parameters and discovers devices listed in its routing table
- **Circuit Viewer**  
Circuit Viewer provides the ability to view on-switch and off-switch circuit information stored in the Administration Database. Circuit Viewer also provides service diagnostic information. This information includes the states of circuits, circuit components, and connection components as well as statistics for connection, interface or port components across a circuit. This tool is one component of the MDM circuit management application. For more information about circuit management, see 241-6001-011 *Preside MDM Fault Management User Guide*.
- **HP OpenView NNM**  
HP OpenView NNM is an optional tool that provides access to the HP OpenView platform.

## Accessing fault management tools

- 1 In the Nortel Networks Preside MDM window, select Fault and then point to the tool name that you want to use. For example, to start the Network Viewer tool, select Fault -> Network Viewer.

The selected fault management tool opens.

## Surveillance architecture

Preside Multiservice Data Manager (MDM) supports both state-based and alarm-based surveillance. State-based surveillance is used by the Network Viewer and Component Status Display tools. Alarm-based surveillance is used by the Alarm Display tool. For an overview of MDM surveillance, see the figure “Surveillance architecture” (page 32).

By using the monitoring tools that correspond with your preferred surveillance models, you can receive information about network element faults, their impact (through the Network Viewer and Component Status Display tools), and their cause (through the Alarm Display). High-level monitoring of the network is also available through the Network Status Bar. Diagnostic tools such as the Component Information Viewer, the DPN Performance Viewer, and the Data Viewer (for Passport and Simple Network Management Protocol (SNMP) devices) provide more information about the fault, its impact, its cause, and its history. After the fault is properly identified, you can perform the following actions:

- Mask the fault using the network model’s acknowledge and maintenance states.
- Clear the alarm through Alarm Display or Component Information Viewer. You can also issue commands to the element through the Command Console utility or one of the remote access tools. For details about the Command Console and Remote Access utilities, see the Command Console section in 241-6001-804 *Preside MDM Workstation Utilities User Guide*
- Correct some configuration parameters using the configuration tools.
- Acknowledge the alarm through the Alarm Display or the Component Information Viewer to indicate to other network operators that the fault causing the alarm is currently being investigated.

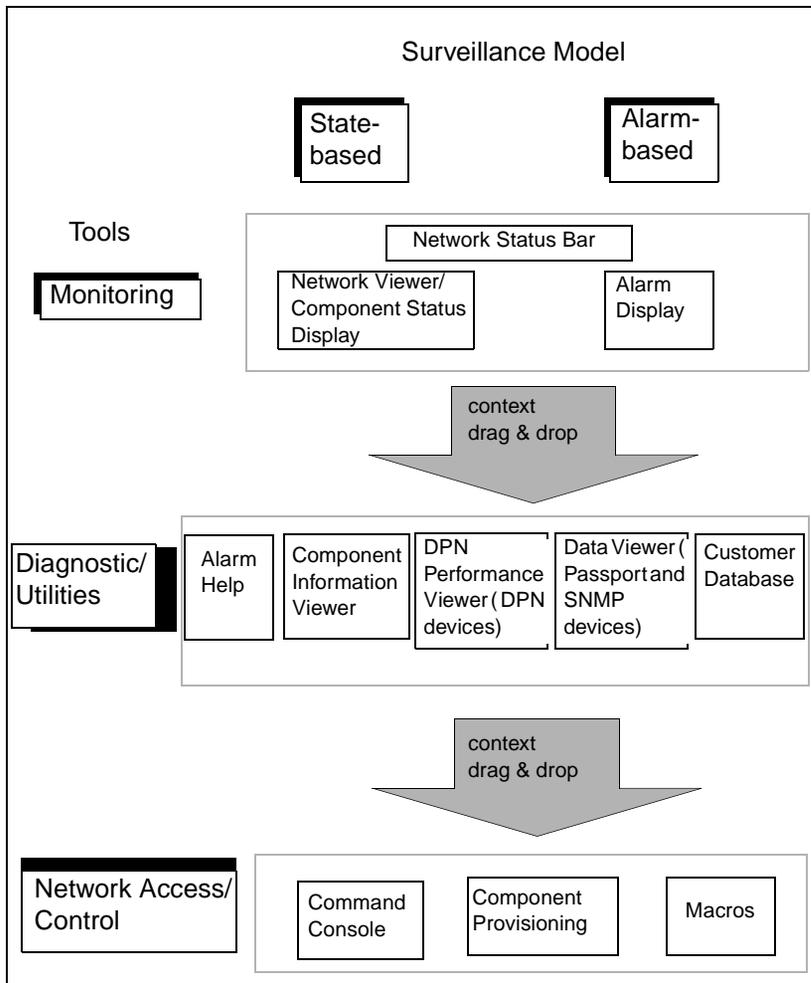
Acknowledging all active alarms against a component causes the component state to become acknowledged. The component state is then masked as though it was directly acknowledged with a state-based surveillance application such as Network Viewer.

Communication between these tools is simplified through cut and paste, and automatic context transfers.

Surveillance draws its information from the network model. For a description on how the network model works and the interactions among the surveillance tools, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

When used with the SNMP Surveillance Adapter, MDM can also manage other devices on the network. For information on how this works, see 241-6001-118 *Preside MDM SNMP Surveillance Adapter Guide*.

**Figure 1**  
**Surveillance architecture**



## Functional overview

Functional overviews are presented for each of the following tools:

- “Network Viewer” (page 33)
- “Alarm Display” (page 34)
- “Alarm Help” (page 35)

- “Network Status Bar” (page 35)
- “Component Information Viewer” (page 36)
- “Component Status Display” (page 37)
- “Command Console” (page 38)

## Network Viewer

The Network Viewer displays the network topology in a graphical format and allows you to monitor the state of the network.

See the table “Network Viewer features” (page 33) for the features of the Network Viewer tool.

**Table 1**  
**Network Viewer features**

Feature	Description
Graphical view	View the network down to the port level.  View different organizational levels of the network at the same time.  Display a defined map in the background
Textual view	Textually display all subcomponents.
Component state	Indicated by the color of the component icon or link line. Color is also used in the textual view.  Put components into maintenance or acknowledged modes.
(Sheet 1 of 2)	

**Table 1 (continued)**  
**Network Viewer features**

Feature	Description
Look and feel	<p>Customize your view of the network.</p> <p>Display subcomponents by a shelf icon or textual list.</p> <p>Temporarily position nodes and links on the screen.</p> <p>Zoom in and view different areas of the network.</p>
Navigation	<p>Use the Component Finder.</p> <p>Move through the levels of the organization using organization or background navigation.</p>
Access	<p>Directly access the Component Information Viewer.</p> <p>Access your tools and macros.</p>
Edit the network	<p>Edit and organize the network through the Network Viewer editor.</p>
(Sheet 2 of 2)	

## Alarm Display

The Alarm Display provides a list of alarm logs and active alarms in the network. Any device can be viewed in the common alarm format. The display can be refreshed manually or automatically in the Active mode.

*Note:* The Passport Active Alarm List feature keeps all non-cleared SET alarms on switch.

For example, when first connecting or after a reset database, those alarms are retrieved from the switch. This enhances the active Alarm Display information since real device alarms are shown instead of MDM generated proxy alarms. To activate this feature on the Passport switch, see 241-5701-611 *Passport 7400, 15000, 20000 Data Collection Guide*.

See the table “Alarm Display features” (page 35) for the features of the Alarm Display tool.

**Table 2**  
**Alarm Display features**

Feature	Description
Textual view	View the alarms that are affecting your network. View the total number of active alarms in the network. Extensive filtering of the alarms. Set Effects for specific visual or audible effects.
Alarms	Clear an active alarm.
Access	Directly access the Component Information Viewer for more data. Directly access Alarm Help to analyze fault codes. Access your macros and tools.

## Alarm Help

The Alarm Help utility lets you view detailed alarm code descriptions to assist in problem detection and correction.

## Network Status Bar

The Network Status Bar provides a high-level view of the state of the network and monitors the network condition using global statistics. From the Network Status Bar, you can display a list of troubled components. Because the Network Status Bar is context-linked to the Component Information Viewer and the Alarm Display tools, you can drag and drop components onto these tools to diagnose faults in the network.

## Component Information Viewer

The Component Information Viewer allows you to diagnose network component faults by viewing information on the component, its related components, and the network management data (alarms and status records). The Component Information Viewer uses alarm-based surveillance to find more information on the impact and history of the fault. It also uses state-based surveillance to provide more information on the probable cause and context of the fault.

See the table “Component Information Viewer features” (page 36) for the features of the Component Information Viewer tool.

**Table 3**  
**Component Information Viewer features**

Feature	Description
Textual view	View a group of related components. View pertinent information such as alarms.
Access to network information	Access all available Network Model information. Get active alarm information. Look up recent alarm history. Access status information (DPN-100).
Component state	View the state of all components displayed. The state is indicated by name and color. Put components into maintenance or acknowledged states.
Alarms	Clear an active alarm.
Look and feel	View only components for the states that you select. Have the Component Information Viewer automatically updated whenever you select a different component in the Network Viewer.
(Sheet 1 of 2)	

**Table 3 (continued)**  
**Component Information Viewer features**

Feature	Description
Navigation	Navigate to related components.
Access	Directly access the Component Information Viewer, General Data Reporter, DPN Performance Viewer, Data Viewer, and Customer Database.  Access your tools and macros.
(Sheet 2 of 2)	

## Component Status Display

The Component Status Display provides a textual representation of the organization at region, site, module, component, and subcomponent levels in the network. For a graphical representation of the same information, use the Network Viewer.

See the table “Component Status Display features” (page 37) for the features of the Component Status Display tool.

**Table 4**  
**Component Status Display features**

Feature	Description
Textual view	View the network down to the subcomponent level in textual format.
Component state	View the state of all components displayed. The state is indicated by an icon.  Put components into maintenance or acknowledged state.
Look and feel	Choose which component types and states you want to display in your Component Status Display.  Sort components by state, component name, or time of last state change.
(Sheet 1 of 2)	

**Table 4 (continued)**  
**Component Status Display features**

Feature	Description
Navigation	Move through the levels of the organization on selected components.
Access	Directly access the Component Information Viewer.
(Sheet 2 of 2)	

## Command Console

For details about the Command Console utility, see the Command Console section in 241-6001-804 *Preside MDM Workstation Utilities User Guide*. The Command Console is the operator command application that allows you to issue operator commands directly to switching devices in the network. You can perform the following functions using the Command Console:

- issue commands to DPN, Passport, and SNMP devices
- support multiple simultaneous connections to OAs or Passport nodes in the network
- issue commands to the local workstation (macros)
- write your own operator command macros. For more information, see the section on creating and using macros in 241-6001-301 *Preside MDM Customization Administrator Guide*.

## Context

Context lets you pass values among those Preside Multiservice Data Manager (MDM) tools that support context. Values are shared through the use of the MDM Context Server.

The Put context command puts an item of information into a context buffer, and the Get context command takes the information from the buffer. By using the context commands, you can avoid some repetitive data entry work. The context buffer, however, can hold only one item of information at a time. Terminating a tool does not erase the contents of a context buffer; the buffers are erased when you log off.

## Start Tool

Several surveillance tools support a Start Tool menu. The purpose of this menu is to integrate tool and utility launching points in Preside Multiservice Data Manager (MDM). So, from one tool you can start other tools and utilities.

The tools and utilities that you can start may vary depending on several factors. Such factors include the type of devices in the network, the tool from which you select the Start Tool command, whether an item is selected when the Start Tool command launches, and whether the Start Tool menu has been customized at your installation.

When you select the Start Tool command, a menu opens and displays a list of tool categories. Each category supports a selection of tools and utilities that you can start. The following list details all MDM Start Tools categories and their associated tools and utilities. Based on the software installed at your organization, you may not see the complete list.

- Fault
  - Component Information Viewer
  - Circuit Viewer
  - Acknowledge Alarms on Component
  - Unacknowledge Alarms on Component
  - Alarm Help
- Configuration
  - Component Provisioning
  - Network Configuration System (NCS)
  - Nodal Provisioning
  - Service Provisioning
    - SPVC
    - SPVP
    - Trunk
    - VCC Bearer Service
    - VPC Bearer Service
    - CES over PVC

- CES SVC
- Frame Relay
- IP VPN Global Update
- DPN Component Provisioning
- Network Reporting System
  - Configuration Reports
  - Configuration Differences
- Web Configuration
- PP4400 Component Provisioning
- Passport/SNMP Data Backup/ Restore
- Performance
  - Data Viewer
  - DPN Performance Viewer
- Utilities
  - Customer Data
  - Operator Commands
  - Command Console
  - Remote MDM Session
  - MIB Browser

For details on customizing the Start Tool menu, see 241-6001-301 *Preside MDM Customization Administrator Guide*.

## Common surveillance tasks

Network operators perform common surveillance tasks, such as monitoring the network for faults (global network status through the Network Status Bar, state-based through the Network Viewer, or Component Status Display or alarm-based through the Alarm Display); diagnosing the cause of the faults and its impacts; and taking remedial actions.

You can use a combination of surveillance tools to perform common tasks. Specific procedures, based on the tool and task, are provided in the following sections:

- “Finding troubled components” (page 41)
- “Monitoring a selected set of components” (page 43)
- “Responding to troubled or out-of-service states” (page 44)
- “Determining a problem” (page 45)
- “Putting a component into maintenance state” (page 46)
- “Putting a component in acknowledged state” (page 47)
- “Clearing an alarm” (page 48)
- “Acknowledging/Unacknowledging an alarm” (page 48)
- “Fixing a problem” (page 49)
- “Changing the Network Viewer display” (page 49)

## **Finding troubled components**

To quickly find troubled components, you can use the Network Status Bar, Network Viewer, Component Status Display, Alarm Display, and Component Information Viewer tools. If the Component Information Viewer is open with Auto Context Active turned on, component information from the Network Viewer, Component Status Display, and Alarm Display is passed to this tool for processing. See “Setting Preferences” (page 350) for more information.

For references to specific tools and tasks for finding troubled components, see the table “Finding troubled components” (page 42).

**Table 5**  
**Finding troubled components**

Tool and task	Reference
<b>Network Status Bar</b>	"Network Status Bar" (page 289)
<ul style="list-style-type: none"> <li>• Monitor network status.</li> <li>• Identify troubled components.</li> </ul>	"Network Status Bar overview" (page 289) "Using the Troubled Components Dialog" (page 297)
Network Viewer	"Network Viewer" (page 51)
<ul style="list-style-type: none"> <li>• Navigate through the network.</li> </ul>	"Using the Component Finder" (page 81) "Using organization navigation" (page 85) "Using background navigation" (page 91)
Component Status Display	"Component Status Display" (page 397)
<ul style="list-style-type: none"> <li>• Navigate through the network.</li> <li>• Set component filtering.</li> </ul>	"Starting the Component Status Display" (page 418) "Changing the Component Filter Settings" (page 421)
Alarm Display	"Alarm Display" (page 221)
<ul style="list-style-type: none"> <li>• Display active alarms</li> <li>• Display alarm logs</li> <li>• Setting alarm filters.</li> <li>• Setting special effects.</li> </ul>	"Viewing alarms in the Active mode" (page 226) "Viewing alarms in the Log mode" (page 236) "Defining filters" (page 245) "Setting alarms by effects" (page 254)
Component Information Viewer	"Component Information Viewer" (page 301).
<ul style="list-style-type: none"> <li>• Turn on Auto context active.</li> </ul>	"Setting Preferences" (page 350)
(Sheet 1 of 2)	

**Table 5 (continued)**  
**Finding troubled components**

Tool and task	Reference
<ul style="list-style-type: none"> <li>Set component filters.</li> </ul>	"Setting component filters" (page 348)
<ul style="list-style-type: none"> <li>Set information type.</li> </ul>	"Displaying additional component information" (page 360)
(Sheet 2 of 2)	

## Monitoring a selected set of components

You can select a set of components that you want to monitor at a site, module, component, or subcomponent level of an organization. In the Alarm Display you can also perform filtering on specific components.

For references to specific tools and tasks for monitoring components, see the table "Monitoring selected components" (page 43)

**Table 6**  
**Monitoring selected components**

Tool and task	Reference
Component Status Display	"Component Status Display" (page 397)
<ul style="list-style-type: none"> <li>Choose the area of the network that you want to monitor.</li> </ul>	"Starting the Component Status Display" (page 418)
<ul style="list-style-type: none"> <li>Select the types of components with particular states or critical levels that you want to monitor.</li> </ul>	"Changing the Component Filter Settings" (page 421)
<ul style="list-style-type: none"> <li>Sort the list of components by state, component name, or time, and set the update interval.</li> </ul>	"Setting the sort key for the components list" (page 423) "Setting the Auto-Refresh interval" (page 424)
Network Status Bar	"Network Status Bar" (page 289)
(Sheet 1 of 2)	

**Table 6 (continued)**  
**Monitoring selected components**

Tool and task	Reference
<ul style="list-style-type: none"> <li>Identify troubled subcomponents.</li> </ul>	"Troubled Components Dialog" (page 294)
Network Viewer	"Network Viewer" (page 51)
<ul style="list-style-type: none"> <li>Navigate through the network.</li> </ul>	"Using the Component Finder" (page 81) "Using organization navigation" (page 85) "Using background navigation" (page 91)
Alarm Display	"Alarm Display" (page 221)
<ul style="list-style-type: none"> <li>Filter alarms.</li> </ul>	"Filtering alarms" (page 245)
(Sheet 2 of 2)	

## Responding to troubled or out-of-service states

If you find a troubled component, or you receive an alarm indicating in-service troubled (ISTB) or out-of-service (OOS) state, use the tools described in the table "Responding to troubled or out-of-service states" (page 44) to respond.

**Table 7**  
**Responding to troubled or out-of-service states**

Tool and task	Reference
Network Viewer	"Network Viewer" (page 51)
<ul style="list-style-type: none"> <li>Use the Component Finder.</li> </ul>	"Finding a component using the Component Finder" (page 82)
<ul style="list-style-type: none"> <li>Use organization navigation.</li> </ul>	"Expanding in place to the next lower level" (page 85)
Component Status Display	"Component Status Display" (page 397)
(Sheet 1 of 2)	

**Table 7 (continued)**  
**Responding to troubled or out-of-service states**

Tool and task	Reference
<ul style="list-style-type: none"> <li>• Navigate through the network.</li> <li>• Set the component filtering.</li> </ul>	<p>“Starting the Component Status Display” (page 418)</p> <p>“Setting component filtering from the Component Filter Settings Dialog” (page 421)</p>
Alarm Display	“Alarm Display” (page 221)
<ul style="list-style-type: none"> <li>• Interact with the Component Information Viewer.</li> </ul>	“Passing component information from Alarm Display to Component Information Viewer” (page 258)
Component Information Viewer	“Component Information Viewer” (page 301)
<ul style="list-style-type: none"> <li>• Select the problem subcomponent.</li> </ul>	“Setting a target in the related components panel” (page 355)
(Sheet 2 of 2)	

## Determining a problem

After you locate the component causing the problem in the network, you need to determine the underlying cause of the problem, its importance, and its impact.

For references to specific tools and tasks for determining a network problem, see the table “Determining the cause of network problems” (page 45).

**Table 8**  
**Determining the cause of network problems**

Tool and task	Reference
Component Information Viewer	“Component Information Viewer” (page 301)
<ul style="list-style-type: none"> <li>• Navigate through the network.</li> </ul>	“Component Information Viewer data” (page 302)
(Sheet 1 of 2)	

**Table 8 (continued)**  
**Determining the cause of network problems**

Tool and task	Reference
<ul style="list-style-type: none"> <li>Set the information type.</li> <li>Get more data from other tools.</li> </ul>	<p>“Setting component filters” (page 348)</p> <p>“Start Tool” on page 39</p>
Alarm Help	See “Alarm Help” (page 267).
<ul style="list-style-type: none"> <li>Look up the fault code.</li> </ul>	
(Sheet 2 of 2)	

## Putting a component into maintenance state

After you find a problem, you may want to put the component in maintenance state while it is being fixed.

For references to specific tools and tasks for putting components in maintenance state, see the table “Putting a component in maintenance state” (page 46).

**Table 9**  
**Putting a component in maintenance state**

Tool and task	Reference
Network Viewer	“Network Viewer” (page 51)
<ul style="list-style-type: none"> <li>Put the subcomponent into maintenance.</li> </ul>	“Putting components into the Acknowledged state” (page 80)
Component Status Display	“Component Status Display” (page 397)
<ul style="list-style-type: none"> <li>Put the subcomponent into maintenance.</li> </ul>	“Putting a component into Maintenance state” (page 420)
(Sheet 1 of 2)	

**Table 9 (continued)**  
**Putting a component in maintenance state**

Tool and task	Reference
Component Information Viewer	"Component Information Viewer" (page 301)
<ul style="list-style-type: none"> <li>Put the subcomponent into maintenance.</li> </ul>	"Setting the maintenance state for a component" (page 357)
(Sheet 2 of 2)	

## Putting a component in acknowledged state

After you find a problem, you may want to put the component in acknowledged state to mask its real state.

For references to specific tools and tasks for putting components in acknowledge state, see the table "Putting a component in acknowledged state" (page 47).

**Table 10**  
**Putting a component in acknowledged state**

Tool and task	Reference
Network Viewer	"Network Viewer" (page 51)
<ul style="list-style-type: none"> <li>Put the subcomponent into acknowledged state.</li> </ul>	"Putting components into the Acknowledged state" (page 80)
Component Status Display	"Component Status Display" (page 397)
<ul style="list-style-type: none"> <li>Put the subcomponent into acknowledged state.</li> </ul>	"Putting a component into Acknowledged state" (page 420)
Component Information Viewer	"Component Information Viewer" (page 301)
<ul style="list-style-type: none"> <li>Put the subcomponent into acknowledged state.</li> </ul>	"Setting the acknowledge state for a component" (page 356)

## Clearing an alarm

Normally, operators do not clear alarms. They are cleared after the component is restored. If necessary, you can clear an active alarm; but once cleared, it cannot be retrieved.

For references to specific tools and tasks for clearing an alarm, see the table “Clearing an alarm” (page 48).

**Table 11**  
**Clearing an alarm**

Tool and task	Reference
Component Information Viewer <ul style="list-style-type: none"> <li>• If necessary, clear the alarm.</li> </ul>	“Component Information Viewer” (page 301) “Clearing active alarms for DPN” (page 361)
Alarm Display <ul style="list-style-type: none"> <li>• If necessary, clear the alarm.</li> </ul>	“Alarm Display” (page 221) “Clearing active alarms for DPN” (page 229)

## Acknowledging/Unacknowledging an alarm

After you investigate a the cause of an alarm, you may choose to acknowledge the alarm. This indicates to other network operators that the problem is under investigation. Conversely, you might choose to unacknowledge a previously acknowledged alarm.

For references to specific tools and tasks for acknowledging or unacknowledging an alarm, see the table. “Acknowledging and Unacknowledging an alarm” (page 49)

**Table 12**  
**Acknowledging and Unacknowledging an alarm**

Tool and task	Reference
Component Information Viewer	“Alarm acknowledgement and unacknowledgement” (page 275)
Alarm Display	“Alarm acknowledgement and unacknowledgement” (page 275)

## Fixing a problem

After a problem is diagnosed, you can fix or circumvent it by issuing commands from the Command Console. See the Command Console section in 241-6001-804 *Preside MDM Workstation Utilities User Guide* for information on this tool.

## Changing the Network Viewer display

You can customize the Network Viewer display by saving different views of the network.

For references to specific tasks for changing the Network Viewer display, see the table “Changing the Network Viewer display” (page 49).

**Table 13**  
**Changing the Network Viewer display**

Tool and task	Reference
Network Viewer	“Network Viewer” (page 51)
<ul style="list-style-type: none"> <li>• Displaying nodes and shelves</li> <li>• Zoom to a larger view.</li> <li>• Save a view of the network that is to be used often.</li> </ul>	<ul style="list-style-type: none"> <li>“Displaying nodes” (page 63)</li> <li>“Zooming in on the display” (page 91)</li> <li>“Using Views of the network” (page 99)</li> </ul>



## Chapter 2

# Network Viewer

---

This section describes the Network Viewer and provides you with instructions on how to use this tool. The following information is included:

- “Network Viewer overview” (page 51)
- “Using the Network Viewer tool” (page 53)
- “Interacting with other tools” (page 56)
- “Understanding the network display” (page 61)
- “Navigating the network display” (page 81)
- “Controlling the network display” (page 93)
- “Customizing the Network Viewer display” (page 100)
- “Troubleshooting” (page 113)

### Network Viewer overview

The Network Viewer is a network component state surveillance tool used for the detection of faults for DPN, Passport, and selected SNMP devices in the network. The Network Viewer displays state and topology information for the physical and organizational components that make up the network.

### Network Viewer capabilities

The Network Viewer allows you to perform the following functions:

- use advanced navigational capabilities to locate components and alter the display of the network with great flexibility

- display module subcomponents down to the port level to trace a high-level problem down to its source at the subcomponent level
- display different organizational levels of the network at the same time (for example, a mixed display of regions, sites, and modules)
- display a defined map in the background of the Network Viewer display
- put both modules and subcomponents into maintenance state or acknowledged state
- save a Network Viewer display configuration so that you can retrieve it and display it again later
- use filtering to make state surveillance more efficient
- customize such items as tools menus, alarms, and the use of color for states
- edit the contents and structure of the network model. For details, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.
- save a number of user-specific preference settings and re-apply them automatically when the Network Viewer is restarted.

## Network Viewer modes

The Network Viewer operates in two modes:

- surveillance
- edit

### Surveillance mode

In surveillance mode, the Network Viewer enables you to navigate the network and to monitor the states of network components.

### Edit mode

In edit mode, the Network Viewer enables you to monitor network element states and allows you to edit the network model. For more information on how to edit the model with Network Viewer, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

## Using the Network Viewer tool

This section describes

- how to start the Network Viewer tool
- how to use the Network Viewer popup menu
- how to use the Network Viewer Menu Bar
- how to use the Network Viewer Icon Bar menu
- how to interact with other Preside Multiservice Data Manager (MDM) tools
- how to exit the Network Viewer tool

### Starting Network Viewer

The Network Viewer connects to the network model server referred to by current service selection. If the service selection changes, you are prompted for confirmation of the change. For additional information, see the section on using the Service Selection tool in 241-6001-303 *Preside MDM Administrator Guide*.

**Note:** Your workstation may be set up so that the Network Viewer window opens when you log on. Your system administrator can set this option.

#### Starting the Network Viewer

- 1 In the Preside MDM window, select Fault ->Network Viewer.

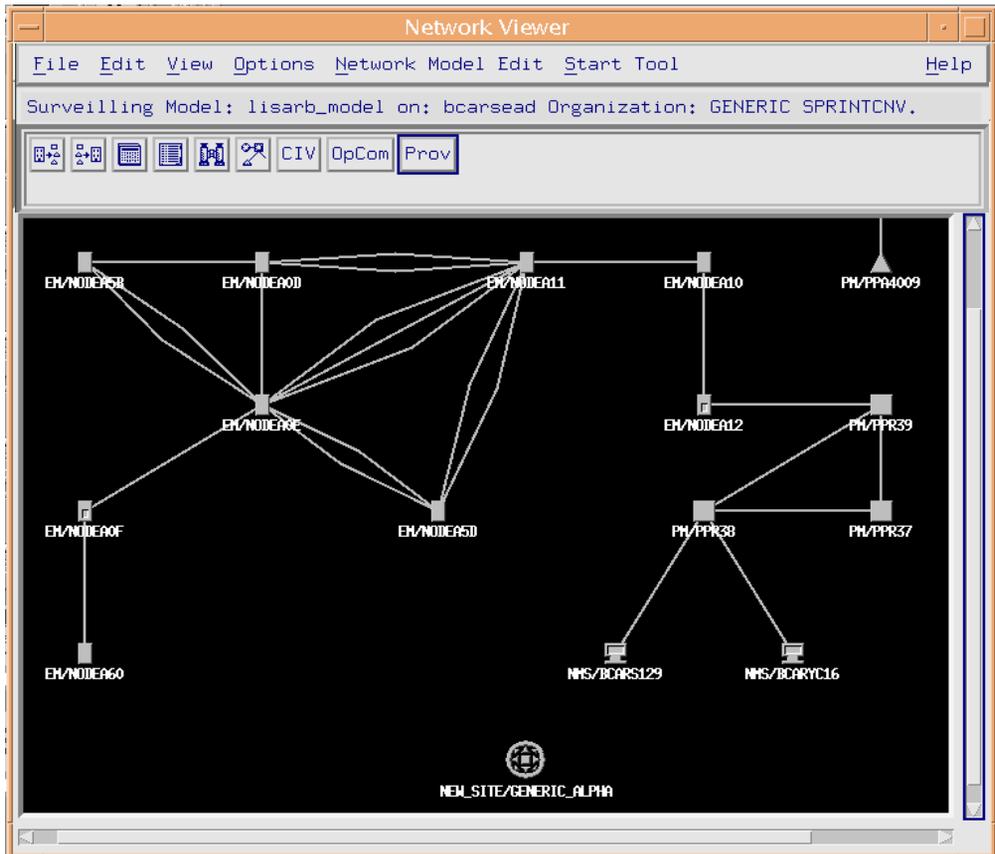
The Network Viewer window opens.

- 2 If more than one organization is defined, the organizational icons display. Go to step 3. If only one organization is defined, Network Viewer opens with the view of that organization. Go to step 3.
- 3 To open the display of an organization, double-click on the organization you want to view.

The first level components of the selected organization display in the Network Viewer window.

General operations are available from these menus positioned in the Network Viewer menu bar: *File*, *Edit*, *View*, and *Options*. Another menu provides access to the network model edit mode and options. See the

online help available from each menu for an explanation of the menu items.



## Using the Network Viewer Icon Bar

The Network Viewer supports an icon bar that consists of a selection of buttons. These buttons provide quick access to frequently used commands and tools. When you position the mouse pointer over a button, the Network Viewer displays a tooltip below that button. This tooltip contains the name of the command represented by the button.

By clicking on a button in the icon bar, you can:

- operate a range of expand and compress view options
- select components and organizations to view
- start other tools and utilities
- pass component IDs to invoked tools
- view context-sensitive help information about individual items from the icon bar

The mode of operation of the Network Viewer determines which buttons appear in the icon bar. Some buttons appear only in edit mode or only in surveillance mode. Other buttons appear in both modes.

You can show or hide the icon bar. If you hide the icon bar, the tool commands contained in it are still available. Access other tools using the Network Viewer pop-up menu and selecting the *Start Tool* command. By default, the tools available from the Network Viewer *Start Tool* menu are the same as those that appear in the icon bar.

You can customize the Network Viewer icon bar (NDIconBar.menu) and the Network Model Edit icon bar (NDIconBarEdit.menu). For details, see 241-6001-301 *Preside MDM Customization Administrator Guide*.

### Showing the icon bar

- 1 From the Options menu, select Show Icon Bar.

The icon bar appears.

### Hiding the icon bar

- 1 From the Options menu, select Hide Icon Bar.

The icon bar disappears.

**Note 1:** Alternatively, use the Preferences Dialog to control the visibility of the Icon Bar. See “Using the Preferences dialog” (page 97) for more information.

**Note 2:** Icon bar contents can be customized. For details on customizing an icon bar, see the section on customizing toolsets and start tool menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

## Interacting with other tools

There are two methods that you can use to access component information available in other tools but not stored in the Network Viewer:

- “Context” (page 56)
- “Start Tool menus” (page 56)

### Context

Context commands allow component identifiers to be passed quickly from one tool to another. For example, the identifier of any node, link, or subcomponent can be put into context by Network Viewer and picked up by the Component Information Viewer to display detailed information for the component. To put an identifier into context, press the *Select* mouse button to ensure that the node, link, or subcomponent is selected.

### Start Tool menus

The Start Tool command supports a Start Tool menu that has a selection of tools and utilities that you can launch from the Network Viewer. Unlike other surveillance tools, the Network Viewer offers more than one type of Start Tool menu. You can access Start Tools from the following locations within the Network Viewer:

- surveillance mode icon bar
- model edit mode icon bar
- Start Tool menu
- Network Viewer pop-up menu
- Node pop-up menu
- Link pop-up menu
- Subcomponent pop-up menu

#### Surveillance mode icon bar

The surveillance mode icon bar contains a series of icons that let you start other tools and utilities. In surveillance mode, the Start Tool submenu in the Network Viewer pop-up menu is a textual representation of the same tools shown graphically in the icon bar. You can customize the content of the surveillance icon bar. Any modifications that you make apply only to the

surveillance icon bar and the Start Tool menu in the menu bar and in the Network Viewer pop-up menu. For details on customizing the surveillance icon bar, see the section on customizing toolsets and start tool menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

### **Model edit mode icon bar**

The model edit mode icon bar contains a series of icons that let you start other tools and utilities. In edit mode, the Start Tool submenu in the Network Viewer pop-up menu is a textual representation of the same tools shown graphically in the icon bar. You can customize the content of the edit mode icon bar. Any modifications that you make apply only to the edit mode icon bar and the Start Tool menu in the menu bar and in Network Viewer pop-up menu. For details on customizing the edit mode icon bar, see the section on customizing toolsets and start tool menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

### **Start Tool menu**

Use the Start Tool menu in the menu bar to launch other tools and utilities. The tools and utilities in the Start Tool menu are the same as those in the icon bar. Similar to the icon bar, the Start Tool menu in the menu bar changes content based on the mode of the Network Viewer. You can customize the content of the Start Tool menu. For details, the section on customizing toolsets and start tool menus in 241-6001-301 *Preside MDM Customization Administrator Guide*. The following list details the default Start Tool menu options and the mode in which they are available:

Expand in Place	Edit & Surveillance
Expand in New Window	Edit & Surveillance
Compress	Edit & Surveillance
Open Shelf Dialog	Edit & Surveillance
Open (Troubled) Subcomponent Dialog	Edit & Surveillance
Find	Edit & Surveillance

Select New Organization	Edit & Surveillance
Load/View Network Model File	Edit
Save Network Model	Edit
Collect Configuration Data	Edit
Apply/View Collection Files	Edit
Create/Edit Node	Edit
Create/Edit Link	Edit
Delete Selected Components	Edit
CIV (Component Information Viewer)	Surveillance
OpCom (Operator Commands)	Edit & Surveillance
Config	Edit & Surveillance
PP4400	Edit & Surveillance

If the corresponding software is installed, the Start Tool menu also displays the following tools:

Ct Viewer (Circuit Viewer)	Surveillance
----------------------------	--------------

### **Network Viewer pop-up menu**

You can access the Network Viewer pop-up menu by positioning the mouse pointer on the Network Viewer background and pressing the mouse menu button.

The Network Viewer pop-up menu contains a Start Tool command that opens a Start Tool submenu. The content of the Start tool submenu changes depending on whether the Network Viewer is in surveillance mode or model edit mode. If you customize a Network Viewer icon bar, the changes are reflected in the Start Tool submenu.

**Node pop-up menu**

You access the Node pop-up menu by positioning the mouse pointer on a single or multiple nodes and pressing the mouse menu button. The Node pop-up menu contains a Start Tool command that opens a Start Tool menu. For a list of tools that you can start from this menu, see “Start Tool” (page 39).

**Link pop-up menu**

You access the Link pop-up menu by positioning the mouse pointer on a link and pressing the mouse menu button. The Link pop-up menu contains a Start Tool command that opens a Start Tool menu. For details on the content of this menu, see “Start Tool” (page 39).

**Subcomponent pop-up menu**

Access the Subcomponent menu using the following procedure:

- 1 Position the mouse pointer on a node and press the mouse menu button.  
A Node pop-up menu opens.
- 2 From the pop-up menu, select the Show Subcomponents command.  
The dialog opens displaying a list of subcomponents.
- 3 Position the mouse pointer on a specific subcomponent in the list and press the mouse menu button.  
The Subcomponent pop-up menu opens.

The Subcomponent pop-up menu contains the Start Tool command that opens a Start Tool menu. For details on the content of this menu, see “Start Tool” (page 39).

**Exiting the Network Viewer**

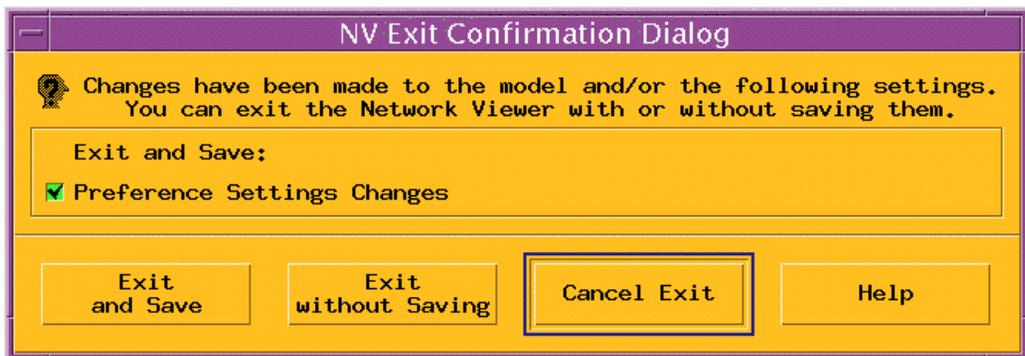
To exit the Network Viewer, select *Exit* from the File menu.

If you have not modified any Filter or Preference Settings, an NV Exit Confirmation Dialog opens. Select *Exit Application* if you want to exit or *Cancel Exit* if you want to remain in Network Viewer.

If you modify any Filter or Preference Settings and do not save them to your user-specific file, Network Viewer asks if you want to do so before exiting. The *NV Exit Confirmation Dialog* allows you to save the modified settings and exit Network Viewer, exit Network Viewer without saving, or cancel the exit and return to the Network Viewer main window.

The figure “NV Exit Confirmation Dialog” (page 60) shows a sample dialog that displays when you exit the Network Viewer.

**Figure 2**  
**NV Exit Confirmation Dialog**



**Note:** This dialog appears only if the filter settings are changed or if the *confirmExit* resource is set to the default *True*.

For the instructions to set this resource, see the section on customizing toolsets and start tool menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

### Canceling exit

- 1 If you do not want to exit, select the Cancel Exit button from the dialog.

The exit dialog disappears and you are returned to the Network Viewer main window.

### Exiting and saving settings

- 1 Select the *Exit and Save* button from the dialog.

The filter or Preference settings (or both) that you create are saved to your user-specific file, and you exit the Network Viewer.

### Exiting without saving settings

- 1 Select the *Exit without Saving* button from the dialog.

The modified filter or Preference settings (or both) are not saved and you exit the Network Viewer.

## Understanding the network display

Two basic kinds of components are displayed by Network Viewer—nodes and links. Nodes include physical nodes and organizational nodes. Links include physical links and organizational links. Each component (node or link) has an object menu from which operations specific to the component are available.

The Network Viewer display can have background maps assigned to organizations, and nodes and link endpoints can be assigned. Network Viewer display configuration is part of the overall task of network model configuration. This is handled by the Network Viewer in edit mode. See 241-6001-015 *Preside MDM Network Model Administrator Guide* for details on network model configuration.

If node positions are not configured in the Network Viewer, the nodes are displayed with a *grid cyclic* policy; that is, they are placed side by side, a row at a time, along an imaginary grid. The grid starts at the upper left corner of the map and works its way from left to right, top to bottom, to the lower right corner of the map. When the grid is filled, the procedure starts over at the upper left corner, placing nodes one on top of the other.

This section describes how to

- display Network Viewer legend
- display Nodes
- display Node labels
- control Node positioning
- display Links
- display Nodes and Links owned by a site or region
- display subcomponents as shelf icons
- display subcomponents in a textual list

- display component states

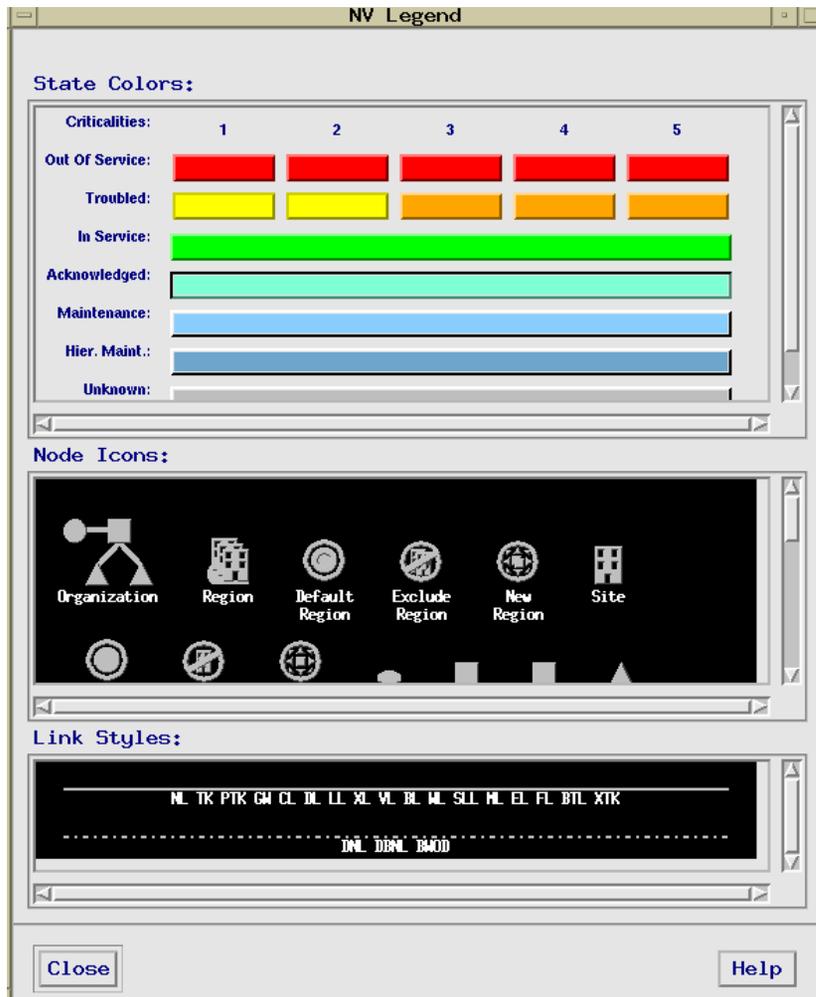
## **Displaying the Network Viewer legend**

The Network Viewer legend shows the colors associated with state values and conditions. It also shows the meaning of icons and link styles.

### **Displaying the Network Viewer legend**

- 1 From the Options menu, select Legend.

The Network Viewer legend opens.



You can leave the legend open for reference or collapse it to an icon.

## Displaying nodes

Nodes are represented by icons positioned on a background map of the organization displayed in the main Network Viewer window. The node type is indicated by the shape of the icon. Nodes can be these types of icons:

- Polygon (or Type)

- Shelf

**Note:** You can display a label with the node name under the icon.

The Network Viewer Legend shows the meaning of these icons. See “Displaying the Network Viewer legend” (page 62).

### **Polygon icons**

*Polygon* or *Type* icons identify the node type by their shape. Polygon icons are simple geometric shapes representing the component type. There are polygon icons for all the network model node types. In addition, a default polygon icon is available for any type not in this set.

**Note:** Polygon icons are full color pixmaps of any size, shape, and detail.

### **Shelf icons**

*Shelf* icons are displayed only for certain node types in a separate dialog. Shelf icons usually represent physical components housed in a shelf. An exception to this is the Passport icon, which displays the node’s logical processors.

## **Node types in the Network Viewer and the network model**

The set of node types that are distinguished by different polygon icons in the Network Viewer differs slightly from the set of node types that are defined in the network model. For example, the Network Viewer has distinct icons for each of AM, RM, DPN-100/1, MAS, LDM, and DPN-100/5, which are all defined as type *PM* in the network model. Network Viewer distinguishes between these module types using attribute information stored in the network model. The set of node types distinguished by the Network Viewer and the corresponding network model node types are shown in the table “Node types and description” (page 65).

**Note:** Many other nodes are distinguished by customer-specific icons.

**Table 14**  
**Node types and description**

Network Viewer node type	Network Model node type	Description	Shelf dialog available
AM	PM	DPN Access Module (Default for PM components)	yes
RM	PM	DPN Resource Module	yes
DPN-100/1	PM	DPN-100/1 and Downloadable DPN-100/1	yes
MAS	PM	Magellan Access Switch (same icon as DPN-100/5)	yes
DPN-100/5	PM	DPN-100/5	yes
PP4100	PM	Passport 4100	yes
NM	NM	DPN Network Module	no
OA	OA	NCS Operations Agent	no
EM	EM	Enterprise Module (Passport 16-slot)	yes
EM3	EM	Passport 3-slot	yes
EM5	EM	Passport 5-slot	yes
EM8	EM	Meridian Passport	yes
EMT	EM	Passport 15000	yes
EMN	EM	Passport 20000	yes
EMX	EM	Passport with unspecified shelf type	yes
MPA	MPA	Passport 4400 Access Device	yes
MPAX	MPA	Passport 4400 with unknown shelf type	no
LDM	MPA	Legacy Data Module	no
PA	PA	Passport Access Module	no
RBSE	RBSE	Radio Base Station Equipment (NNE)	yes
RCPE	RCPE	Radio Customer Premise Equipment (NIU)	yes

(Sheet 1 of 2)

**Table 14 (continued)**  
**Node types and description**

Network Viewer node type	Network Model node type	Description	Shelf dialog available
M1	M1	Meridian-1 Module	no
M1_11	M1	Meridian-1 Option 11 Module	no
SLAN	SLAN	Local area network (LAN) managed through SNMP	no
E_RTR	E_RTR	MAS embedded router	no
RTR/HUB/BR	RTR, HUB, BR	Router, hub, bridge, managed through SNMP	no
HOST	HOST	Host	no
FNMOD	FNMOD	Foreign Network Module (gateways)	no
NMS	NMS	generic network management system	no
BB	BB	Backbone Module	no
SITE	Organization node	Site node	no
REGION	Organization node	Region node	no
Organization	Organization node	Network model organizational hierarchy	no

(Sheet 2 of 2)

## Displaying the node labels

You can show or hide node labels independently of one another.

### Displaying node labels

- 1 To have all nodes show or hide their labels, choose *Show all node labels* or *Hide all node labels* from the options menu.
- 2 To have a single node show or hide its label, choose *Show label* or *Hide label* from its pop-up menu.

The nodes either show or hide their labels depending on which option you chose.

**Note:** Use the Preferences Dialog to control the appearance of the nodes. See “Using the Preferences dialog” (page 97).

## Positioning the nodes

You can use the mouse to position nodes in the Network Viewer display. If the Network Viewer is currently in Editing mode, these position changes are permanent in the network model and, therefore, available to all instances of Network Viewer monitoring this network. Otherwise, these changes are temporary and are known only to the current Network Viewer session.

Nodes are recorded in the network model exactly where you position them in the display. Cluster and pin options are available to help you position legibly and efficiently.

The Network Viewer allows you to enable/disable an invisible grid to run in the background. If the grid is enabled, nodes and endpoints snap to it as they are moved. This helps to position nodes and endpoints accurately.

**Note:** The various node positioning and clustering options described here are also controlled through the Preferences Dialog. See “Using the Preferences dialog” (page 97).

### Enabling the grid

- 1 On the *View* menu, choose *Snap to Grid*.

The invisible grid is enabled. Nodes and endpoints snap to the grid as they are moved.

### Disabling the grid

- 1 On the *View* menu, choose *Do Not Snap to Grid*.

The invisible grid stops running in the background. Nodes and endpoints, when moved, need to be aligned more carefully since they do not snap to a grid.

### Positioning a single node

- 1 To move a single node, press and hold the left mouse button and move the node to the position in the display you want it to occupy.

An outline of the node follows the cursor.

- 2 Release the left mouse button to position the node in the display.

The new node location appears in the Network Viewer display and is recorded in the network model.

### Positioning multiple nodes

- 1 To select several nodes, draw a rubber band around them; or press and hold the *Shift* key, and use the left mouse button to select nodes and links.

**Note:** To remove a node from the set of selected nodes, press and hold the *Control* key and click with the left mouse button.

- 2 Position the cursor on one of the selected nodes, and press the *Shift* key and the left mouse button.

When you start the move, a rectangle outlines the group.

- 3 Move the group to a chosen position and release the left mouse button.

Nodes are repositioned in the Network Viewer display and are recorded in the network model. Selected links with end points are also moved.

### Using the cluster and pin options

- 1 If you do not want to move certain nodes, invoke the *Node* pop-up menu, and select the *Pin* option from the *Edit* cascade menu.

Selected nodes are pinned to their positions in the display and are not affected by cluster commands.

- 2 Select a node with the left mouse button, and invoke the *Node* pop-up menu using the right mouse button.

- 3 On the *Edit* cascade menu, select *Cluster Connected Nodes* or *Cluster Child Nodes*.

Cluster Connected Nodes positions all nodes that connect to the selected node in a circle around the selected node; Cluster Child Nodes expands the selected node, and positions all subordinate nodes in a grid around the expanded node's original position.

**Note:** Nodes are never allowed to be positioned outside the map or viewspace boundaries, and will be automatically forced on if needed.

### Positioning a node to its previous or original position

- 1 Select the node with the left mouse button, and invoke the *Node* pop-up menu using the right mouse button.

- 2 To position the node to its previous position, select *Move to Previous Position* from the *Node* pop-up menu.

The node is repositioned to its previous position.

- 3 To position the node to its original position, select *Move to Original Position* from the *Node* pop-up menu.

The node is repositioned to its original position.

### Reverting all nodes to their current network model location

- 1 To revert all nodes to their current network model location, on the *View* menu choose *Set Shared Model Positions for all Nodes and Links*.

To revert *selected* nodes to their current network model location, on the *View* menu, choose *Set Shared Model Positions for Selected Nodes and Links*.

The nodes revert to their current network model location.

### Aligning and distributing nodes

- 1 To align and distribute selected nodes, on the *View* menu, choose *Align and Distribute Selected Nodes*.

## Displaying links

A link is displayed as a sequence of lines connecting the two link endpoints. Network links, trunks, gateways, and organizational links all appear as simple solid lines. Dial back-up network links (DBNL) are distinguished from other types of links through the use of a different line pattern. The line patterns are shown in the Network Viewer legend. For details, see “Displaying the Network Viewer legend” (page 62).

The link type for any link can be determined from the link identifier that appears in the link’s object menu. A link identifier has this format:

```
<-link type-> end1ID <-> end2ID
```

For example, the link identifier for a DPN network link might look like this:

```
<-NL-> PM/A15 PE/1 /PI/1 PO/4 <-> PM/R72 PE/3 PI/3 PO/5
```

A link identifier for a Passport to Passport trunk looks like this:

```
<-PTK-> EM/PASS1 TRK/20 <-> EM/PASS2 TRK/21
```

### Accessing the link menu

- 1 Move the pointer over the link you want to work with, and press *menu* to display the link menu selections.
- 2 Choose an action from the menu.

See online help for a full explanation of the menu selections.

### Link endpoints

You may add endpoints to a link to separate it from other links that may be superimposed over one another. Endpoints are the points where the lines meet.

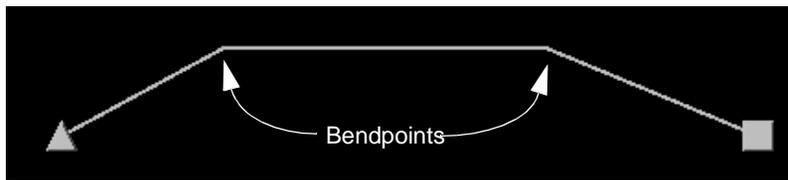
Link menus contain commands to show and hide endpoint handles.

Endpoint handles must be visible to move or delete single endpoints. You can access a endpoint menu to perform endpoint-related activities.

Overlapping links between two nodes can also be spread out by the automatic insertion of endpoints.

For an example of endpoints, see the figure “Link with endpoints” (page 70). For an example of endpoint handles, see the figure “Link with endpoints and handles” (page 70).

**Figure 3**  
**Link with endpoints**



**Figure 4**  
**Link with endpoints and handles**



### Accessing the endpoint menu

- 1 Move the pointer over the link whose endpoints you want to work with, press *menu*, and choose *Show Endpoint Handles*.

**Note:** If the endpoint handles are already showing, skip this step and proceed to step 2.

- 2 Move the pointer over the bendpoint handle you want to work with, and press *menu* to display the bendpoint menu selections.
- 3 Choose an action from the bendpoint menu.

### Automatically spreading the overlapping links

**Note:** This is available only if more than one link exists between two given nodes.

- 1 Spread the links using the *Link* pop-up menu. Use the Spread Links command, or double-click on the link.

All previous bendpoints are removed. New bendpoints are inserted at midsection to spread the links evenly.

**Note:** Use the Preferences Dialog to control the Link Spreading distance. See “Using the Preferences dialog” (page 97) for more information.

## Displaying nodes and links owned by a site or region

Nodes and links directly owned by a site or region can be displayed within a dialog. The dialog contains a list of components and an option button that enables you to toggle between the *All Components* and the *Filtered Components Only* view. In Filtered mode, only the nodes and links matching the current filter settings of the main window are displayed.

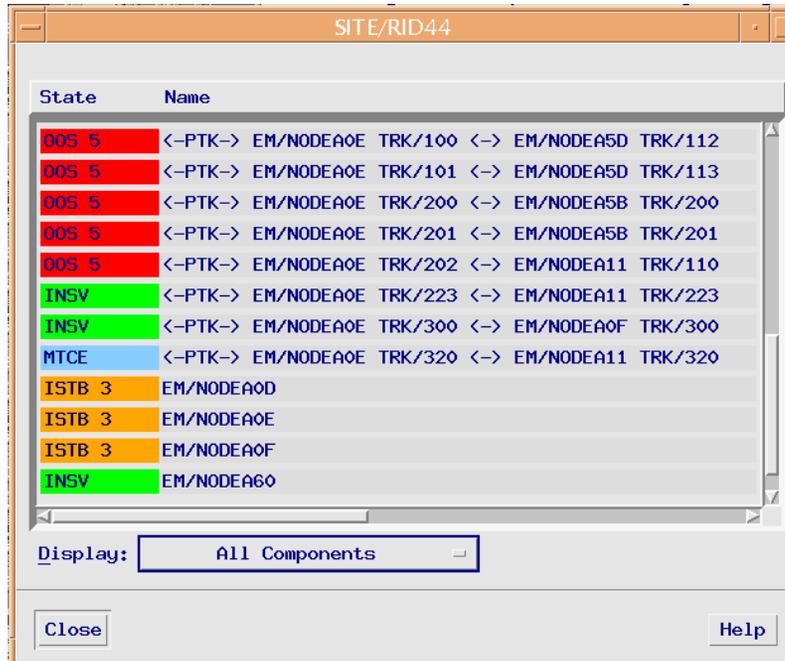
The nodes in the list support the standard Node pop-up menu, where all graphical commands are disabled. Similarly, the links in the list support the standard Link pop-up menu. Nodes and links also support the same double-click actions as in the main window. The components in the list can also be used as a drag source.

The Components Dialog can be invoked from the Node pop-up menu. For Organizational Nodes, the *Show Subcomponents...* command is replaced by *Show Children...*. The Icon Bar command for *Show Subcomponents* can also be used if the selected node is an organizational node.

### Displaying nodes and links owned by a site or region

- 1 Move the pointer over the site or region that contains the nodes and links you want to view.
- 2 Press *menu* to display the nodes and links.
- 3 Choose *Show Subcomponents...* from the cascade menu or, for Organizational nodes, choose *Show Children*.

A dialog containing the nodes and links is displayed.



## Displaying shelf views

You can display the logical shelf view for DPN devices or the logical and physical views for Passport multiservice devices. If you select a DPN device and then select the Shelf View command, the DPN logical shelf view displays as a shelf icon within the Network Viewer tool. If you select a Passport device and then select the Shelf View command, the Passport Surveillance Shelf View tool opens and display the logical and physical views of the Passport device. For details about the Passport Surveillance Shelf View tool, see “Passport Shelf View” (page 117).

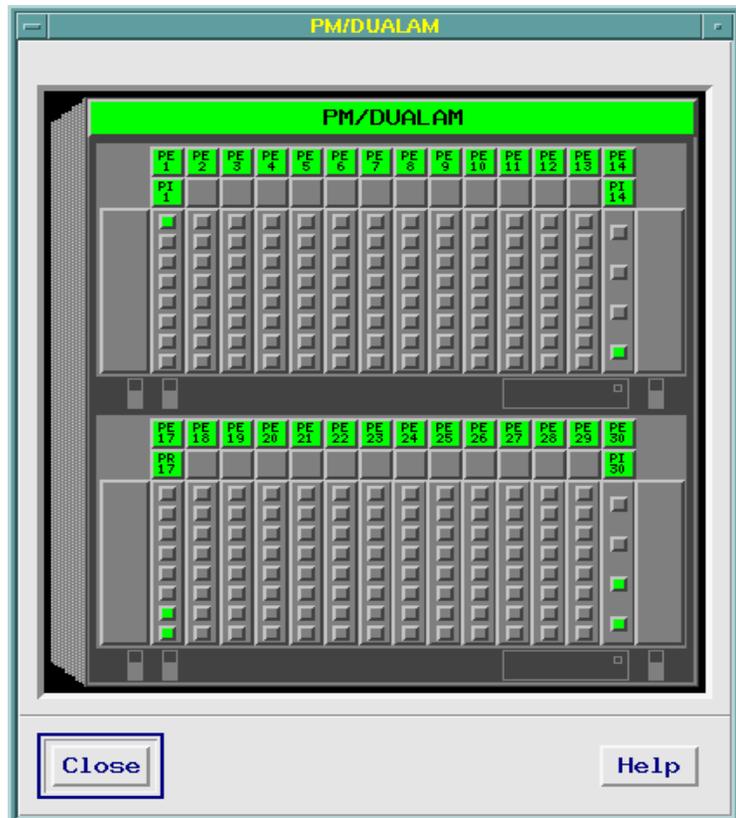
Each icon is configured according to the subcomponent information contained in the network model for the node. If the *Network Viewer* cannot determine the exact shelf type for a PM module, it uses an AM dual-shelf layout by default.

### Displaying the DPN shelf icon

- 1 Move the pointer over the node that contains the subcomponents you want to view.
- 2 Right-click on the node to display the Node pop-up menu.
- 3 From the Node pop-up menu, select **Show Menu**.

**Note:** The default display for a dual AM or dual RM shelf dialog has Shelf 0 on the top and Shelf 1 on the bottom. However, you can customize Network Viewer to display a dual AM or dual RM shelf dialog with Shelf 1 on the top and Shelf 0 on the bottom by entering `NV*reverseShelf:True` in your `Xdefaults` file.

A dialog containing the shelf icon for the node is displayed. The icon is colored according to its state. See “Displaying the Network Viewer legend” (page 62) in this guide and the section on network model states in 241-6001-015 *Preside MDM Network Model Administrator Guide*, for information on component states.



You can view pop-up menus for the node and its subcomponents by right-clicking a button in the shelf icon. See the menu's online help for a description of its commands.

### Displaying subcomponents in a textual list

Not all subcomponents of a node are displayed as part of a shelf icon. To see all subcomponents, use the Subcomponent dialog.

The Subcomponent dialog displays subcomponents in one of two modes: *All Subcomponents* or *Troubled Subcomponents Only*. The *All Subcomponents* mode displays all subcomponents. The *Troubled Subcomponents Only* mode displays only those subcomponents whose raw state is in-service—troubled (ISTB) or out of service (OOS). Components whose states are propagated as

ISTB or OOS are not included in the list. In *Troubled Subcomponents Only* mode, components are sorted so that troubled components appear first, components in Acknowledged state are shown second, and components in Maintenance state appear last. These categories are separated by labels. An option menu at the bottom of the dialog lets you change the display mode.

You can also reduce the number of subcomponents that are fetched and displayed by setting a criticality cutoff in the Preference Dialog (see “Using the Preferences dialog” (page 97)). Only subcomponents whose criticality is greater or equal to the specified criticality cutoff value are initially fetched (the default value is 1, indicating that all subcomponents should be displayed). Note that subcomponent notifications received for the node displayed in the dialog are added to the list regardless of their criticality value.

When the Subcomponent is displaying subcomponents with a criticality cutoff higher than 1, a label at the top of the dialog indicates this fact. An action button (*Load All*) is added to force all the remaining subcomponents to be loaded.

### **Displaying the subcomponent text dialog**

- 1 Move the pointer over the node that contains the subcomponents you want to view.
- 2 To open the *Subcomponent* dialog in the troubled mode, double-click the *Select* mouse button on the node icon, **or** press *menu* to display the Node object menu
- 3 Choose *Show Subcomponent Dialog...* from the menu.

The text dialog opens and displays the subcomponents belonging to the node. States of the subcomponents are also listed in this dialog. See “Displaying the Network Viewer legend” (page 62) in this guide and the section on network model states in 241-6001-015 *Preside MDM Network Model Administrator Guide*, for information on component states. Multiple subcomponent dialogs for different components may be displayed at the same time.

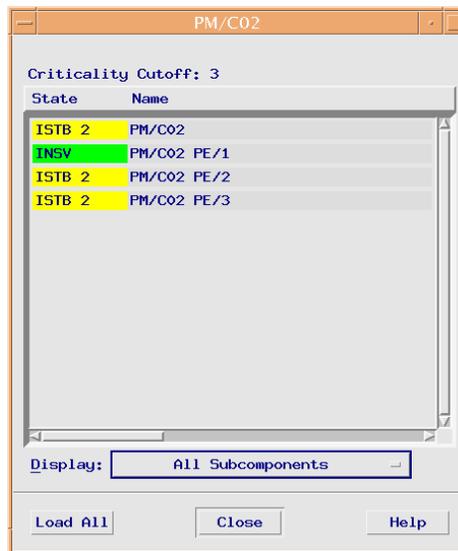
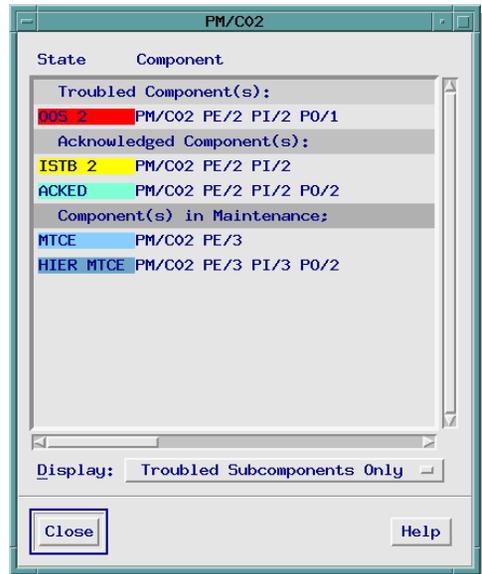
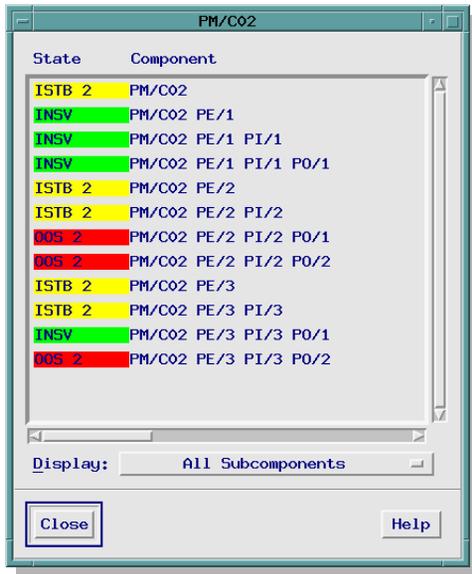
Object menus for the node and its subcomponents are accessible by pressing the *menu* button on their state or name fields. See the menu's online help for a description of its commands.

### **Changing the display mode of the subcomponent dialog**

- 1 Press the *menu* option button in the *Display* area.

- 2 Select the *All Subcomponents* or *Troubled Subcomponents Only* option.

**Note:** You can use the accelerators CTRL-a and CTRL-t from the dialog to change to the *All Subcomponents* or *Troubled Subcomponents Only* option respectively.



## Displaying component states

Component states are shown by colors. The Network Viewer Legend shows the meaning of these icons. See “Displaying the Network Viewer legend” (page 62).

Component states are managed by the Surveillance Network Model Updater, which is responsible for computing states and storing them in the network model. For more details on how component states are computed, see 241-6001-015 *Preside MDM Network Model Administrator Guide*. The Network Viewer is notified by the network model server whenever a component changes state. The Network Viewer responds to this notification by updating the network display.

The state displayed for a component is computed from the following factors:

- the network state of the component as determined from network data (alarms or status records, or both, depending on the type of component). The possible values for network state are described in the table “Component states” (page 78). The network states common to all component types.

**Table 15**  
**Component states**

State	Description
Unknown	No alarms or status records have been received for the component.
In-service	The component is functioning normally.
In-service-troubled	The component is functioning, but is experiencing some problem.
Out-of-service	The component or one of its parents is not functioning.

**Table 15 (continued)**  
**Component states**

State	Description
Maintenance / Hierarchic Maintenance	The component's real state and that of its subcomponents is masked pending corrective action.
Acknowledged	The component's real state is temporarily masked. If the real state changes, the acknowledgment is automatically removed.

- the criticality of the component: a number reflecting the importance of the component ranging from 1 (low importance) to 5 (high importance). Each component type has a default criticality that may be redefined during network model population. The criticality assigned to a component may be viewed in both the Component Information Viewer and the Network Viewer in edit mode.
- the states of related components. For more information on state and state propagation, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

A legend showing the state-color mapping is available from the Network Viewer *Options* menu. See “Displaying the Network Viewer legend” (page 62) to display the legend.

### **Node state display**

An icon is colored according to its state. If the shelf dialog is being displayed, a stripe across its shelf icon is colored to display the overall node state. The individual shelf components are colored to display the subcomponent states.

### **Link state display**

The line representing the link is colored according to the state.

### **Maintenance state**

Maintenance state hides a component's current state and any subsequent state changes. If you perceive a problem on a component, you can put the component into Maintenance state when you do not want to be distracted by the state display.

### Putting components into the Maintenance state

- 1 Move the pointer over the component to be put into the Maintenance state.
- 2 Press *menu* and choose *Set Maintenance On* from the menu.

The request is sent to the network model and, if accepted, the state of the component is changed to Maintenance state. See 241-6001-015 *Preside MDM Network Model Administrator Guide*, for more information on the Maintenance state.

### Taking components out of the Maintenance state

- 1 Move the pointer over the component to be taken out of the Maintenance state.
- 2 Press *menu* and choose *Set Maintenance Off* from the menu.

The component is taken out of the Maintenance state. The Network Model Updater recomputes the component's state based on its state when received from the network and on the states of its related components.

### Acknowledged state

Acknowledged state temporarily hides a component's current Troubled state (indicated by the network). As soon as the component changes state, the acknowledgment is automatically removed and the component's real state shows. When a component is acknowledged, it acts as though it is in an *In Service* state. That is, if a lower subcomponent is also troubled, it is reflected on the Acknowledged state through the usual propagation mechanisms—thus showing hidden faults. The only difference is that, if no other related components are troubled, the acknowledged component displays a state of *Acked* instead of *In Service*. Only troubled modules and subcomponents (from the network) can be acknowledged.

### Putting components into the Acknowledged state

- 1 Move the pointer over the component to be put into the Acknowledged state.
- 2 Press *menu* and choose *Set Acknowledged State On* from the menu.

The request is sent to the network model and, if accepted, the state of the component is changed.

**Note:** You can also acknowledge all active alarms against the component by using the corresponding *Start Tool* menu option.

### Taking components out of the Acknowledged state

- 1 Move the pointer over the component to be taken out of the Acknowledged state.
- 2 Press *menu* and choose *Set Acknowledged State Off* from the menu.

The component is taken out of the Acknowledged state. The Network Model Updater recomputes the component's state based on its state when received from the network and on the states of its related components.

**Note:** You can also unacknowledge all active alarms against the component using the corresponding *Start Tool* menu option.

## Navigating the network display

For large networks, it is generally neither feasible nor desirable to view the entire network at once in the Network Viewer display window. These kinds of navigation are provided by the Network Viewer:

- Component Finder
- Organization navigation
- Background navigation
- Double-click actions

### Using the Component Finder

The Component Finder is the main navigational tool. It allows you to quickly locate components and to change the main window display to bring different components into view. The Component Finder Dialog contains a *mini map* representing the entire Network Viewer background. A rectangle, called the *mini view window*, indicates the part of the background that is currently displayed in the Network Viewer window (especially when zoom is used). This gives you a sense of where you are in the overall network display. The bitmap being displayed (if any) is not visible in the mini map.

When the finder locates a specific node, it displays this found node as a *mini node* in the mini map. Like the real node, the mini node can be selected by dragging the mouse pointer over it while pressing the *Select* button, or by double-clicking the *Select* button while the mouse pointer is on it. After the mini node is selected, you can access a pop-up menu from which you can issue actions such as expanding and opening dialogs.

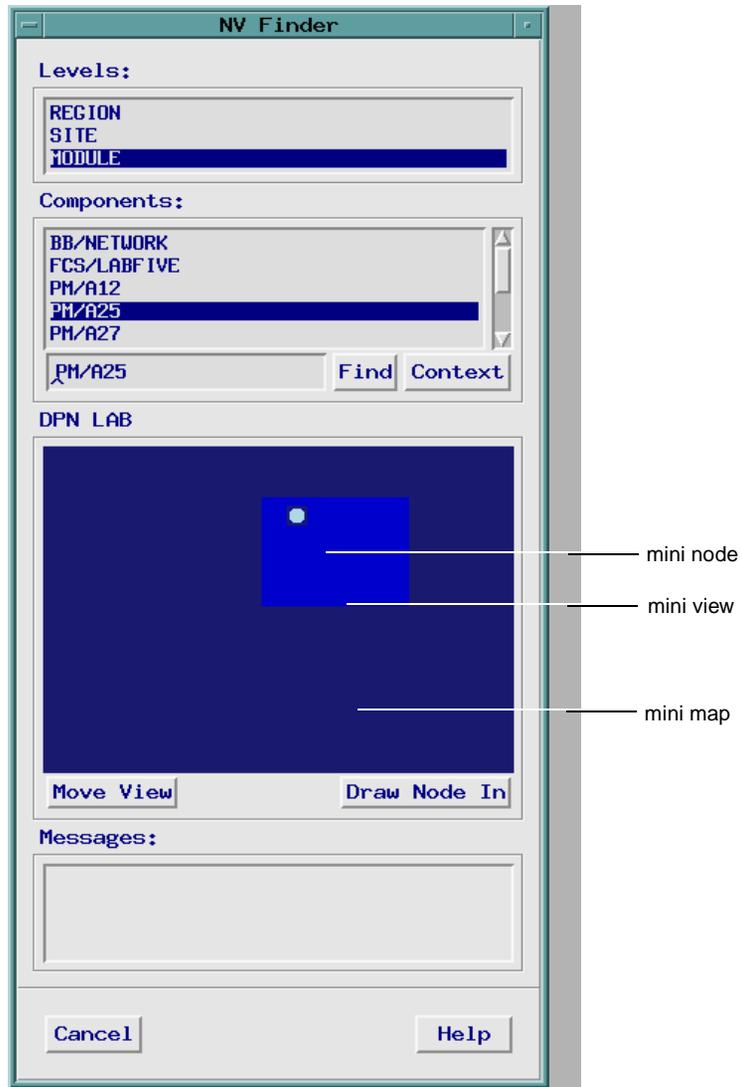
The Component Finder provides an input field where you can enter the identifier of the component you want to find. The identifier may be selected from a list of components, typed in directly, or retrieved from context. The contents of the Component Selection List are determined by the selection in the Level Selection List, which lists the levels of the organization. For standard organizations, the levels are region, site, and module. Components below the module level are not listed since they do not have individual locations on a map. However, they are displayed as icons that are accessible from the module.

### **Finding a component using the Component Finder**

- 1 Press *menu* with the pointer over *View* in the Network Viewer menu bar.
- 2 Choose *Find* from the cascade menu.

The Component Finder Dialog opens.

**Note:** You can search for only one component at a time.



- 3 Type a component ID in the *component ID field*, retrieve it from context, or select an item in the Components List.
- 4 Select *Find*.

The location of the module is shown in the mini map.

If the specified component is not found in the model, is an already un-expanded node, is not part of the currently displayed organization, or is invisible due to some exclusive expansions, a message indicating this is displayed in the message area. If the node is not available for filtering, a message appears indicating this.

If the specified component is found in the current display, the finder indicates its location by displaying a circle in the mini map. The component is highlighted in the Network Viewer display window. The component remains highlighted until the next selection is made, or the component is deselected in the main navigation window (which also removes the tracking of the node in the finder dialog). If the component is found in compressed state, the mini node is displayed as a slightly larger square. The larger square represents the organizational node that needs to be expanded to display the component (which can be done by double-clicking the mini node).

If the circle is outside the rectangle, you can move the current window view to include the component, or move the component into the current window view.

**Note 1:** When a component is retrieved from context, this step is performed automatically.

**Note 2:** If an item in the Components List is double-clicked instead of just single-clicked, this step is performed automatically.

### **Changing the window view to include the target component**

- 1 Repeat steps 1 to 4 of “Finding a component using the Component Finder” (page 82).
- 2 Drag the mini view window over the indicated component, or select the *Move View* button located under the mini map.

This automatically moves the window over to the indicated component so that it is just inside the view. The Network Viewer window view changes correspondingly.

**Note:** Dragging the mini view window may be done only if the view area is not the entire map background (possible due to zooming in on a particular area of interest). If the view area is the entire map, then the mini view window fills the entire mini map space in the finder.

### **Moving a component into the current view**

- 1 Repeat steps 1 to 4 of “Finding a component using the Component Finder” (page 82).

- 2 Drag the mini view window over the indicated component, or select the *Draw Node In* button located under the mini map.

The component moves to the interior of the window rectangle. The component icon is correspondingly moved into the Network Viewer window view.

**Note:** To move the component back to its previous or original position, select *Undo Last Move* or *Undo All Moves* from its object menu. See “Positioning the nodes” (page 67).

## Using organization navigation

Organization navigation allows you to navigate through the network organizational hierarchy, expand nodes to show their subcomponents or compress subcomponents into their higher level parents.

**Note:** An organizational component and the components it contains are never displayed simultaneously.

You can expand a node by the following methods:

- in-place
- exclusive
- in a new window

### Expanding in place

Expanding in place replaces any selected organizational node with its children while leaving the display of unselected nodes unchanged. Links between the newly shown nodes and other organizations are visible.

### Expanding in place to the next lower level

- 1 Move the pointer over the component that you want to expand to the next lower level.
- 2 Double-click the *Select* mouse button. Alternatively, press the *Menu* mouse button and choose *Expand In Place*.

The selected component is replaced with the next level of subcomponents.

**Note:** Only the selected component is expanded; all other components in the display remain unchanged.

### Expanding in place to the lowest level

1

2 Move the pointer over the component that you want to expand to the lowest level.

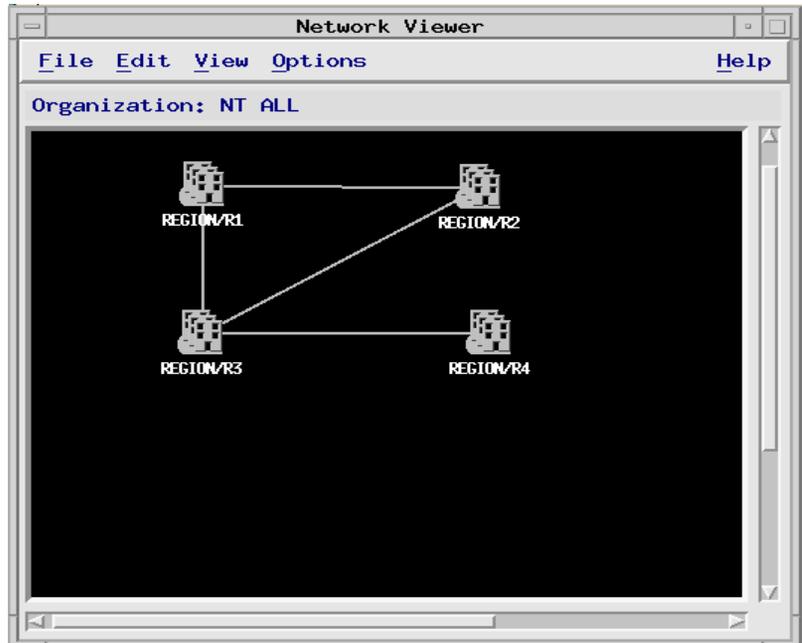
3 While holding down the Shift key, double-click the *Select* mouse button. Alternatively, press the mouse *Menu* button and choose *Full Expand In Place*.

The selected component is replaced with a view of all its subcomponents (if any) down to the module level.

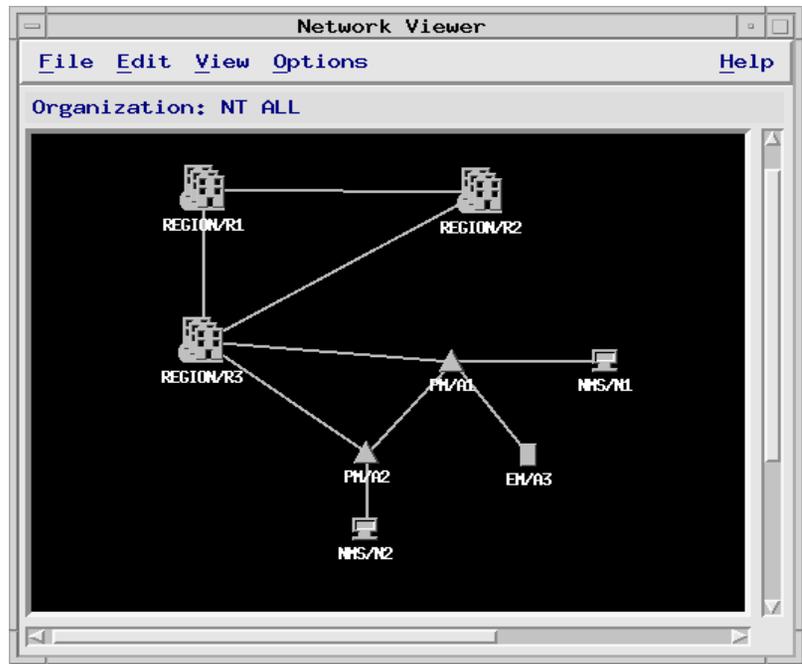
The figure “Before in-place expansion to the lowest level” (page 87) illustrates the network view before in-place expansion for REGION 4.

The figure “After in-place expansion to the lowest level” (page 88) illustrates the view after REGION 4 is expanded down to its module level. The single link between REGION 3 and REGION 4 is expanded to two physical links—one to PM A1 and the other to PM A2.

**Figure 5**  
**Before in-place expansion to the lowest level**



**Figure 6**  
**After in-place expansion to the lowest level**



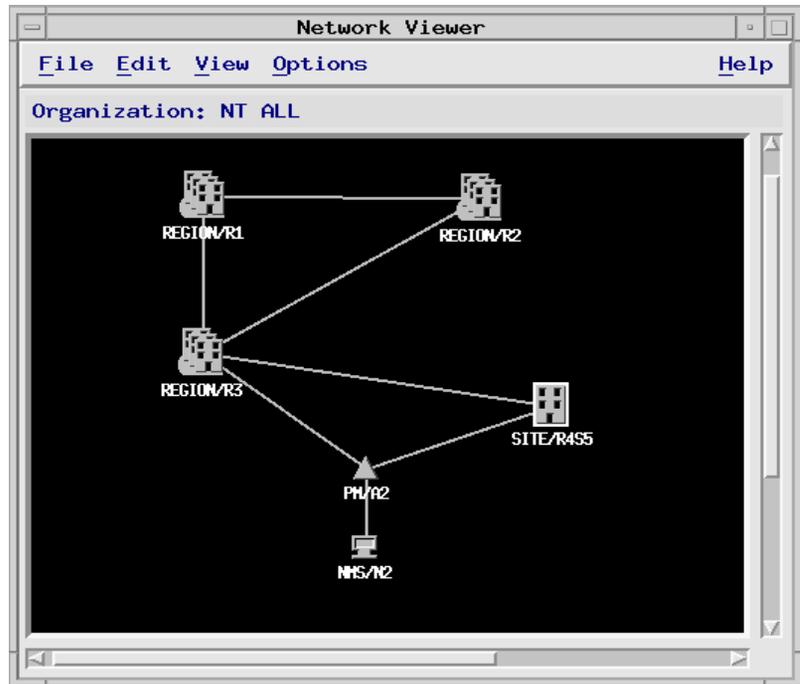
### Compressing a component back to the parent level

- 1 Move the pointer over the component whose parent you want to view.
- 2 While holding the Control key, double-click the *Select* mouse button.  
**Alternatively**, press the mouse *Menu* button and choose *Compress In Place*.

The selected component and all other components having the same immediate parent component are replaced by the parent component.

The figure “After in-place expansion to the lowest level” (page 88) illustrates the network view after SITE 5 is compressed in place. EM A3 and all other modules in SITE 5 are replaced by the SITE 5 icon.

**Figure 7**  
**Compressing a component to its parent level**



### Expanding exclusively

Exclusive expansion replaces any selected organizational node with its children and hides the display of other unselected and unexpanded nodes. Links between the visible nodes and other organizations are not visible. When nodes are hidden due to exclusive expansions, the word *Partial* appears in the status label.

### Expanding exclusively to the next lower level

- 1 Move the pointer over the component that you want to exclusively expand to the next lower level.
- 2 Press the *Menu* mouse button and choose *Expand Exclusively*.

The selected component is replaced with the next level of subcomponents. All other nodes are hidden.

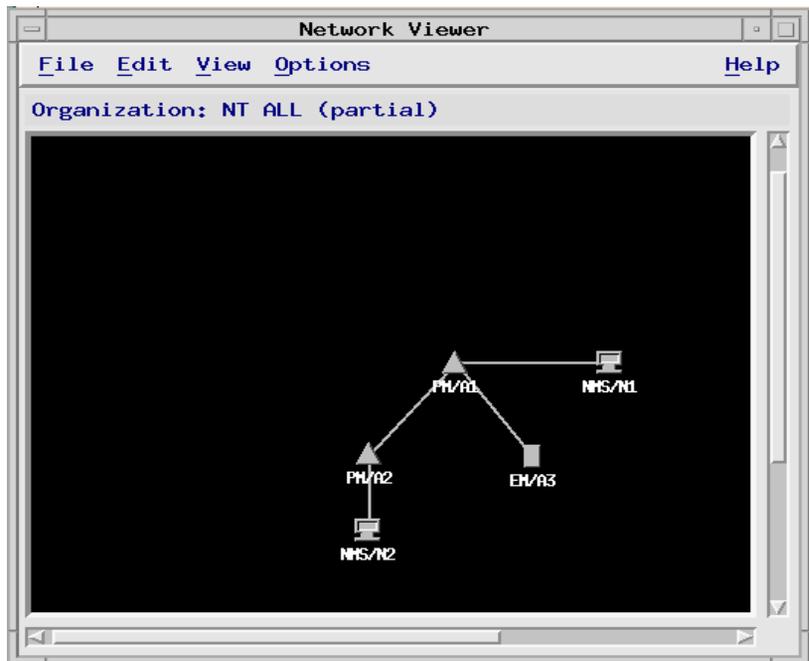
### Expanding exclusively to the lowest level

- 1 Move the pointer over the component that you want to exclusively expand to the lowest level.
- 2 Press the *Menu* mouse button and choose *Full Expand Exclusively*.

The selected component is replaced with a view of all its subcomponents (if any) down to the module level. All other nodes are hidden.

In this example SITE 5, as shown in the figure “Exclusive expansion to the lowest level” (page 90), is exclusively expanded to the lowest level.

**Figure 8**  
**Exclusive expansion to the lowest level**



### Expanding in a new window

Expanding in a new window provides exclusive expansion of organizational nodes into new subwindows. These subwindows provide functionality similar to that of the main window. You can distinguish subwindows by their title bar.

A node or link cannot appear in more than one window at any one time. As a result, non-organizational nodes cannot be included in subwindows during expansion as this would result in the same node being displayed in two windows.

### **Expanding to the next lower level in a new window**

- 1 Select one or more regions or sites, or both.
- 2 From the View menu or the Node pop-up menu, choose *Expand in New Window*.

A new subwindow opens displaying the next lower level for each selected organizational node.

### **Expanding to the lowest level in a new window**

- 1 Select one or more regions or sites, or both.
- 2 From the View menu or the Node pop-up menu, choose *Full Expand in New Window*.

A new subwindow opens displaying the lowest level for each selected organizational node.

### **Closing a subwindow**

- 1 From the File menu, select *Compress parent node which closes this window and its subwindows*. Alternatively, you can use the Network Viewer pop-up menu. From this pop-up menu, point to *File* and select *Compress parent node which closes this window and its subwindows*.

The subwindow closes.

## **Using background navigation**

Background navigation allows you to change the visible part of the map. You can use the scroll bars across the bottom and along the right side of the Network Viewer display window to change the area displayed. You can also zoom the display.

### **Zooming in on the display**

- 1 Move the pointer over the *View* button in the menu bar and press *menu*.
- 2 Choose *Zoom*.

A cascade menu appears listing the available magnification factors.

- 3 Choose a magnification factor.

The display is zoomed around the current center point to the selected magnification factor.

### Zooming out

- 1 Move the pointer over the *View* button in the menu bar and press *menu*.
- 2 Choose Zoom.  
A cascade menu appears listing the available magnification factors.
- 3 Choose a lower magnification factor than the current setting.

## Using double-clicking actions

You can double-click the *Select* mouse button and use it with the *Shift*, *Control*, or *Meta* keyboard keys to act on nodes, links, and subcomponents in the Network Viewer. The table “Default double-clicking actions” (page 92) lists the default actions for Network Viewer. These actions can be customized.

**Table 16**  
**Default double-clicking actions**

Node type	Key held down	Default action
Organizational root node	none	Opens the organization
Organizational node	none	Same as <i>Expand In Place</i> pop-up menu command
Organizational node	Shift	Same as <i>Full Expand In Place</i> pop-up menu command
Organizational node	Ctrl	Same as <i>Compress</i> pop-up menu command
Organizational node	Meta	Starts CIV tool
Module node	none	Same as <i>Open Subcomponent Dialog</i> pop-up menu command, but in Troubled mode
Module node	Shift	Same as <i>Open Shelf Dialog</i> pop-up menu command
Module node	Ctrl	Same as <i>Compress</i> pop-up menu command
(Sheet 1 of 2)		

**Table 16 (continued)**  
**Default double-clicking actions**

Node type	Key held down	Default action
Module node	Shift + Meta	Same as <i>Expand in New Window</i>
Module node	Meta	Starts CIV tool
Subcomponent	Meta	Starts CIV tool
Link	Meta	Starts CIV tool
Link	none	spreads overlapping links
(Sheet 2 of 2)		

## Controlling the network display

You can control the network display by

- setting Component filtering using the Network Viewer Filter Settings Dialog. For more information, see “Using the NV Filter Settings Dialog” (page 93).
- setting node, cluster and positioning, and other preferences using the Preferences Dialog. For more information, see “Using the Preferences dialog” (page 97).
- setting various Views of the network. For more information, see “Using Views of the network” (page 99).

## Using the NV Filter Settings Dialog

Network Viewer component filtering enhances state surveillance by

- showing only the modules and links that require attention
- minimizing the display clutter by hiding irrelevant nodes and links
- speeding up display operations by reducing the number of displayed modules

The *NV Filter Settings Dialog* allows you to tailor the NV Component Filter to your own preferences. With the *NV Filter Settings Dialog*, you can select active filtering options. You can also *Save to file* or *Restore from file* the settings and *Apply* the defined settings to the main Network Viewer display.

Whether Component filtering is enabled or not when the Network Viewer starts is controlled by the Preference Dialog. See “Using the Preferences dialog” (page 97) for more information.

**Note:** Filtering is turned off by default; however, you can change this default by setting the *ND\*compFilteringOn* resource to *True* in your user specific file: *\${HOME}/MagellanNMS/Xdefaults*. If you set this resource, the saved preferences are automatically restored the next time the Network Viewer is started.

The Network Viewer supports filtering on component states and overriding conditions. After you select the node states and link states that you want filtered, you have the option of overriding these state filters by

- hiding DPN-100/1 nodes
- hiding Magellan Access switches (MAS)
- hiding cross-level links (links from a node to a site or from a site to a region in the context of Network Viewer’s in-place expansions)
- showing DNLs and DBNLs

**Note:** This override does not apply to BWODs. BWODs are not considered to be DBNLs or DNLs for filtering purposes; they are filtered like NLs.

- showing backbone components (RM, Passports, TKs, and PTKs by default)
- hiding Passport trunks
- hiding ATM links

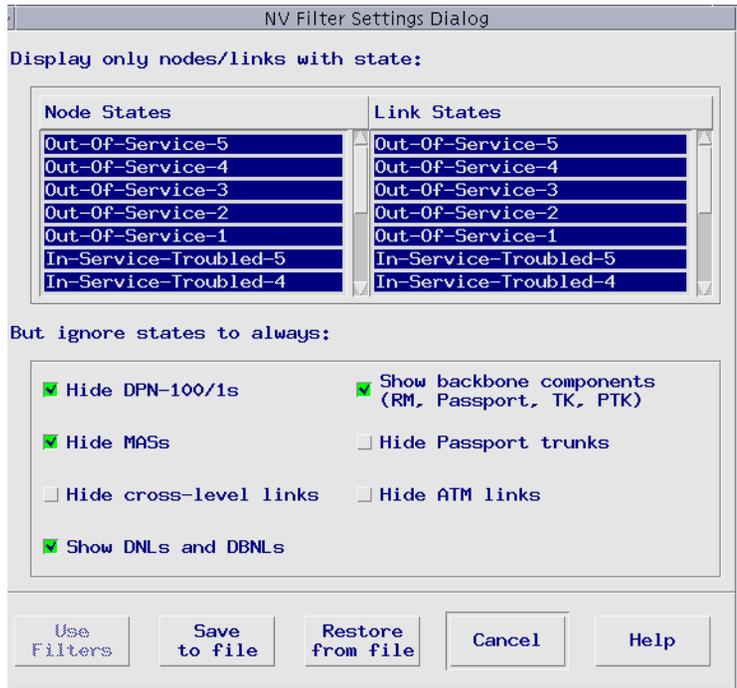
### **Changing the filtering of the states of nodes and links**

- 1 Ensure that the *Set filtering* option under the *View* menu in the Network Viewer main window is turned to On.

See “Activating and deactivating filter settings from the Network Viewer main window” (page 96) for more information.

- 2 Open the NV Filter Settings Dialog:
  - a. From the Network Viewer main window menu bar, select *Options*.

- b. From the *Options* menu, select *Change filter settings*.  
The NV Filter Setting Dialog opens.



- 1 Select the node states you want to filter from the *Node States* column.
- 2 Select the link states you want to filter from the *Link States* column.
- 3 Select the overriding conditions from the *But ignore states to always* list.

**Note:** These overrides function only if the network model is properly populated with the information necessary to identify these components.

- 4 Save the settings:

If you want to save the settings to the *NDFilter.cfg* file in your *\$HOME/MagellanNMS* directory, select *Save to File*.

If you want to save the settings to the Network Viewer main window, select *Apply*.

**Note:** The settings are applied to the Network Viewer main window only if the *Set filtering* option under the *View* menu in the Network Viewer main window is set to *On*. See “Activating and deactivating filter settings from the Network Viewer main window” (page 96) for more information.

- 5 Close the NV Filter Settings Dialog by selecting *Close*.

The NV Filter Settings Dialog closes.

### **Activating and deactivating filter settings from the Network Viewer main window**

The *Set Filtering On* option under the *View* menu in the Network Viewer main window enables the filter parameters set in the *NV Filter Settings Dialog* to be applied to the Network Viewer main window.

- 1 Press *Select* on the *View* menu in the Network Viewer main window.
- 2 Choose *Set Filtering On* to activate the filter parameters or *Set Filtering Off* to deactivate them.

The Preference Dialog enables and disables the Component filtering when Network Viewer starts. See “Using the Preferences dialog” (page 97) for more information.

### **Using previously saved filter settings**

You can retrieve and apply previously filter settings saved to the *NDFilter.cfg* file in your *\$HOME/MagellanNMS* directory.

### **Restoring previously saved filter settings**

- 1 Open the NV Filter Settings Dialog:
  - a. From the Network Viewer main window menu bar, select *Options*.
  - b. From the *Options* menu, select *Change filter settings*.

The NV Filter Setting Dialog opens.

- 2 Select *Restore from file*. to apply the filter settings saved to the *NDFilter.cfg* file.

The restored filter settings are displayed in the dialog.

- 3 Select *Apply* to save the filter settings to the Network Viewer main window.

## Using the Preferences dialog

The NV Preferences dialog allows you to modify a number of display and behavioral settings for the Network Viewer. You can save these settings so they can be automatically restored and applied whenever the Network Viewer is invoked. The Preference Settings come in the following categories:

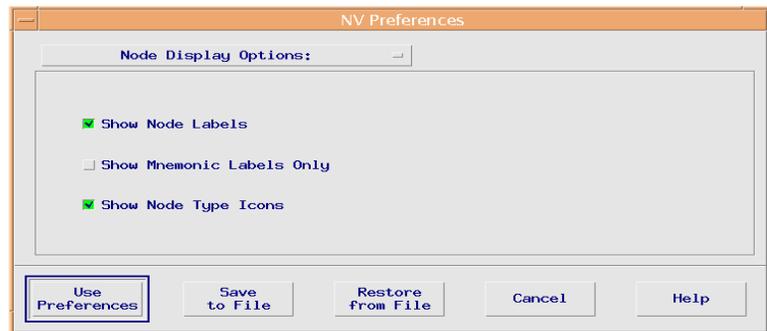
- Node Display
- Clustering and Positioning
- Miscellaneous

Some of the settings, including Snap to Grid, are also available from other Network Viewer menus.

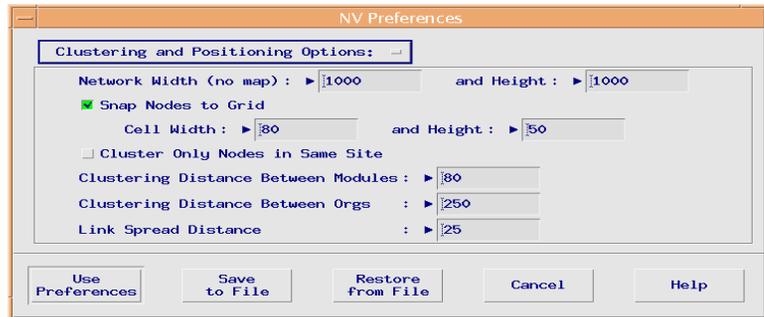
### Changing the display options for Network Viewer

- 1 Press *menu* on *Options* in the Network Viewer main window menu bar.
- 2 Choose *Change Preferences* from the menu.

The NV Preferences dialog window opens.



- 3 Select the option you wish to use from the *Node Display Options* button.



- 4 Select *Save to File* if you want to save these filter settings to the *NVFilter.cfg* file in your *\$HOME/MagellanNMS* directory.

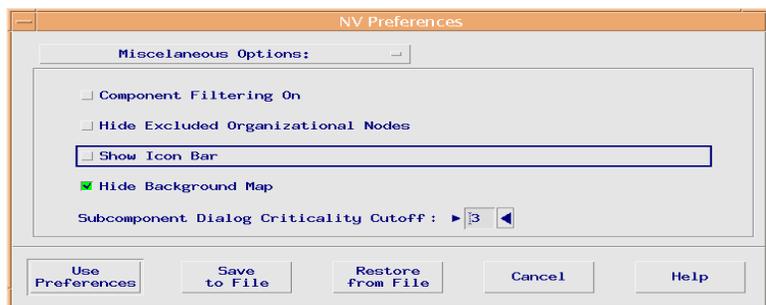
The settings made in the dialog are saved. The changes are not applied and the dialog remains open.

- 5 Select *Apply* to apply these settings to the Network Viewer main window.

**Note:** These settings are applied only if the *Set filtering* option under the *View* menu in the Network Viewer main window is set to *On*. See “Activating and deactivating filter settings from the Network Viewer main window” (page 96) for more information.

- 6 Select *Close* to close the dialog window.

The NV Filter Settings Dialog closes.



## Using Views of the network

You can save a *view* that is used often under a view *name* to quickly retrieve and display it. By saving the view under a view name, you can store key portions of the network and switch very rapidly to different views. A named view stores the following information:

- organization that is displayed
- coordinates and zoom factor of the visible section of the organization's map
- components that are expanded in the view
- visibility of node labels
- visibility of link bendpoint handles
- modified node and bendpoint positions (optional)
- snap-to-grid state
- the network dimensions (without map if they are changed in the Preferences Dialog)

### Saving a view

**1** Have your network display in the format you want to save.

**2** Press *menu* on *File* in the menu bar.

**3** Choose *Save View* from the menu.

The current view is saved to its file.

You can also choose *Save View As* from the menu.

A dialog opens, enabling you to save the view under a specified name.

**4** If you chose to save the view under a specified name, enter the filename, or select the name if it appears on the menu.

**5** To save the positions of nodes and bendpoints that are changed in the view, ensure that *Save Node Positions in View* is enabled on the toggle button.

If enabled, a checkmark appears on the left. Modified node positions are saved in the view.

If you do not want to save modified node positions in the view, deselect the toggle button.

The checkmark disappears and nodes are not saved in view.

### Restoring a view

1 Press *menu* on *File* in the menu bar.

2 Choose *Restore View...* from the menu.

A file selection dialog that contains a list of the names of all saved views is displayed.

3 Select the view you want to display in the window.

**Note:** For instructions on setting a default view for Network Viewer, see “Selecting the default view” (page 102).

4 To restore modified node positions that are saved in the view, ensure that *Restore Node Positions in View* is enabled on the toggle button.

If enabled, a checkmark appears on the left. Saved node positions are restored from the view.

If you do not want to restore saved node positions from the view, deselect the toggle button.

The checkmark disappears and saved node positions are not restored from the view.

## Customizing the Network Viewer display

You can perform the following types of customization on the Network Viewer:

- select the background pixmap image
- select the default view
- select the color and display options
- modify the Start Tool menus and icon bars

### Selecting the background pixmap image

The Network Viewer uses XPM3 format pixmaps for the background. This is a widely supported format. Various public- and commercial-domain tools allow you to create in, or convert other images to, this format. The *Solaris Common Desktop Environment (CDE)* software provides a pixmap editor that you can use for modifying pixmaps. This editor is located in the file */usr/dt/bin/dticon*. For instructions on how to use this pixmap editor, see the Help menu in the tool itself.

**Note:** The dticon editor is limited to relatively small pixmaps (256x256). To edit larger pixmaps, use a commercial tool or, if preferred, a public domain tool (such as xpaint, which is available from the MIT ftp site ftp.x.org).

The pixmap files used by Network Viewer are stored in the directory */opt/MagellanNMS/lib/nds/pixmaps*.

You can use the pixmaps stored in this directory as a starting point, and edit them with a pixmap editor; or you can import your own pixmaps. Store any pixmaps that you edit or create in the directory */opt/MagellanNMS/cfg/nds/pixmaps*. After your custom pixmaps are stored there, they are available to the Network Organization Populator through the Set organization map dialog. For more information, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Additional geographical area pixmaps are available from the Preside Multiservice Data Manager (MDM) CD ROM in the directory */cdrom/cdrom0/NVMaps*. Use the *installmap* tool on the CD ROM to install these pixmaps.

## Changing node icon pixmap images

Network Viewer uses XPM3 pixmaps to define the appearance of node icons. The pixmaps for all Network Viewer node icons can be found in the directory */opt/MagellanNMS/lib/nds/pixmaps*.

To change these pixmaps, use any available tool (commercial or otherwise) capable of editing XPM format images. The Icon Editor that comes with CDE is ideal for these pixmaps. When editing node icon pixmaps, keep the following points in mind:

- Define the bulk of the image using the symbolic colors Background, TopShadow, BottomShadow, and Select. The symbolic color Background is replaced by the appropriate color for the node's current state. TopShadow and BottomShadow are dynamically calculated based on the current Background color. The Select color is defined as a Network Viewer (ND) resource. Set any area of the image that should never be filled with any color to the symbolic color Transparent.

- Use TopShadow and BottomShadow symbolic colors to give your icon a 3D effect.
- Use Static Colors and Static Grays only to add details and accents to the image. Use them sparingly to prevent confusion with state colors.
- Keep the node pixmaps small to conserve screen real estate (20X20 is a good average size).
- If you create new node pixmaps (as opposed to editing existing filenames), be sure to update the ND resource file appropriately.

### Selecting the default view

You can set a default view that is restored automatically whenever Network Viewer is started. To do so, create the new default view in the standard directory (/opt/MagellanNMS/data/nvs/views) and name it DEFAULT\_VIEW. Alternatively, you can set the defaultViewName resource for Network Viewer to the full path name of the view description file to use as default. For more details, see the section on customizing the toolsets and start tools menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

### Modifying the Start Tool menus and icon bars

You can customize the Start Tool menus and icon bars. For details on the available Network Viewer Start Tool menus, see "Start Tool menus" on page 56.

For details on customizing the Start Tool menus and icon bars, see the section on customizing the toolsets and start tools menu in 241-6001-301 *Preside MDM Customization Administrator Guide*.

When you modify the Start Tools menu file, use one of the following substitution variables on the command line:

- \$COMP: the selected component ID in API format (for example, EM TORONTO LP 1 PO 1)
- \$COMP2: the second selected component ID in API format
- \$DCOMP: the selected component ID in display format (for example, EM/TORONTO LP/1 PO/1)
- \$DCOMP2: the second selected component ID in display format

- `$NMHOST`: the current host from the Server Selection tool
- `$DNAME`: the module name only from the selected component ID in display format
- `$DNAME2`: the module name only from the second selected component ID in display format
- `$SNAMES`: the module names only from the selected component IDs in API format
- `$SDNAMES`: the module names only from the selected component IDs in display format

## Customizing Network Viewer resources

The *Network Viewer* tool uses resources to describe certain functional and appearance aspects. You can customize some of these aspects. Others cannot be changed without affecting the functionality of Network Viewer.

	<p><b>CAUTION</b> <b>Risk of altering the functionality of Network Viewer</b> Do not modify resources that are not listed in the following table. Changing unlisted resources may negatively affect Network Viewer's appearance and functionality.</p>
---	--

The Network Viewer resource files are `/opt/MagellanNMS/lib/app-defaults/C/ND` and `/opt/MagellanNMS/lib/app-defaults/C/NDIcons`.

The table “Resources that you can customize in the Network Viewer” (page 104) lists the Network Viewer resources that you can customize. Note that the application classname of the Network Viewer applications is actually ND.

**Table 17**  
**Resources that you can customize in the Network Viewer**

Resource	Description	Legal values
ND*stateINVALID ND*stateUNKNOWN ND*stateINSV ND*stateINSV ND*stateSTB_1 ND*stateSTB_2 ND*stateSTB_3 ND*stateSTB_4 ND*stateSTB_5 ND*stateOOS_1 ND*stateOOS_2 ND*stateOOS_3 ND*stateOOS_4 ND*stateOOS_5 ND*stateMTCE ND*stateHIER_MTCE ND*stateACKED ND*stateModuleUNKNOWN	These resources specify the state-to-color mapping used to indicate the current state of components in ND.	Any X windows color name specification, for example, gray98. See <i>/usr/lib/X11/rgb.txt</i> for a list of X11 color names.
ND*differentModuleUnknownColor	If differentModuleUnknownColor is true, then the unknown color for the node at the module level is different from the default unknown color.	True or False
ND*nmsNodeStates*nvmColors ND*nmsNodeStates*xpmBgColor <n>	These resources specify the colors that represent the various node states. <n> ranges from zero to (numColors - 1). Each unique color needs to be defined in this list only once (even if the same color is used for more than one state).	
(Sheet 1 of 9)		

**Table 17 (continued)**  
**Resources that you can customize in the Network Viewer**

Resource	Description	Legal values
ND*nmsNodeStates*nvmImages ND*nmsNodeStates*xpm Image<n>	These resources specify all the unique XPM3 pixmaps that represent the various node types. <n> ranges from zero to (numImages -1). Each unique pixmap needs to be defined in this list only once (even if the same pixmap is used for more than one node type).	
ND*nmsLinkStates*nvmLinkColors ND*nmsLinkStates*linkColor<n>	These resources specify the colors that represent the various link states. <n> ranges from zero to (numLinkColors -1). Each unique color needs to be defined in this list only once (even if the same color is used for more than one state).	
ND*nmsLinkStates*nvmLinkStyles ND*nmsLinkStates*LinkStyleName<n> ND*nmsLinkStates*LinkStyleWidth<n> ND*nmsLinkStates*LinkStyleStyle<n> ND*nmsLinkStates*LinkStyleDashOffset<n> ND*nmsLinkStates*LinkStyleDashes<n>	These resources specify all the unique line styles that represent link types. <n> ranges from zero to (numLinkStyles -1). Each style needs to be defined only once. LinkStyleName is arbitrary. LinkStyleWidth can be any whole number. LinkStyleStyle must be zero for solid lines, and one or two for dashed lines. See X Window System graphics context documentation for explanations of LinkStyleDashOffset and LinkStyleDashes.	
(Sheet 2 of 9)		

**Table 17 (continued)**  
**Resources that you can customize in the Network Viewer**

Resource	Description	Legal values
ND*numNodeTypes ND*nodeName<n> ND*nodeTypeImageIndex<n>	These resources specify the mapping of node types to node images defined by the ND*nmsNodeStates*xpmlImage resources. <n> ranges from zero to (numNodeTypes - 1). The nodeName must match the node type string defined by the network model. The nodeTypeImageIndex specifies (by index) which image to use for this node type.	
ND*numStateNames ND*stateName<n> ND*stateColorIndex<n>	These resources specify the mapping of node state names to the colors defined by the ND*nmsNodeStates*xpmBgColor resources. <n> ranges from zero to (numStateNames - 1). The stateName strings must match the state names defined by the network model. The stateColorIndex values specify (by index) which color to use for this node state.	
ND*numLinkTypes ND*linkTypeName<n> ND*linkTypeStyleIndex<n>	These resources specify the mapping of link types to link styles defined by the ND*nmsLinkStates*linkStyle resources. <n> ranges from zero to (numLinkTypes - 1). The linkTypeName must match the link type string defined by the network model. The linkTypeStyleIndex specifies (by index) which line style to use for this link type.	
(Sheet 3 of 9)		

**Table 17 (continued)**  
**Resources that you can customize in the Network Viewer**

Resource	Description	Legal values
ND*numLinkStateName ND*linkStateName<n> ND*linkStateColorIndex<n>	These resources specify the mapping of link state names to the colors defined by the ND*nmsLinkStates*linkColor resources. <n> ranges from zero to (numLinkStateNames - 1). The linkStateName strings must match the state names defined by the network model. The linkStateColorIndex values specify (by index) which color to use for this link state.	
ND*nmsLinkStates*linkSelectColor	This resource specifies the color of the lines that bound a selected link to show that it is selected.	
ND*nmsLinkStates*linkSelectWidth	This resource specifies the width (in pixels) of the selection lines on either side of a selected link.	
ND*nmsLinkStates*solidSelectionLines	This boolean resource specifies whether or not the selection lines follow the style pattern of the link, or if they are always drawn as solid lines.	
ND*nmsNodeStates*selectColor	This resource specifies the color of the "halo" that surrounds selected nodes.	
ND*labelOffset	This integer resource specifies the distance (in pixels) from the bottom of a node icon to the top of its label.	
ND*labelFontList	This resource specifies the X Window System font to be used for node labels.	
(Sheet 4 of 9)		

**Table 17 (continued)**  
**Resources that you can customize in the Network Viewer**

Resource	Description	Legal values
ND*restrictClusterToSite	This resource indicates if Network Viewer needs to consider only connected nodes in the same parent Organizational Node when <i>Cluster Connected Nodes</i> is invoked on a node. This setting is now controlled by the Preferences Dialog.	False
ND*clusterModuleSpacing ND*clusterOrgNodeSpacing	These resources indicate the distance left between nodes when the Cluster Child Nodes or Cluster Connected Nodes commands are applied. For Cluster Connected Nodes, these values are implicitly majored by an increment based on the number of connected nodes. This setting is now controlled by the Preferences Dialog.	If the target node is a module, the value is 80. If the target node is an Organizational Node, the value is 250.
ND*drawAreaBackgroundColor	This resource specifies the color of the background when no map is assigned (for example, the background when the organization roots are being displayed)	Any X windows color name or numerical specification
ND*worldMinX ND*worldMinY ND*worldMaxX ND*worldMaxY	These resources specify the dimension of the network when no map is assigned. Any node lying outside this area is forced within to ensure that it is visible. This setting is now controlled by the Preferences Dialog.	X or Y coordinates in pixels
ND*rubberbandColor	This resource specifies the color of the selection rectangle and the rubber band when positioning links. If you modify the background colors, you may also need to change these colors to get a better contrast.	Any X windows color name or numerical specification
(Sheet 5 of 9)		

**Table 17 (continued)**  
**Resources that you can customize in the Network Viewer**

Resource	Description	Legal values
ND*linkSelectionSensitivity	These resources specify the number of pixels to either side of a link's drawn line. If the mouse is clicked inside this margin, the link is selected. When set to zero, links can only be selected when the mouse is directly over the line (which can be tricky when trying to select a diagonal line).	
ND*displacementInertia	These resources pacify the number of pixels a node or bendpoint needs to be displaced before Network Viewer considers the object as moved. This helps to prevent accidental moves when selecting nodes.	
ND*bendpointDimension	This resource specifies the width and height of the bendpoint handles in pixels.	
ND*labelForeground ND*labelBackground	These resources specify the color of the node and link labels. If you changed the background color, you may also need to change these colors to get a better contrast.	Any X windows color name or numerical specification
ND*autoManageOrgs ND*organizationName	If autoManageOrgs is True (default), Network Viewer automatically tries to open an organization when it starts (no default view is specified). If organizationName is specified (commented out by default), it can hold the name of the organization that it is opening. If not specified, Network Viewer opens the DEFAULT ALL view if it is the only one or it opens the non DEFAULT one if only two organizations exist.	True or False Organization name
(Sheet 6 of 9)		

**Table 17 (continued)**  
**Resources that you can customize in the Network Viewer**

Resource	Description	Legal values
ND*defaultViewName	If it is specified (commented out by default), this resource indicates the full path name of the view description file to restore automatically when Network Viewer starts.	A view description file full path name
ND.geometry	This resource specifies the default size of the Network Viewer window in terms of X geometry.	Standard X windows geometry specification
ND*mainWindow.width ND*mainWindow.height	These resources specify the default size of the Network Viewer window in terms of width and height (defaults to 750x649)	Width and height in pixels
ND*showAllLabels	If True, Network Viewer displays all node labels by default. Default is False. This setting is now controlled by the Preferences Dialog.	True or False
ND*reverseShelf	If True, displays DPN 100 shelf 0 at the bottom of the display. If False, displays DPN 100 shelf 0 at the top of the display.	True or False
ND*confirmExit	If True (default), Network Viewer prompts with a confirmation dialog when Exit is selected. If False, Network Viewer directly exits.	True or False
*fontList	If a fontList resource is added to Network Viewer's resource file, or your <i>Xdefaults</i> file (NV.*fontList) and the default font is set to "Default" in MSM's font menu, the specified font is used by Network Viewer (usually not specified).	Available font name
(Sheet 7 of 9)		

**Table 17 (continued)**  
**Resources that you can customize in the Network Viewer**

Resource	Description	Legal values
*multiClickTime	This resource specifies the maximum time (in milliseconds) between two consecutive mouse clicks to recognize a double click.	Time in milliseconds
ND*orgDbIclickAction ND*orgShiftDbIclickAction ND*orgMetaDbIclickAction . . .	These resources control what happens when you double-click on a node, a link, or a subcomponent in the Network Viewer tool while the Shift key is pressed, the Control key is pressed, the Meta key is pressed, or no key is pressed.	See the description in resource file Network Viewer.
ND*showIconBar	If True, the command icon bar is displayed in the main Network Viewer window. If False, the command icon bar is not displayed. This setting is now controlled by the Preferences Dialog.	True or False
ND*allowViewPositions	This resource indicates if Network Viewer displays the toggle button in the <i>Save</i> and <i>Restore view</i> dialogs, allowing you to save/restore the modified node/bendpoint positions to/from the view.	True or False
ND*preferViewPositions	This resource indicates if <i>view</i> positions are preferred. This results in the default value of the toggle button in the <i>Save</i> and <i>Restore view</i> dialogs. It also determines if positions should be restored when the default view is restored at startup and when a view is opened through the icon bar.	True or False
(Sheet 8 of 9)		

**Table 17 (continued)**  
**Resources that you can customize in the Network Viewer**

Resource	Description	Legal values
ND*gridOn	This resource indicates if the Positioning Grid is enabled by default. This setting is now controlled by the Preferences Dialog.	False
ND*gridWidth	This resource indicates the width of the Positioning Grid cells. This setting is now controlled by the Preferences Dialog.	80
ND*gridHeight	This resource indicates the height of the Positioning Grid cells. This setting is now controlled by the Preferences Dialog.	50

(Sheet 9 of 9)

## Customizing color and display attributes

Your Preside Multiservice Data Manager (MDM) system administrator can customize the following display attributes for you. See the section on customizing the toolsets and start tools menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

- color
  - state color mappings for nodes and links
  - background color when no maps are used
  - rubber band and label colors
- double-clicking actions
- initial size of Network Viewer display window
- view space dimensions (when no background maps are used)
- initial organization or named view
- initial component label display state
- double-click speed

- backbone definition and custom override definition for component filtering

## Troubleshooting

While Network Viewer is running, the network model may be edited either manually through the NetworkViewer in edit mode, or automatically. Network Viewer is informed of network model changes of the types listed in the table “Network model actions and results” (page 113) and updates its display.

**Table 18**  
**Network model actions and results**

Network model action	Network Viewer result
Link Deleted	If the link is currently displayed, it is removed from the display.
Node Deleted	If the node is currently displayed, it and any attached links are removed from the display.  If a Subcomponent or Shelf dialog is currently up for this node, they are removed.
Subcomponent Deleted	If the subcomponent is currently displayed in a shelf dialog, its state is set to INVALID. If the subcomponent is currently displayed in its parent node's subcomponent dialog, the component is removed from the dialog's component list.
Link Created	If both endpoints of the link are currently displayed, the link is added to the display. The link is drawn with any bendpoints that are defined for the link. (If either of the link's endpoints are not defined in Network Viewer, the link is ignored.)
Node Created	If the parent of the new node is currently expanded on the display, the node is added to the display.  If coordinates are defined, the node appears in the defined position; otherwise, it appears in the top left-hand corner of the Network Viewer display. If created manually, it appears with a <i>grid cyclic</i> policy.
(Sheet 1 of 3)	

**Table 18 (continued)**  
**Network model actions and results**

Network model action	Network Viewer result
Subcomponent Created	If the subcomponent has a shelf location and the shelf is currently displayed, the state display of the subcomponent changes from INVALID to the subcomponent's reported state. If the parent node's subcomponent dialog is currently displayed, the subcomponent is added to the dialog's component list.
Node Reassigned	If the node is currently displayed and the new parent is not currently expanded, the node is removed from the display. If the node is not currently displayed and the new parent is currently expanded, the node is displayed.
Model Locked	Network Viewer displays a <i>lock</i> icon indicating that no surveillance information is available until further notice.
Model Unlocked	If no submessage indicates the change that was made to the model while it was locked, Network Viewer removes the <i>lock</i> icon, indicating that surveillance information is now available.
	<p><b>New Model</b></p> <p>A new model is loaded into shared memory. Network Viewer displays a dialog indicating this, explaining that the Network Viewer display needs to be re-initialized from the network model. You may either confirm the reinitialization (Load new model) or terminate Network Viewer (Exit Application). If you confirm, Network Viewer clears the display and reinitializes its internal model. After initialization is complete, it displays the top level organization nodes of the new model.</p>
Model in Editing mode	Either this Network Viewer or another Network Viewer is used to edit the model. A caution icon is displayed at the right of the status label.
(Sheet 2 of 3)	

**Table 18 (continued)**  
**Network model actions and results**

<b>Network model action</b>	<b>Network Viewer result</b>
Node or bendpoint position changes	If a node or bendpoint position is changed by another Network Viewer in edit mode, the new positions are received, but are displayed only if the <i>Set Shared Model Positions for All Nodes and Links</i> , or the <i>Set Shared Model Positions for Selected Nodes and Links</i> command is invoked from the <i>View</i> menu.
CDF (Component Data File) loaded in the model	You can make these changes. Effects on the model are indicated in the changes described in this section.
PI or card type is changed	If the shelf dialog is up, the shelf is redisplayed to match the new information.
Module or shelf type changes	The node is destroyed and reconstructed to match the new type. If the shelf or subcomponent dialogs are up, they are brought down and need to be re-invoked manually.
(Sheet 3 of 3)	

If the connection to the network model is lost or the network model becomes inconsistent, a dialog is displayed to indicate this problem. It allows you to exit the Network Viewer application since the network model is crucial to its operation. Restarting the Network Viewer usually solves the problem; otherwise, contact your Preside Multiservice Data Manager (MDM) system administrator.



## Chapter 3

# Passport Shelf View

---

This section describes the Passport Shelf View tool and contains the following topics:

- “Overview” (page 117)
- “MDM state color conventions” (page 118)
- “Passport Shelf View window” (page 119)
- “Procedures” (page 134)
- “Errors and warnings” (page 172)

## Overview

Passport Shelf View is a Preside Multiservice Data Manager (MDM) tool that communicates directly with a Passport device to assist in troubleshooting network problems in real time. The Passport Shelf View window displays both physical and logical shelf views for Passport 6000, 7000, 15000, and 20000 multiservice switches; related component information; associated alarms; and sparing relationships for logical processors and cards. The tool also supports a selection of nodal surveillance and provisioning activities.

The Passport Shelf View tool uses the psvagent server to collect its required data. For details about this server, see the section on psvagent in 241-6001-310 *Preside MDM Server Reference Guide*.

For more details about Passport Shelf View, see the following topics:

- “MDM state color conventions” (page 118)

- “Passport Shelf View window” (page 119)
- “Procedures” (page 134)
- “Errors and warnings” (page 172)

## MDM state color conventions

The Passport Shelf View tool uses standard MDM color conventions to indicate the network model states of components. Provisioned components display with a background color. For a description of the colors and their meaning, see the table “MDM state color conventions” (page 118).

**Table 19**  
**MDM state color conventions**

If the background color is...	Then the component state is...	And its description is...
Green	INSV	In-service
Yellow/orange	ISTB	In-service—troubled
Red	OOS	Out-of-service
Grey	UNK	Unknown
Light Blue	MTCE	Maintenance
	HIER_MTCE	Hierarchical maintenance
Aqua	ACK	Acknowledged
No color	UNDEF	Undefined. The component has not been given a state by the Network Model Server.

Passport Shelf View displays alarms in tabular format. The entries in the alarm severity column display with colored backgrounds, with different colors representing different alarm severities. In addition, the column indicating raw state displays its text in color.

## Passport Shelf View window

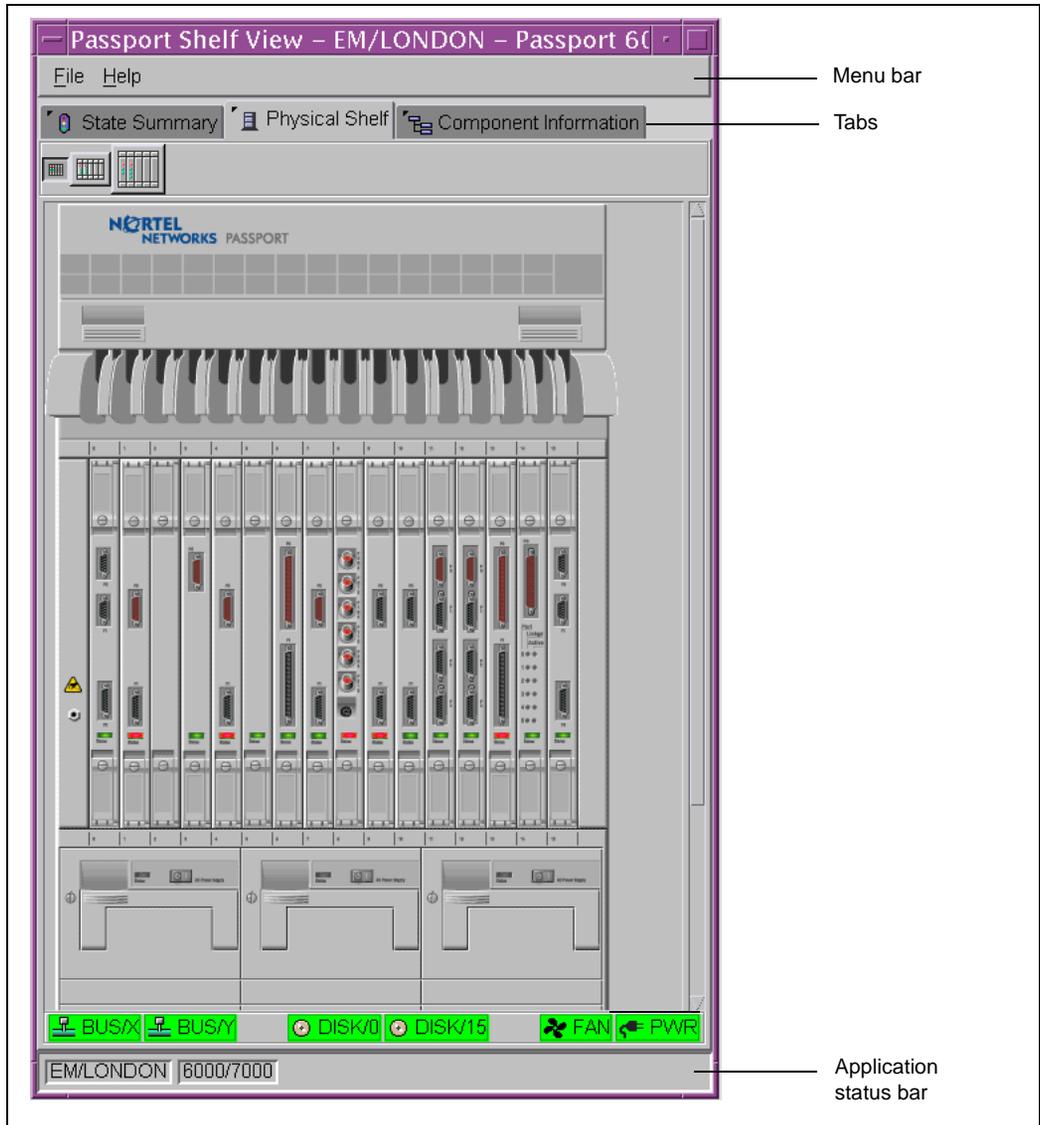
The Passport Shelf View tool provides consolidated MDM functionality in a single window. A selection of tabs lets you display the logical shelf, the physical shelf, and component information. You can also perform surveillance and provisioning activities from these tabbed pages.

The figure “Passport Shelf View” (page 120) shows a sample Passport Shelf View window with the Physical Shelf tab selected. The callouts in this figure indicate those elements that are common to all the tabbed pages.

The Passport Shelf View window contains the following items:

- “Menu bar” (page 121)
  - “File” (page 121)
  - “Help” (page 121)
- “State Summary” (page 121)
  - “Logical Processor Summary pane” (page 123)
  - “Processor Card Summary pane” (page 124)
  - “Supplementary component pane” (page 125)
- “Physical Shelf” (page 126)
  - “Card faceplates” (page 128)
  - “Supplementary component bar” (page 128)
- “Component Information” (page 129)
  - “Component Navigator pane” (page 131)
  - “Related component pane” (page 131)
  - “Component details pane” (page 132)
- “Application status bar” (page 133)

**Figure 9**  
**Passport Shelf View**



For more details about Passport Shelf View, see the following topics:

- “Overview” (page 117)

- “MDM state color conventions” (page 118)
- “Procedures” (page 134)
- “Errors and warnings” (page 172)

## Menu bar

The menu bar contains the following menus:

- “File” (page 121)
- “Help” (page 121)

## File

The File menu contains the following commands:

- **Exit** closes the window and exits the tool. See the procedure “Quitting Passport Shelf View” (page 142).

## Help

The Help menu contains the following commands:

- **On Context** displays information about a selected area of the Passport Shelf View window. See the procedure “Displaying Passport Shelf View online help” (page 143).
- **On Window** displays descriptive information about the Passport Shelf View window components. See the procedure “Displaying Passport Shelf View online help” (page 143).

## State Summary

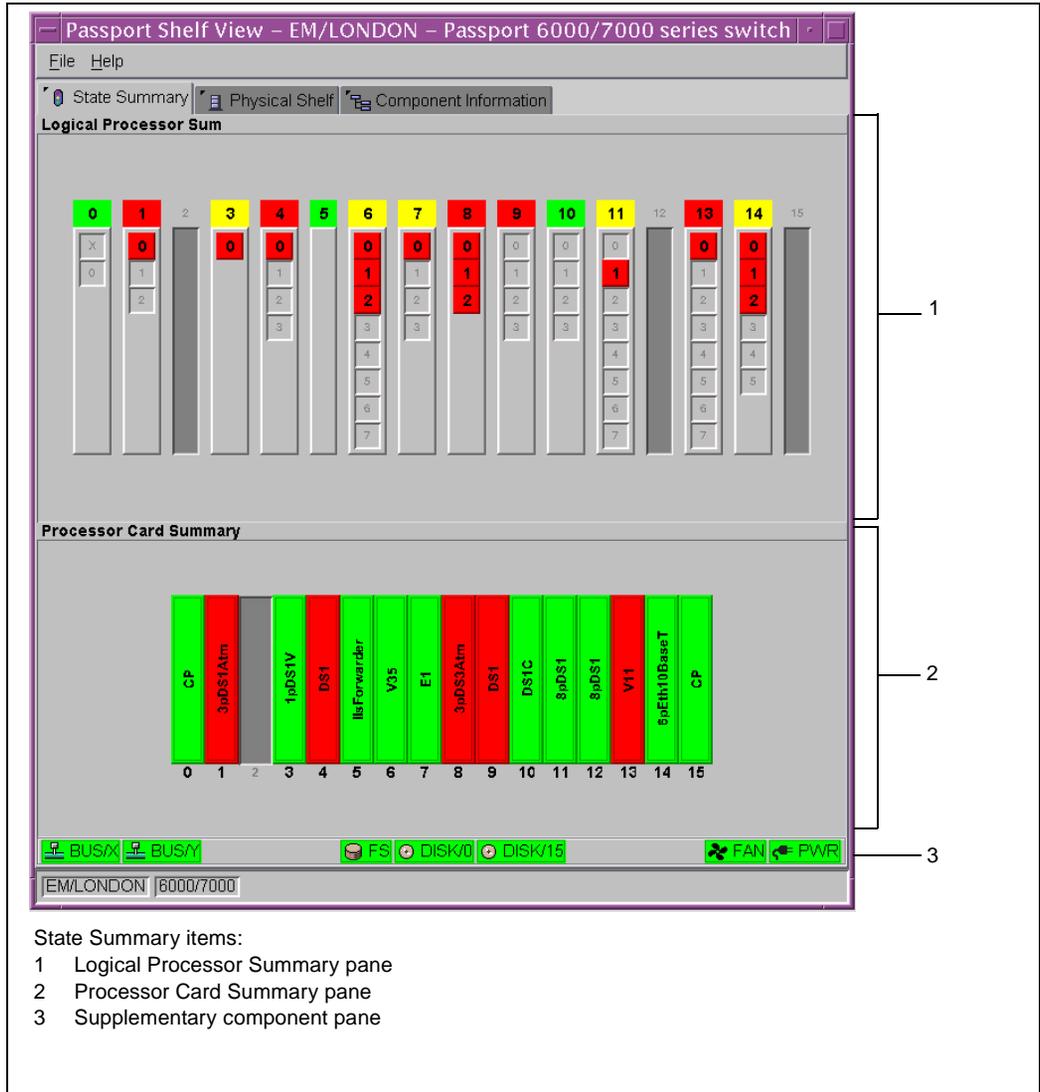
The State Summary tab displays summary state information for logical processors (LP) and cards. It also provides sparing information for logical processors and cards. The figure “Passport Shelf View: State Summary” (page 122) shows a sample Shelf View window with the State Summary tab selected.

The State Summary tab contains the following items:

- “Logical Processor Summary pane” (page 123)
- “Processor Card Summary pane” (page 124)

- “Supplementary component pane” (page 125)

**Figure 10**  
**Passport Shelf View: State Summary**



- State Summary items:
- 1 Logical Processor Summary pane
  - 2 Processor Card Summary pane
  - 3 Supplementary component pane

## Logical Processor Summary pane

The Logical Processor Summary pane provides information about the architecture for logical processors (LP) and their associated ports. This pane also provides sparing relationships, port to physical connector mappings, and access to LP subcomponent information.

### LP graphical representation

The Logical Processor Summary pane displays 16 LP slots (0 to 15) and their ports. For Passport Shelf View, an LP slot refers to the graphical representation of the collection of logical ports associated with an LP, not the physical card cage slots in the Passport. Ports display in columns of eight. If an LP has more than eight ports, multiple columns display. The number of logical port buttons in a slot depends on the LP's associated card type.

LPs and ports that are not provisioned appear recessed; provisioned LPs and ports appear raised. If a port is predefined as not being able to be provisioned, then that port is labelled with a X rather than a port instance number. Ports for Passport 6000 and 7000 series display in ascending order; ports for Passport 15000 and 20000 series display in descending order.

### LP to connector mapping

To help map logical ports to the physical connectors of the card faceplate, when you select a port in the LP Summary pane, the physical connector associated with that port is highlighted in the physical view.

### Subcomponent information

To view the subcomponents of any component on the Logical Processor Summary pane, double-click on that component. The Component Information tab opens with selected component at the top level of the Component Navigator pane and, if applicable, all subcomponents underneath.

### Sparing relationships

When you select a component in the Logical Processor Summary pane, any provisioned sparing relationship for that object automatically displays. For a list of sparing types, see the table "Shelf View supported sparing types" (page 124).

**Table 20**  
**Shelf View supported sparing types**

Sparing type	View from	Indicators
LP/CARD (logical processor/card)	State Summary and Physical Shelf tabbed pages.	When you select an LP or port, the associated main and spare cards display with colored borders. A magenta border surrounds the main card; a grey border surrounds the spare card.
LAPS/APS (line automatic protection switching/automatic protection switching)	State Summary - Logical Processor Summary pane	A dashed line connects the spared ports. <b>W</b> indicates the working line end, <b>P</b> indicates the protection line end, and <b>A</b> indicates the currently active end.
DLEP	State Summary - Logical Processor Summary pane	A dashed line connects the spared ports. <b>M</b> indicates the main LP end, <b>S</b> indicates the spare LP end, and <b>A</b> indicates the currently active end.
PBG (port bridge group)	State Summary - Logical Processor Summary pane	A dashed line connects the spared ports. <b>W</b> indicates the working line end, <b>B</b> indicates the bridge end.

## Processor Card Summary pane

The Processor Card Summary pane identifies the inserted card types and card layout used for the Passport device. Passport Shelf View supports all Passport cards types, except those for wireless. For a list of supported cards, see the section on shelf card components in 241-5701-060 *Passport 7400, 15000, 20000 Components*.

In the Processor Card Summary pane, card slots with inserted cards appear raised and empty card slots appear recessed. If a card is provisioned, its card slot displays with an etched border.

The Processor Card Summary pane indicates LP-CARD sparing. When you select an LP or port in the Logical Processor Summary pane, the associated main and spare cards display with colored borders in the Processor Card Summary pane. A thick magenta border surrounds the main card; a thin grey border surrounds the spare card. Conversely, when you select a card in the

Processor Card Summary pane, all LPs configured to use that card as the main card have a thick magenta border; all LPs configured to use the card as a spare have a thin grey border.

To view the subcomponents of any component on the Processor Card Summary pane, double-click on that component. The Component Information tab opens with selected component at the top level of the Component Navigator pane and, if applicable, all subcomponents underneath.

## Supplementary component pane

The supplementary component pane provides information about the following additional Passport components:

- BUS/X and BUS/Y (for Passport 6000 and 7000 series) or FABRICCARD/X and FACRICCARD/Y (for Passport 15000 and 20000 series)
- FS (File System)
- DISK/0
- DISK/1 if configured (for Passport 15000 and 20000 series)
- DISK/15 if configured (16-slot Passport 6000 and 7000 series)
- FAN
- PWR (power supply)

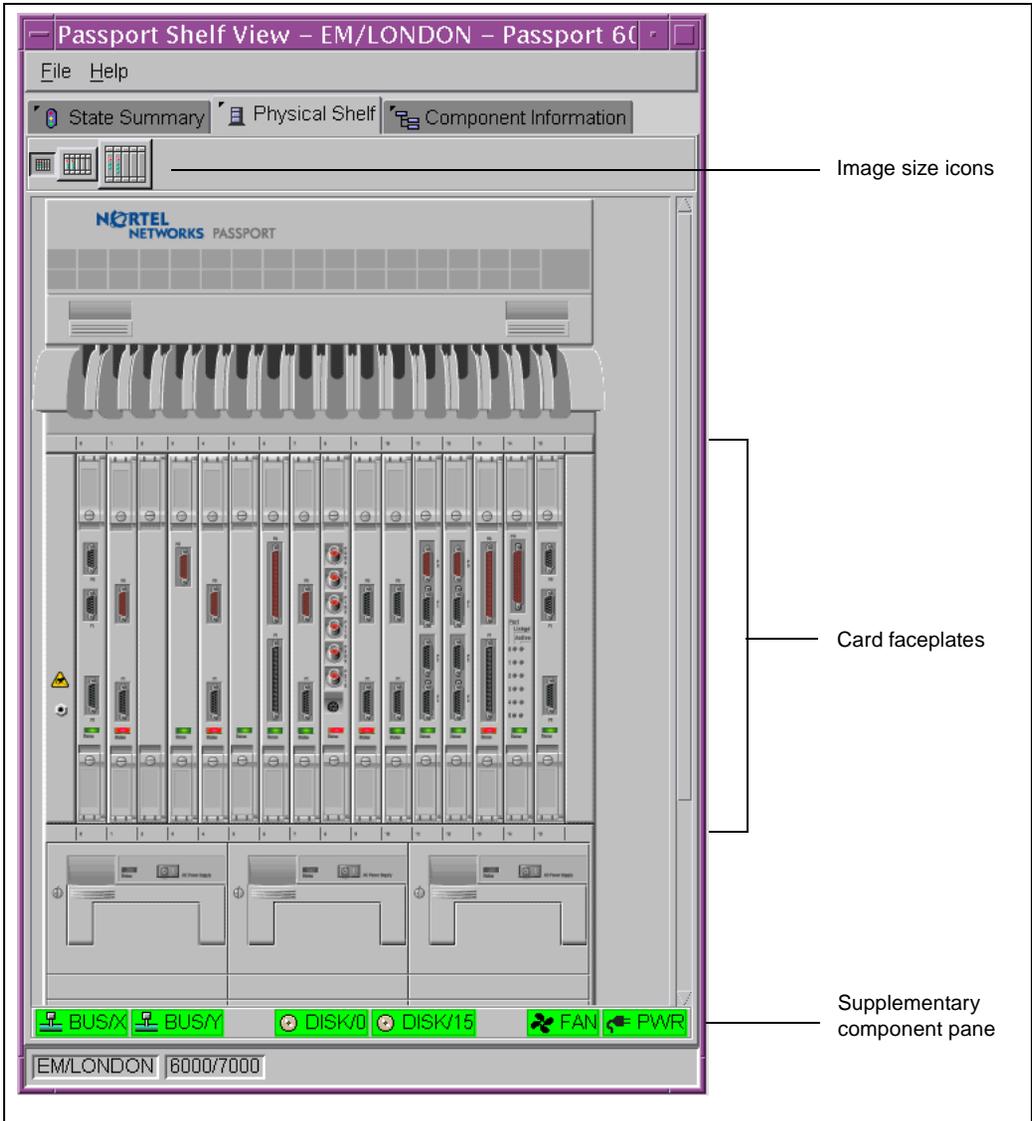
To view subcomponents of the BUS, FACRICCARD, FS, or DISK, double-click on any of these components. The Component Information tab opens with the selected component at the top level of the Component Navigator pane and, if applicable, all subcomponents underneath.

The FAN and PWR components are not MDM modelled component types. The states for these components are simulated by monitoring the Passport device for specific alarms and are presented in the Passport Shelf View window to further assist in fault detection.

## Physical Shelf

The Physical Shelf view represents the Passport device as it is currently equipped, including components that are present but not yet active. This view includes the shelf, card cages, card faceplates, frames and other hardware of the selected Passport device. Entire Passport 15000 and 20000 series frames do not display because the Passport Shelf View tool cannot determine whether a shelf is mounted in the upper or lower half of the frame. For this reason, a small separation appears between the breaker interface panel (BIP) and the shelf in the Physical Shelf view. The figure “Passport Shelf View: Physical Shelf” (page 127) shows a sample Passport Shelf View window with the Physical Shelf tab selected. You can use the image size icons to increase or decrease the shelf view display. See “Adjusting the image size of the Physical Shelf” (page 147).

**Figure 11**  
**Passport Shelf View: Physical Shelf**



The Passport Shelf View window automatically refreshes to capture changes to components or states as they occur. The color of the card LED in the Passport Shelf View reflects the state of the card as assigned by MDM network model, not the actual physical LED. As a result, in some instances the derived Passport Shelf View LED color may differ from the actual LED.

To assist in troubleshooting, when you select a port in the Logical Processor Summary pane, the physical connector associated with that port is highlighted in the Physical Shelf pane.

When you select a card in the Physical Shelf tab, its associated LPs display with colored borders in the State Summary tab. LPs associated with a main card have a thick magenta border; LP's associated with the spare card have a thin grey border.

The Physical Shelf tab consists of the following components:

- “Card faceplates” (page 128)
- “Supplementary component bar” (page 128)

## Card faceplates

In the physical view, only the cards represent modelled Passport components. Connectors may map to multiple connectors, each according to its card type. Cards, card LEDs, and port connectors are the only interactive portions of the physical view. The color of the LEDs on the faceplates indicate the state of the card. The color overlay on the physical connectors is in accordance with MDM state hierarchical propagation rules and represent a composite of the states of all the logical ports that map to the connector.

## Supplementary component bar

The supplementary component bar provides MDM state information for some additional components. This bar includes states for the following Passport components:

- BUS/X and BUS/Y (for Passport 6000 and 7000 series) or FABRICCARD/X and FACRICCARD/Y (for Passport 15000 and 20000 series)
- DISK/0
- DISK/1 if configured (for Passport 15000 and 20000 series)

- DISK/15 if configured (16-slot Passport 6000 and 7000 series)
- FAN
- PWR (power supply)

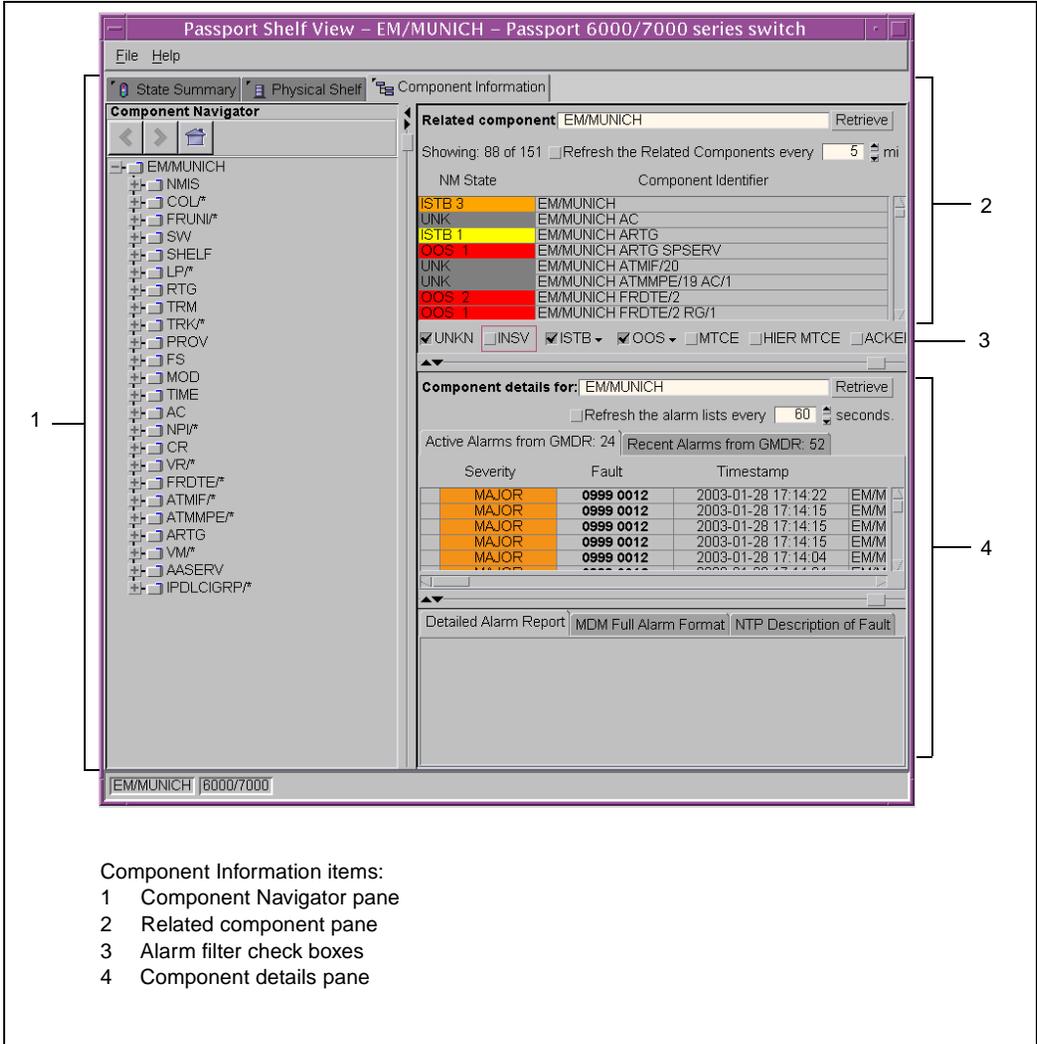
The FAN and PWR components are not MDM modelled component types. The states for these components are simulated by monitoring the Passport device for specific alarms and are presented in the Passport Shelf View window to further assist in fault detection.

## Component Information

The Component Information view lets you navigate the component tree structure, display related component information, and view component alarms.

The figure “Passport Shelf View: Component Information” (page 130) shows a sample Shelf View window with the Component Information tab selected.

**Figure 12**  
**Passport Shelf View: Component Information**



- Component Information items:
- 1 Component Navigator pane
  - 2 Related component pane
  - 3 Alarm filter check boxes
  - 4 Component details pane

The Component Information tab contains the following items:

- “Component Navigator pane” (page 131)
- “Related component pane” (page 131)

- “Component details pane” (page 132)

## Component Navigator pane

The Component Navigator pane represents the hierarchical component structure of the Passport device. From this pane, you can navigate down the component tree structure. You can also navigate across the component tree structure using links. For navigation procedures, see “Navigating the Passport component tree structure” (page 150). In addition, you can select a component for populating the Related component pane and Component details pane.

Provisioning activities are made possible from the Passport Shelf View by an embedded interface to the key elements of the Nodal Provisioning application. This embedded interface is called Embedded Nodal Provisioning. Embedded Nodal Provisioning lets you create, modify, and delete components and apply service templates to the current view. Embedded Nodal Provisioning only supports a subset of changes to a small number of components in the current active Passport view. To navigate and provision large numbers of Passport components in a variety of Passport views, you need to use the Nodal Provisioning tool. For a description of Embedded Nodal Provisioning and how to use it, see the Embedded Nodal Provisioning section in 241-6001-023 *Preside MDM Configuration Management for Passport User Guide*. For details about the Nodal Provisioning, see 241-6001-610 *Preside MDM Nodal Provisioning User Guide*.

## Related component pane

The related component pane displays parents, children, and related links of a selected component. Each entry in the list displays with a background color to indicate the state value. For details about colors and their associated states, see the table “MDM state color conventions” (page 118).

The list also displays component states and full component IDs. Components with a state of in-service—troubled (ISTB) or out-of-service (OOS) display with an MDM network model component criticality factor, ranging from a low of 1 to a high of 5. You can control whether or not the related component list refreshes and the frequency of refreshes. You can also sort the list so that it is organized by severity of network model state or by component identifier.

The Related component pane supports filtering so that you can limit the amount of information that displays in the list. A selection of check boxes in this pane lets you filter components based on the network model (NM) state.

This pane also displays the total number of related components in the list. When you select any of the filter check boxes, the pane displays both the number of items in the filtered list and the total number of related components.

To change the value in the Related component field, double-click on a component in the list. The list refreshes the display of related components for the selected component. As well, the Component details pane refreshes its display with information about the selected component.

### **Component details pane**

The Component details pane provides alarm information for a specific Passport component. It provides both an active and recent alarms list. The tab labels for these alarm types indicates the number of alarms in its list. The Active Alarms tab displays only uncleared SET alarms. The Recent Alarms tab shows all alarms in the GMDR buffer, including SET and CLEAR, for the selected component and its subcomponents.

Both active and recent alarms display all alarm record fields in tabular format. A horizontal scroll bar lets you view all fields in the window. By default, the alarm tables are sorted by the order in which they are received by GMDR. However, you can sort the table based on other columns. You can also control whether or not the alarms refresh and the frequency of refreshes.

The alarm details display in a series of tabbed panes. Clicking an alarm in the alarm list populates the alarm details pane. In the details pane, both the alarm code and component ID are hypertext links. Clicking the alarm code in the Detailed Alarm Report tab displays NTP Description of Fault tab which contains the alarm help information. Clicking the component ID in the Detailed Alarm Report refocuses the Component Details pane on that component ID.

## Application status bar

The application status bar is common to all application views and provides information about the status of the application as a whole. The following information is available from the application status bar:

- the name of the Passport node
- the type of Passport device including
  - 6000/7000 (for all 6000 and 7000 series Passport devices)
  - 15000 (for Passport 15000 only)
  - 20000 (for Passport 20000 only)

## Procedures

The Passport Shelf View tool lets you monitor, diagnose, and correct network faults. The tool monitors the Passport and returns component state values. Based on these state values, you can further diagnose problems and take corrective action. This section contains the following Passport Shelf View procedures:

### **Starting and stopping the Passport Shelf View tool**

- “Starting Passport Shelf View from the MDM toolset” (page 136)
- “Starting Passport Shelf View from the UNIX command line” (page 138)
- “Starting Passport Shelf View from other MDM tools” (page 140)
- “Quitting Passport Shelf View” (page 142)

### **Displaying online help**

- “Displaying Passport Shelf View online help” (page 143)

### **Modifying the Passport Shelf View window**

- “Moving tabbed pages onto the desktop” (page 144)
- “Displaying tool tips” (page 145)
- “Opening pop-up menus” (page 146)
- “Adjusting the image size of the Physical Shelf” (page 147)
- “Adjusting pane sizes” (page 148)
- “Adjusting column widths” (page 149)

### **Working with components**

- “Navigating the Passport component tree structure” (page 150)
- “Setting the maintenance state for a component” (page 152)
- “Locking a logical port” (page 153)
- “Unlocking a logical port” (page 154)

**Working with related components**

- “Displaying related components” (page 155)
- “Sorting related components” (page 156)
- “Setting filters for related components” (page 157)
- “Setting an automatic refresh interval for related components” (page 158)
- “Displaying component attributes” (page 159)

**Working with alarms**

- “Displaying alarms” (page 160)
- “Sorting alarms” (page 161)
- “Setting an automatic refresh interval for alarms” (page 162)
- “Acknowledging an alarm” (page 163)
- “Acknowledging all active alarms on a component” (page 164)
- “Unacknowledging an alarm” (page 165)
- “Unacknowledging all active alarms on a component” (page 166)
- “Clearing local alarms” (page 167)
- “Clearing global alarms” (page 168)

**Making provisioning changes**

- “Making provisioning changes to components and services” (page 169)

**Starting other MDM tools**

- “Starting other MDM tools from Passport Shelf View” (page 170)

## Starting Passport Shelf View from the MDM toolset

Using Passport Shelf View, you can display Passport physical and logical views to perform a selection of surveillance and nodal provisioning tasks.

### Prerequisite

Before you can start the Passport Shelf View tool, you need to authenticate to a Passport or Passport group. If you have not already authenticated during your current MDM session and try to start Passport Shelf View, a Connection Management dialog automatically opens and prompts for authentication information.

### Procedure steps

- 1 In the Preside Multiservice Data Manager window, select **Fault** and then **Passport Shelf View**.

If you have already authenticated, the **Passport Shelf View** window opens and you have completed the procedure.

If you have not already authenticated, the **Passport Shelf View Authentication** dialog box opens. You need to complete the remaining steps in the **Passport Shelf View Authentication** dialog box to start Passport Shelf View.

- 2 In the **Destination** list, select a destination.

All Passports in the selected destination group display in the **Passports** list.

- 3 In the **Passports** list, select the Passport to which you want to authenticate.

- 4 If the destination group is currently connected, go to step 6. If the destination group is currently disconnected, then complete the following steps:

- In the **User Id** field, type a valid user ID.
- In the **Password** field, type the password associated with the specified user ID.

- 5 Click **Connect**.

The status of the selected destination changes to connected and the **Select** button is enabled.

- 6 If required, in the **Destination** list, select a destination.

- 7 Select a Passport to which you want to connect using one of the following methods. In the **Passports** list
  - double-click a Passport
  - select an entry and then click **Select**

The **Passport Shelf View Authentication** dialog box closes and the **Passport Shelf View** window opens.

## Starting Passport Shelf View from the UNIX command line

Using Passport Shelf View, you can display Passport physical and logical views to perform a selection of surveillance and nodal provisioning tasks.

### Prerequisite

Before you can start the Passport Shelf View tool, you need to authenticate to a Passport or Passport group. If you have not already authenticated during your current MDM session and try to start Passport Shelf View, a Connection Management dialog automatically opens and prompts for authentication information.

### Procedure steps

- 1 From the UNIX command line, type the following command:

```
/opt/MagellanNMS/bin/shelfview
```

If you have already authenticated, the **Passport Shelf View** window opens and you have completed the procedure.

If you have not already authenticated, the **Passport Shelf View Authentication** dialog box opens. You need to complete the remaining steps in the **Passport Shelf View Authentication** dialog box to start Passport Shelf View.

- 2 In the **Destination** list, select a destination.

All Passports in the selected destination group display in the **Passports** list.

- 3 In the **Passports** list, select the Passport to which you want to authenticate.

- 4 If the destination group is currently connected, go to step 6.  
If the destination group is currently disconnected, then complete the following steps:

- In the **User Id** field, type a valid user ID.
- In the **Password** field, type the password associated with the specified user ID.

- 5 Click **Connect**.

The status of the selected destination changes to connected and the **Select** button is enabled.

- 6 If required, in the **Destination** list, select a destination.

- 7 Select a Passport to which you want to connect using one of the following methods. In the **Passports** list
  - double-click a Passport
  - select an entry and then click **Select**

The **Passport Shelf View Authentication** dialog box closes and the **Passport Shelf View** window opens.

## Starting Passport Shelf View from other MDM tools

Using Passport Shelf View you can display Passport physical and logical views and to perform a selection of surveillance and nodal provisioning tasks. You can start the Passport Shelf View tool from other MDM tools by using component context or by using the MDM Start Tool menu.

### Procedure steps

- 1 If you are using component context, use the following steps:
  - a. From any Preside MDM tool that supports context, select a Passport to put it into context. Generally, selecting a component puts that component into context. Some MDM tools may support a component popup menu that contains a **Put Context** command.
  - b. In the Preside Multiservice Data Manager window, select **Fault** and then **Passport Shelf View**.
- 2 If you are using the Start Tool menu, use the following steps:
  - a. From any MDM tool that supports a Start Tool menu, open the Start Tool menu. Generally, this step is done by right-clicking on a component to open a pop-up menu.
  - b. On the **Start Tool** pop-up menu, point to **Fault** and then select **Passport Shelf View**.
- 3 If you have already authenticated, the **Passport Shelf View** window opens and you have completed the procedure.

If you have not already authenticated, the **Passport Shelf View Authentication** dialog box opens. You need to complete the remaining steps in the **Passport Shelf View Authentication** dialog box to start **Passport Shelf View**.

- 4 In the **Destination** list, select the group destination for the Passport in context. If you select a group destination that does not contain the Passport in context, no entries display in the **Passports** list.
- 5 In the **Passports** list, select the Passport in context.
- 6 If the destination group is currently connected, go to step 8.  
If the destination group is currently disconnected, then complete the following steps:
  - In the **User Id** field, type a valid user ID.
  - In the **Password** field, type the password associated with the specified user ID.

**7** Click **Connect**.

The status of the selected destination changes to connected and the **Select** button is enabled.

**8** If required, in the **Destination** list, select a destination.**9** Select the Passport to which you want to connect using one of the following methods. In the **Passports** list

- double-click a Passport
- select an entry and then click **Select**

The **Passport Shelf View Authentication** dialog box closes and the **Passport Shelf View** window opens.

## Quitting Passport Shelf View

Use this procedure to quit the Passport Shelf View tool.

### Procedure steps

- 1 From the **File** menu, select **Exit**

The **Passport Shelf View** window closes.

## Displaying Passport Shelf View online help

Use this procedure to view online help for the Passport Shelf View tool. You can display various types of online help.

### Prerequisite

To request context help for a tabbed page, you need to select the tabbed page first and then request help on context. Otherwise, the help information is not refreshed in the browser window.

### Procedure steps

#### Help On Context

Help on Context displays online information about a specific area of the Passport Shelf View window.

- 1 From the **Help** menu, select **On Context**.

The mouse pointer changes to a question mark (?).

- 2 Move the mouse pointer onto an area of the window for which you want help and click the mouse button.

The online help window opens with information specific to the area you selected.

#### Help on Window

Help on Window provides a description of the elements of the Passport Shelf View window.

- 1 From the **Help** menu, select **Help on Window**.

The online help window opens with a description of the Passport Shelf View window.

## Moving tabbed pages onto the desktop

When you start Passport Shelf View, by default, the window opens with the State Summary tab selected. Clicking on the other tabs lets you view the information one tabbed page at a time. You can move a tabbed page from the Passport Shelf View window to its own subwindow on the desktop. Use this procedure to drag a tabbed page onto the desktop.

### Prerequisite

Tabs that you can move onto the desktop have a small black triangle in the upper left corner of the tab label.

### Procedure steps

- 1 Position the mouse pointer on the label of the tab you want to move to the desktop and drag it off the Passport Shelf View window.  
  
The tabbed page moves from the Passport Shelf View window to its own desktop subwindow.
- 2 To return the tabbed page back to the Passport Shelf View window, close the desktop subwindow.

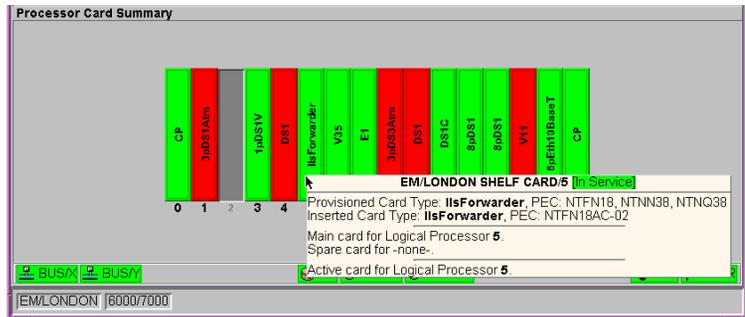
## Displaying tool tips

The Passport Shelf View tool supports tool tips. Tool tips are pop-up text boxes that provide additional information. The contents of the tool tip depends on the mouse pointer location. Tool tips provide such information as full component ID and sparing scenarios for logical processors and cards. Use the following procedure to display tool tips.

### Procedure steps

- 1 Move the mouse pointer over a provisioned component for a few seconds.

The tool tip for that component opens. The following figure shows a sample card tool tip.



## Opening pop-up menus

Pop-up menus are visible when you right-click on components in the Passport Shelf View window. These pop-up menus provide additional commands that are specific to the selected area of the window. Use this procedure to open a pop-up menu.

### Procedure steps

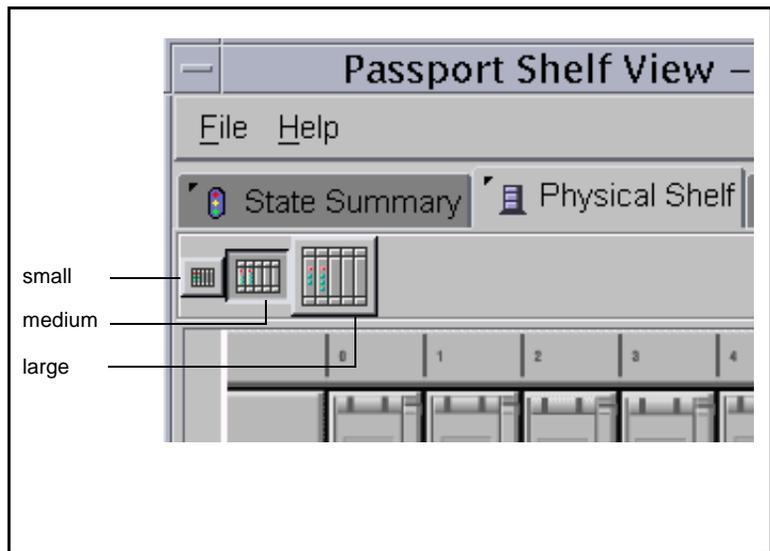
- 1 Right-click on any provisioned (colored) component in any of the tabbed pages.  
A pop-up menu opens.
- 2 Select a command from the pop-up menu.  
The command executes and the pop-up menu closes.

## Adjusting the image size of the Physical Shelf

The Physical Shelf supports three image sizes: small, medium, and large. When the Passport Shelf View tool opens, the Physical Shelf uses the medium image as its default. Use this procedure to change the physical shelf size image.

### Procedure steps

- 1 Click the **Physical Shelf** tab to select it.
- 2 Click one of the small, medium, or large image size icons.



The Physical Shelf increases or decreases in size, depending on your selection.

## Adjusting pane sizes

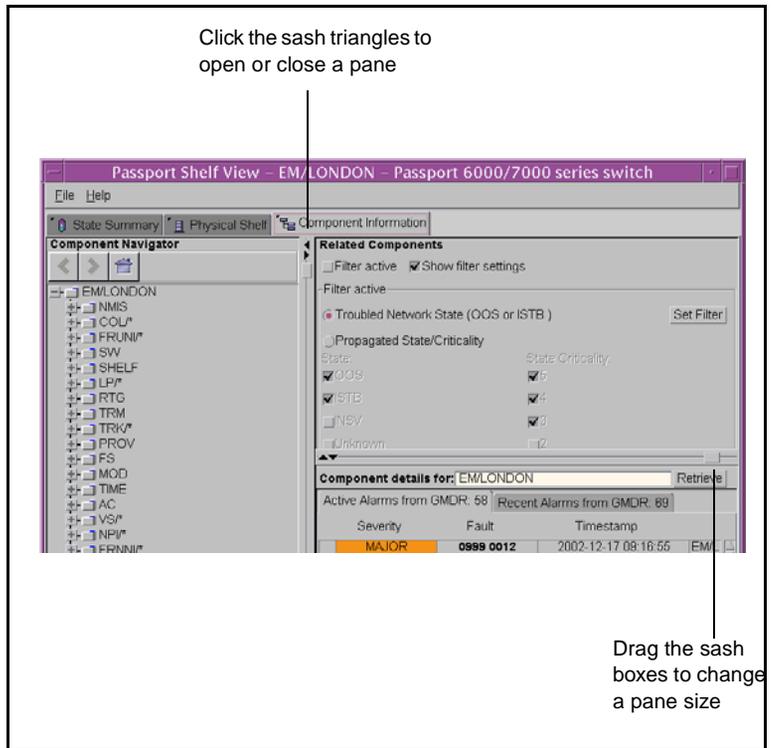
The Component Information tab contains various panes. You can adjust these pane sizes. Any adjustments that you make remain in effect until you readjust the settings or until you close the window. Use this procedure to adjust the sizes of these panes

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 To adjust the height or width of a pane, drag the box in the sash to the desired location.

When you move a sash to increase the amount of space in one pane, the space for the other panes decreases correspondingly.

- 3 To open or close a pane, click the triangles in the sash.

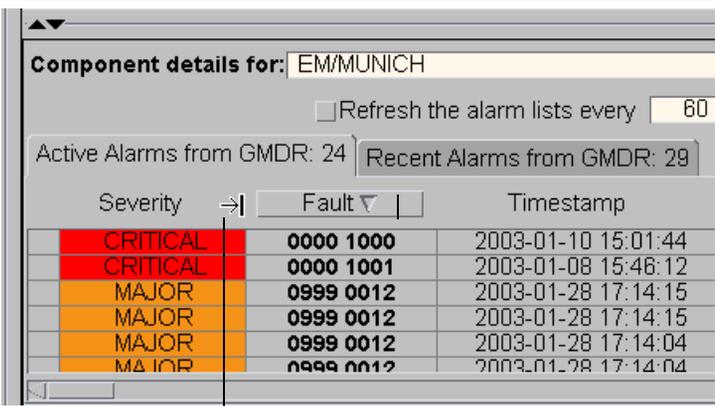


## Adjusting column widths

The Component Information tab displays alarm information in tabular format. You can change the default column width in the alarm table. Use this procedure to resize columns.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 In the **Component Details** pane, drag the boundary on the right side of the column heading until the column is the size you want.



The screenshot shows the 'Component details for: EM/MUNICH' pane. It includes a 'Refresh the alarm lists every' checkbox set to 60 seconds. Below are two tabs: 'Active Alarms from GMDR: 24' and 'Recent Alarms from GMDR: 29'. The active tab displays a table with the following data:

Severity	Fault	Timestamp
CRITICAL	0000 1000	2003-01-10 15:01:44
CRITICAL	0000 1001	2003-01-08 15:46:12
MAJOR	0999 0012	2003-01-28 17:14:15
MAJOR	0999 0012	2003-01-28 17:14:15
MAJOR	0999 0012	2003-01-28 17:14:04
MAJOR	0999 0012	2003-01-28 17:14:04

When you move the mouse pointer to the boundary of the column heading, the pointer changes to a right-pointing arrow and the header boundary displays.

## Navigating the Passport component tree structure

The Component Navigator pane in the Component Information tab represents the hierarchical component structure of the Passport device. You can navigate down the component tree to explore the component architecture. You can also navigate across the logical Passport component branches through links to explore relationships between components. Use this procedure to navigate the component tree structure.

### Procedure steps

- 1 Click the **Component Information** tab to select it.

Initially, all first level components in the **Component Navigator** pane display with a plus (+) sign in the folder icon, whether or not there are subcomponents. If you try to expand a first-level component that has no subcomponents, the component remains in the list but the folder and plus sign are removed.

- 2 To expand a component in the **Component Navigator** pane, click on the plus sign (+) adjacent to the component you want to expand.

When the component expands, the plus sign changes to a minus sign (-). Expanding a component in the tree requires communication with the Passport device. A short delay may be incurred during such expansion operations.

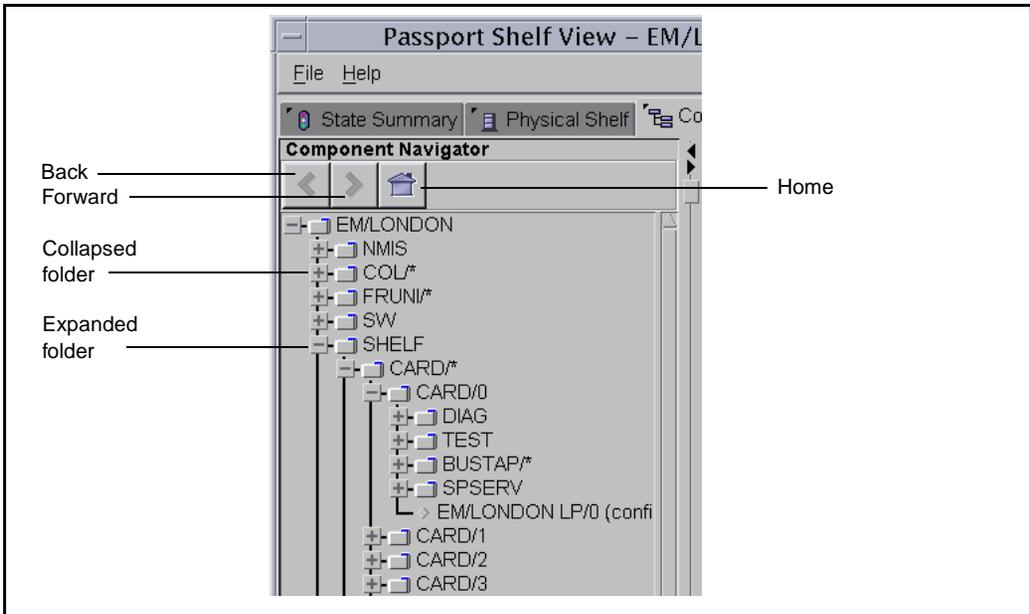
- 3 To compress subcomponents, click the minus sign (-) adjacent to the parent component.

- 4 To navigate across the component tree, you need to use links. In the Component Navigator, links are colored blue. Move the mouse pointer over the link until the pointer changes to the figure of a hand and then click.

The Component Navigator pane refreshes with the linked component at the top level of the component hierarchy.

- 5 To return the node to the top level of the component hierarchy, click the Home button.

- To move forward or backward through the link history, click the back and forward buttons.



## Setting the maintenance state for a component

Use this procedure to set the maintenance state for a component on or off. Setting the maintenance state permanently hides the current troubled state of a component. Any children of the selected component are also put into maintenance state. For more information on maintenance state, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

### Procedure steps

- 1 To set the maintenance state, right-click on a provisioned component and then from the resulting pop-up menu, select either **Set Maintenance State On** or **Set Maintenance State Off**.

When maintenance state is on, the selected component has a blue background. When maintenance state is off, the selected component displays a color that reflects its current MDM state.

## Locking a logical port

Locking an LP prevents it from providing services. When an LP is in the process of locking, its OSI administration state (`adminState`) changes to shutting down. In this state, the component continues to provide services to existing clients but does not accept any new requests for services. When the lock process completes, the `adminState` changes to `locked` and the LP no longer provides any services.

### Prerequisite

When Shelf View opens, you need to authenticate to a Passport group. If you want to use the lock and unlock commands, you need to authenticate with a user ID that has the following administration capabilities:

- `impact = service`
- `scope = network`
- `customer ID = 0`

### Procedure steps

- 1 Use one of the following steps on an unlocked LP:
  - On the **State Summary** tabbed page, right-click on an LP to open its pop-up menu.
  - On the **Physical Shelf** tabbed page, right-click on a connector to list the associated LPs and then select an LP from the list to open the pop-up menu.
- 2 On the pop-up menu, select **Fault** and then **Lock**.  
The **Confirm Lock Request** dialog opens and prompts for confirmation.
- 3 On the **Confirm Lock Request** dialog, select one of the following options:
  - **Lock** to lock the LP
  - **Lock -force** to immediately lock a component and skip the shutting down state
  - **Cancel** closes the dialog

Passport Shelf View replaces the LP instance in the LP Summary with a padlock icon for locked ports and a downward arrow for LPs that are shutting down. These icons also display in the LP label, menu, and tooltip.

## Unlocking a logical port

Unlocking a currently locked LP allows it to provide services. Unlocking an LP changes its administration state (adminState) to unlocked.

### Prerequisite

When Shelf View opens, you need to authenticate to a Passport group. If you want to use the lock and unlock commands, you need to authenticate with a user ID that has the following administration capabilities:

- impact = service
- scope = network
- customer ID = 0

### Procedure steps

- 1 Use one of the following steps on an LP that is locked or shutting down:
  - On the **State Summary** tabbed page, right-click on an LP to open its pop-up menu.
  - On the **Physical Shelf** tabbed page, right-click on a connector to list the associated LPs and then select an LP from the list to open the pop-up menu.
- 2 On the pop-up menu, select **Fault** and then **Unlock**.

The **Confirm Unlock Request** dialog opens and prompts for confirmation.

- 3 On the **Confirm Lock Request** dialog, click OK.

Passport Shelf View replaces the locked or shutting down icon with the LP instance in the LP Summary. These icons are also removed from the LP label, menu, and tooltip.

## Displaying related components

Use this procedure to populate the related component list or to refresh the contents with related information for another component.

### Procedure Steps

- 1 Click the **Component Information** tab to select it.
- 2 Use one of the following methods to populate or modify the **Related Component** pane:
  - In the **Related Components** pane, type the application's node name or any of its subcomponents in the **Related components for** field.
  - In the **Component Navigator**, right-click on a component and from the resulting popup menu, select the **Show Related Components** command.
- 3 Click **Retrieve**.

The Related Components List refreshes with related component information.

## Sorting related components

The related component pane displays related component information in tabular format. By default, the table sorts the related components by their component identifier. Use this procedure to change the sort order.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 To sort the table on a specific column, click its column header.  
The header of the current sort column displays a border and an arrowhead. An upward pointing arrowhead indicates ascending order and a downward pointing arrowhead indicates descending order.
- 3 To reverse the order of the current sort column, click the column header.  
The arrowhead in the column header reverses order. For example, when the column is in ascending order, clicking the column header reverses the order to descending.

## Setting filters for related components

The Related component pane in the Component Information tab supports filters. Filters reduce the amount of information to let you focus on what is relevant. Use this procedure to display a subset of related components based on their network model component state.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 In the Related component pane, select any of the filter check boxes, as required. The ISTB and OOS filters have criticality levels ranging from a low of 1 to a high of 5. By default, all levels display. If required, you can change the criticality levels.
  - **UNKN** displays related components whose state is unknown.
  - **INSV** displays related components whose state is in-service.
  - **ISTB** displays related components whose state is in-service—troubled. If required, change the criticality levels by selecting from the associated drop-down list.
  - **OOS** displays related components whose state is out-of-service. If required, change the criticality levels by selecting from the associated drop-down list.
  - **MTCE** displays related components whose state is maintenance.
  - **HIER MTCE** displays related components whose state is hierarchical maintenance.
  - **ACKED** displays related components whose state is acknowledged.

The related component list refreshes, based on the selected filters.

## Setting an automatic refresh interval for related components

You can control whether or not the related component list refreshes and the frequency of refreshes. Use this procedure to establish or change the automatic refresh settings.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 In the related component pane, type a value in the **minute** box or use the arrows to increase or decrease the current number of minutes. The minimum value is 2 minutes.
- 3 To set the automatic refresh value, select the **Refresh the Related Components** check box.

The related component list automatically refreshes at the specified time interval.

- 4 To stop automatic refreshes, clear the **Refresh the Related Components** check box.

## Displaying component attributes

You can display attributes and their associated values for Passport components. Passport Shelf View retrieves these attributes directly from the Passport device. Use this procedure to display component attributes.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 In the **Component Navigator** pane, right-click on the component for which you want to view attributes.

**Note:** Select an actual component instance from the component tree, not a entry that has a wildcard (\*). For example, you can display component attributes for CARD/2, but you cannot display attributes for CARD/\*. CARD/\* represents a category of components, not an actual component instance.

A pop-up menu opens.

- 3 From the pop-up menu, select **Show Attribute....**

A dialog opens and displays all the attributes and their values for the selected component.

- 4 To update the list with current information, click **Refresh**.

## Displaying alarms

Use this procedure to display detailed alarm information for a component.

### Procedure Steps

- 1 Click the **Component Information** tab to select it.
- 2 Use one of the following methods to populate the **Component details for** field:
  - In the related component pane, double-click on a component.
  - In the **Component details for** field, type or paste a component identifier and click **Retrieve**.

The component detail pane refreshes with the information for the selected component.

## Sorting alarms

The Component Information tab displays alarm information in tabular format. By default, the alarm table sorts alarms by the order in which they are received by the General Management Data Router (GMDR). You can change the order from ascending to descending chronological order and you can change the column on which the table is sorted. Use this procedure to sort alarms.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 To sort the alarm table on a specific column, click its column header.  

The header of the current sort column displays a border and an arrowhead. An upward pointing arrowhead indicates ascending order and a downward pointing arrowhead indicates descending order.
- 3 To reverse the order of the current sort column, click the column header.  

The arrowhead in the column header reverses order. For example, when the column is in ascending order, clicking the column header reverses the order to descending.

## Setting an automatic refresh interval for alarms

You can control whether or not the alarm list refreshes and the frequency of refreshes. Use this procedure to establish or change the automatic refresh settings.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 In the component detail pane, type a value in the **seconds** box or use the arrows to increase or decrease the current number of seconds. The minimum value is 10 seconds.
- 3 To set the automatic refresh value, select the **Refresh the alarm lists** check box.  
The alarm list automatically refreshes at the specified time interval.
- 4 To stop automatic refreshes, clear the **Refresh the alarm lists** check box.

## Acknowledging an alarm

Acknowledging an alarm indicates that you are currently investigating the problem associated with the alarm. Use this procedure to acknowledge a selected alarm.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 In the **Active Alarms from GMDR** list, right-click on an alarm.  
A pop-up menu opens.
- 3 From the pop-up menu, select **Acknowledge Alarm...**  
An **Input** dialog opens and prompts for the acknowledgement reason.
- 4 In the **Input** dialog, type the reason for alarm acknowledgement and click **OK**.  
The **Input** dialog closes.
- 5 To view the acknowledgement, the alarm list need refreshing. Use one of the following methods:
  - Click **Retrieve**.
  - If you have set an automatic refresh interval set up, wait for the list to update automatically.

## Acknowledging all active alarms on a component

You can acknowledge all active alarms on a component. Acknowledging the alarms indicates that you are currently investigating the problems associated with the component. Use this procedure to acknowledge all active alarms for a selected component.

### Procedure steps

- 1 Position the mouse pointer on any provisioned (colored) component in the Passport Shelf View window and right-click.  
A pop-up menu opens.
- 2 From the pop-up menu, select **Fault -> Acknowledge Alarms on Component...**  
The **Acknowledge Alarm(s) Dialog** opens.
- 3 In the **Acknowledge Alarm(s) Dialog**, type a reason for the alarm acknowledgement.
- 4 Optionally, to acknowledge all alarms for related subcomponents, select the **Also ack all alarms on related sub-components** check box.
- 5 Click **Ack Alarm(s)**.  
The dialog closes.
- 6 Alarm acknowledgement displays in the alarm list after the specified refresh interval. To immediately view the acknowledgement, click **Refresh**.

## Unacknowledging an alarm

If an alarm has been acknowledged, you can turn off the acknowledgement when required. Use this procedure to unacknowledge an alarm.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 In the **Active Alarms from GMDR** list, right-click on an alarm that is currently acknowledged.  
  
A pop-up menu opens.
- 3 From the pop-up menu, select **Unacknowledge Alarm....**  
  
An **Input** dialog opens and prompts for the unacknowledgement reason.
- 4 In the **Input** dialog, type the reason for alarm unacknowledgement and click **OK**.  
  
The **Input** dialog closes.
- 5 To view the unacknowledgement, the alarm list need refreshing. Use one of the following methods:
  - Click **Retrieve**.
  - If you have set an automatic refresh interval set up, wait for the list to update automatically.
- 6 Alarm unacknowledgement displays in the alarm list after the specified refresh interval. To immediately view the unacknowledgement, click **Refresh**.

## Unacknowledging all active alarms on a component

If you have acknowledged all alarms for a component, you can turn off this acknowledgement when required. Use this procedure to unacknowledge all active alarms for a selected component.

### Procedure steps

- 1 Position the mouse pointer on any provisioned (colored) component in the Passport Shelf View window and right-click.  
A pop-up menu opens.
- 2 From the pop-up menu, select **Fault -> Unacknowledge Alarms on Component...**  
The **Unacknowledge Alarm(s) Dialog** opens.
- 3 In the **Unacknowledge Alarm(s) Dialog**, type a reason for the alarm unacknowledgement.
- 4 Optionally, to unacknowledge all alarms for related subcomponents, select the **Also unack all alarms on related sub-components** check box.
- 5 Click **Unack Alarm(s)**.  
The dialog closes and the active alarms for the selected component are unacknowledged.
- 6 Alarm unacknowledgement displays in the alarm list after the specified refresh interval. To immediately view the unacknowledgement, click **Refresh**.

## Clearing local alarms

You can clear active alarms from the workstation's fault stack. This action clears the alarms from Preside Multiservice Data Manager only, not from the on-switch active alarm list.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 In the **Active Alarms from GMDR** list, right-click on an alarm.  
A pop-up menu opens.
- 3 From the pop-up menu, select **Local Clear**.
- 4 In the **Component details for** field, click **Retrieve** to refresh the alarm list.

The selected alarm is removed from the active alarm list.

## Clearing global alarms

You can clear active alarms from the workstation's fault stack and from the on-switch active alarm list. Use this procedure to globally clear alarms.

### Prerequisite

The ability to clear global alarms is available in Passport releases PCR 4.2 and above.

### Procedure steps

- 1 Click the **Component Information** tab to select it.
- 2 In the **Active Alarms from GMDR** list, right-click on an alarm.  
A pop-up menu opens.
- 3 From the pop-up menu, select **Global Clear**.
- 4 In the **Component details for** field, click **Retrieve** to refresh the alarm list.

The selected alarm is removed from the active alarm list.

## Making provisioning changes to components and services

You can perform component and service provisioning tasks from the Passport Shelf View tool using the Embedded Nodal Provisioning tool.

### Limitations

The Embedded Nodal Provisioning tool lets you perform a selection of provisioning tasks to a small number of components in the current active Passport view. To navigate and provision large numbers of Passport components in a variety of Passport views, use Nodal Provisioning rather than Embedded Nodal Provisioning.

### References

For details about the Embedded Nodal Provisioning tool, see the embedded nodal provisioning section in 241-6001-610 *Preside MDM Nodal Provisioning User Guide*.

### Procedure steps

- 1 To open the component pop-up menu, from any tabbed page right-click on the component you want to provision.
- 2 From the component pop-up menu, select **Configuration** and from the resulting submenu, select one of the following provisioning tasks:
  - **Add Subcomponent...**
  - **Change...**
  - **Delete...**
  - **Apply Service Template...**

The Embedded Nodal Provisioning tool opens.

## Starting other MDM tools from Passport Shelf View

The Passport Shelf View tool provides a selection of fault and configuration capabilities. To perform additional fault, configuration, and performance tasks, you can start other tools from the Passport Shelf View. Use this procedure to start other MDM tools with component context from Passport Shelf View.

### Procedure steps

- 1 From any of the panes in the Passport Shelf View window, right-click on the component that you want to put into context.  
A component pop-up menu opens.
- 2 From the component pop-up menu, select one of **Fault**, **Configuration**, or **Performance** and from the resulting submenu select the tool you want to start.

The table “Tools you can start from Passport Shelf View” (page 170) provides references to further information.

**Table 21**  
**Tools you can start from Passport Shelf View**

Start Tool	Related Information
Fault:	
Component Information Viewer	“Component Information Viewer” (page 301)
Circuit Viewer	“Circuit Viewer” (page 467)
Acknowledge Alarms on Component	“Alarm acknowledgement and unacknowledgement” (page 275)
Unacknowledge Alarms on Component	“Alarm acknowledgement and unacknowledgement” (page 275)
Configuration	Embedded Nodal Provisioning in 241-6001-610 <i>Preside MDM Nodal Provisioning User Guide</i>
(Sheet 1 of 2)	

**Table 21 (continued)**  
**Tools you can start from Passport Shelf View**

Start Tool	Related Information
Performance:  Data Viewer	Data Viewer in 241-6001-031 <i>Preside MDM Performance Management User Guide</i>
(Sheet 2 of 2)	

## Errors and warnings

The Passport Shelf View provides the following error and warning messages to help you take corrective action:

- “Non-Passport Context” (page 172)
- “Unknown Passport” (page 172)
- “Cannot connect to psvagent” (page 173)
- “Cannot Connect To Server” (page 173)
- “Cannot Connect To mnsdagent” (page 173)
- “Invalid or Missing Definition File” (page 174)

### Non-Passport Context

**Message** MDM’s current context does not refer to a Passport. Unable to launch the Passport Shelf View.

**Cause:** Passport Shelf View has tried to start with a component in context that is not a Passport device.

**Action:** Acknowledge the message to close Passport Shelf View. Put a Passport device in context and then start the Passport Shelf View.

### Unknown Passport

**Message:** MDM does not recognize the Passport <Passport Name>. Verify that the Passport is accessible and that it belongs to a Passport group.

**Cause:** HGDS cannot find the specified Passport device. The node may be in the network model but Service Selection might be focused on a host that does not support connections to that host.

## **Cannot connect to psvagent**

**Message:** The connection to the psvagent has been lost. Verify the server is running, and restart the application.

**Cause:** The socket connection between the client and the Passport Shelf View tool is no longer available. The cause is usually that the server is stopped. This error causes the client to exit.

## **Cannot Connect To Server**

**Message:** A connection to the server could not be made. Verify the server is running, and restart the application.

**Cause:** The client has started but it cannot connect to the psvagent. The cause is usually an error during startup of the psvagent. This error causes the client to exit.

**Action:** Refer to the MDM System Log for details about the error encountered by the psvagent and verify that the Shelf View ApplicationServer is reachable.

## **Cannot Connect To mnsdagent**

**Message:** A connection to the mnsdagent could not be made. Verify that the mnsdagent is running, and restart the application.

**Cause:** The client has started but it cannot connect to the mnsdagent. If the error occurs when the client is accessing context, the client exits. If the error occurs when the client is setting context to launch another tool, the client continues but the tool launches without context.

## Invalid or Missing Definition File

Message: The file <filename> is missing or contains an invalid definition.

Cause: The client has encountered errors reading or parsing shelf, card, or port definition files.

---

## Chapter 4

# VPN Monitor

---

### Overview

VPN Monitor is a Preside Multiservice Data Manger (MDM) tool that provides fault management capabilities for Passport Internet Protocol (IP) Virtual Private Network (VPN) services. This tool monitors network components that make up the VPN services to detect and identify troubled elements within the service. VPN Monitor displays VPN topology along with state information so that you can easily identify and navigate troubled areas. From VPN Monitor, you can also start other MDM fault management tools to further investigate and correct faults.

VPN Monitor supports the following types of Passport VPNs:

- “RFC 2764” (page 178)
- “RFC 2547” (page 187)
- “Direct virtual router to virtual router” (page 193)

**ATTENTION**

Passport 6000 nodes with P7.0.x software release do not support the VPN ID attribute so the virtual routers are not loaded into the MDM Admin DB. Consequently, the VPN management tools introduced in MDM 14.3, including IP VPN Service Provisioning and VPN Monitor cannot be used.

For more details about VPN Monitor, see the following topics:

- “Service views” (page 176)

- “VPN Monitor architecture” (page 177)
- “RFC 2764” (page 178)
- “RFC 2547” (page 187)
- “Direct virtual router to virtual router” (page 193)
- “VPN state color conventions” (page 198)
- “VPN Monitor window” (page 201)
- “Procedures” (page 207)

## Service views

The VPN Monitor tool extracts VPN-related information from the MDM Administration Database and creates service-level views of VPNs. VPN Monitor displays these views as basic services or service clusters.

### Basic services

Basic services are logical representations of network services. These services are an aggregation of components, some of which have state values. The basic service state is derived from the actual state of the components it contains. An example of a basic service is the router element which represents the Passport software entity that emulates a physical router.

For details about basic services, see the following topics:

- “RFC 2764 basic services” (page 178)
- “RFC 2547 basic services” (page 187)
- “Direct VR-VR basic services” (page 193)

### Service clusters

Service clusters represent an aggregation of basic services or an aggregation of other service clusters. These aggregations create the following service types: VPN, site, core router, and customer router. Service cluster states are derived from the state of its constituent service clusters or basic services. An example of a service cluster is the VPN cluster which represents the collection of basic services the represent the whole customer VPN.

For details about service clusters, see the following topics:

- “RFC 2764 service clusters” (page 183)
- “RFC 2547 service clusters” (page 189)
- “Direct VR-VR service clusters” (page 196)

## VPN Monitor architecture

VPN Monitor provides a client-server based monitoring system for VPNs and consists of the following components:

- VPN Monitor extractor
- VPN Monitor server
- VPN Monitor client

The VPN Monitor extractor collects VPN configuration data from the MDM Administration Database and delivers this data to the VPN Monitor server and client. For details, see the section on the VPN Monitor Extractor section in 241-6001-310 *Preside MDM Server Reference Guide*.

The VPN Monitor server collects fault data consisting of raw state and state change notifications for basic service components, calculates the overall state of each VPN basic service, and passes this information to the VPN Monitor client. For details, see the section on the VPN Monitor Server section in 241-6001-310 *Preside MDM Server Reference Guide*.

The VPN Monitor client displays the VPN services and the status of those services. From the client, you can start other MDM fault, configuration, and performance management tools.

## RFC 2764

For a description of RFC 2764 VPNs, see the following topics:

- “RFC 2764 basic services” (page 178)
- “RFC 2764 service clusters” (page 183)
- “RFC 2764 provider edge network service views” (page 184)

### RFC 2764 basic services

The table “RFC 2764 basic service descriptions” (page 178) lists the RFC 2764 basic services and their descriptions.

**Table 22**  
**RFC 2764 basic service descriptions**

Basic service	Description
Router element	represents a Passport software entity that emulates a physical router or a virtual connection gateway
Core access point	represents a backbone-facing IP interface on a VCG.
Tunnel end point	represents the point-to-multipoint (PTMP) tunnel end point at the router element (corresponds to a private address)
Tunnel access point	represents a customer VR-facing IP interface on the VCG. It represents the PTMP tunnel access point on the VCG
Site access point	represents an instance of customer access to a router element on the Passport device

#### Basic service creation conventions

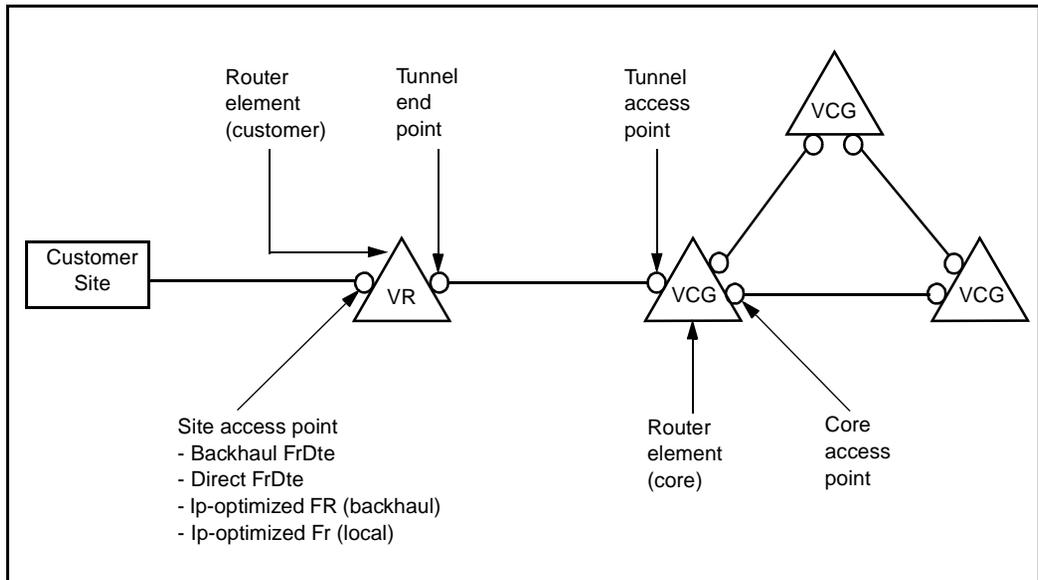
During the creation of a tunnel access point when you have created a logical interface on a core router but have not yet linked this interface to a customer VR, VPN Monitor associates a basic service of core access point with this logical interface. When you link a customer VR to the logical interface, VPN Monitor changes the association to tunnel access point.

If a loopback logical interface for IP routing is present on the VR (for example, when using BGP), then VPN Monitor associates a basic service of core access point with the interface.

### Basic service schema

The figure “RFC 2764 basic service schema” (page 179) shows these basic services in an RFC 2764 IP VPN.

**Figure 13**  
**RFC 2764 basic service schema**



### Basic service components

The table “RFC 2764 basic service components” (page 180) details the Passport components that comprise each of the basic service.

**Table 23**  
**RFC 2764 basic service components**

Basic services	Components
Router element	
Customer	EM/ Vr/ EM/ Vr/ Ip EM/ Vr/ Ip Tunnel
Core	EM/ Vr/ EM/ Vr/ Ip
Core access point	EM/ Vr/ Pp/ EM/ Vr/ Pp/ IpPort EM/ Vr/ Pp/ IpPort LogicalIf/ EM/ <media component> <sup>1</sup>
Tunnel end point	EM/ Vr/ Pp/ EM/ Vr/ Pp/ IpPort EM/ Vr/ Pp/ IpPort LogicalIf/ EM/ Vr/ Ip Tunnel
Tunnel access point	EM/ Vr/ Pp/ EM/ Vr/ Pp/ IpPort EM/ Vr/ Pp/ IpPort LogicalIf/ EM/ Vm/ If
Site access point	
(Sheet 1 of 3)	

**Table 23 (continued)**  
**RFC 2764 basic service components**

Basic services	Components
Backhaul FrDte	<p>at the Fruni connection end point node:  EM/A Fruni/x  EM/A Fruni/ xFramer  EM/A Fruni/ xLMI  EM/A Fruni/ xDlci/ <sup>2</sup></p> <p>at the IP service node where the router element resides:  EM/B Fruni/y  EM/B FrDte/y  EM/B FrDte/ RemoteGroup/  EM/B Vr/ Pp/  EM/B Vr/ Pp/ IpPort  EM/B Vr/ Pp/ IpPort LogicalIf/</p>
Direct FrDte	EM/A Fruni/x EM/A Fruni/ Framer EM/A Fruni/ Lmi EM/A Fruni/ Dlci/x <sup>2</sup> EM/B Fruni/x EM/B FrDte/x EM/B FrDte/ Remote Group/ EM/B Vr/ Pp EM/B Vr/ Pp/ IpPort EM/B Vr/ Pp/ IpPort LogicalIf/
IP-optimized FR (backhaul)	<p>at the Fruni connection end point node:  EM/A Fruni/x  EM/A Fruni/ LMI  EM/A Fruni/ Framer  EM/A Fruni/ Dlci/ <sup>2</sup></p> <p>at the IP service node where the virtual router resides:  EM/B Fruni/y  EM/B Vr/ Pp/  EM/B Vr/ Pp/ IpPort  EM/B Vr/ Pp/ IpPort LogicalIf/  EM/B IpDlciGroup/</p>
(Sheet 2 of 3)	

**Table 23 (continued)**  
**RFC 2764 basic service components**

Basic services	Components
IP-optimized FR (local)	EM/ Fruni/x EM/ Fruni/ Framer EM/ Fruni/ Lmi EM/ Fruni/ Dlci/ <sup>2</sup> EM/ Vr/ Pp/ EM/ Vr/ Pp/ IpPort EM/ Vr/ Pp/ IpPort LogicalIf/ EM/ IpDlciGroup/
<p><sup>1</sup> Media component may change depending on the backbone.  <sup>2</sup> One for each IPCos.</p> <p><b>Note:</b> Where applicable, Fruni can be replaced by Frnni.  <b>Note:</b> For backhaul scenarios, there may be more than one Fruni with Dlci. In this case, these Frunis and their associated Dlci, Lmi, and Framer components are included in the basic service.</p>	
(Sheet 3 of 3)	

### Basic service state after component deletion

When you delete components of a basic service, the basic service state, as shown in VPN Monitor, remains as is until the following events occur:

- the MDM Administration Database is updated to reflect the component changes
- the VPN Monitor Extractor detects the changes when it automatically polls the MDM Administration Database or the administrator manually polls for database changes using the VPNMonitorExtractor.kick script

After VPN Monitor receives these component changes through polling, it determines the new state of the basic service.

### Basic service initial timestamp

When the VPN Monitor Server starts, it collects and calculates the state of each basic service, based on the state of the service's components. If there are no faults against a basic service's components, the basic service is given a state of in-service. To maintain the integrity of performance and scalability, when VPN Monitor starts, the client retrieves the states for all basic services

which are not currently in-service. As a result, the initial time stamp for services that are in-service is “00/01/01 00:00:00”. The initial time stamp remains until a state change occurs.

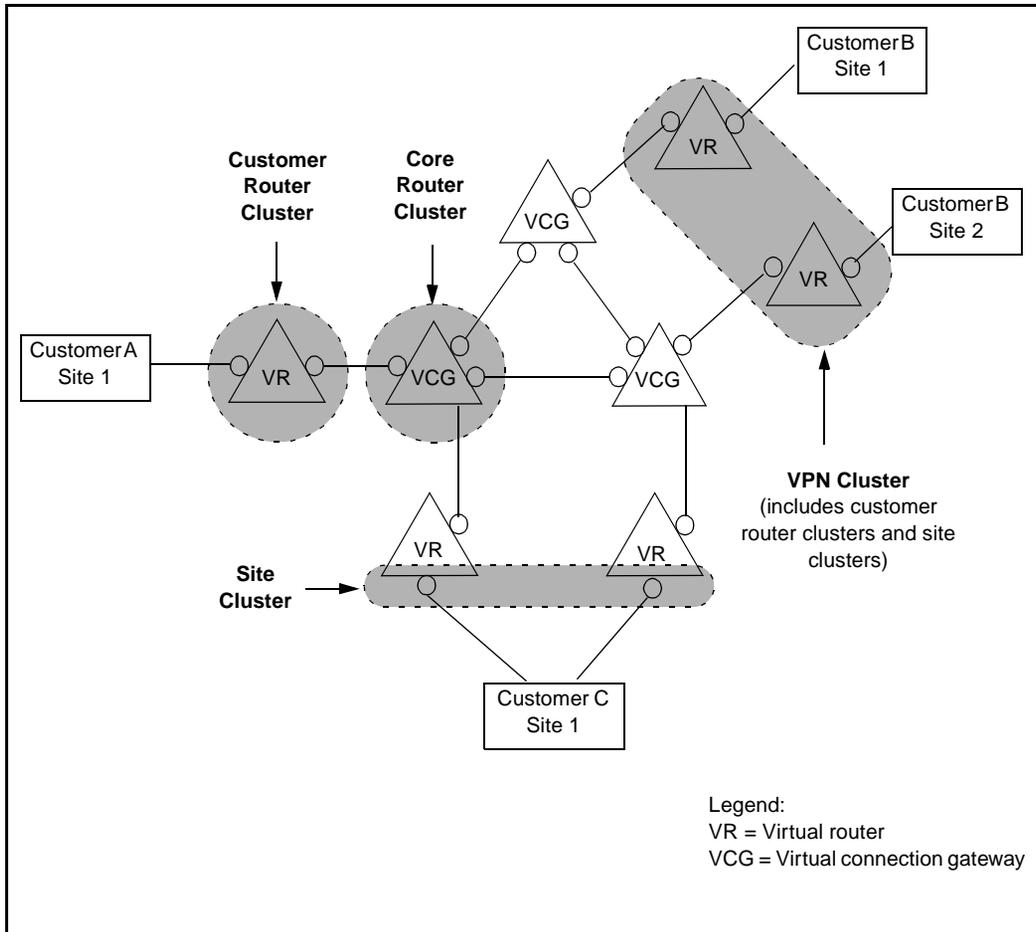
## RFC 2764 service clusters

The table “RFC 2764 service cluster descriptions” (page 183) lists RFC 2764 service clusters and their description. The figure “RFC 2764 service clusters” (page 184) shows sample service clusters.

**Table 24**  
**RFC 2764 service cluster descriptions**

<b>Service cluster</b>	<b>Description</b>
Core router	represents the core router and its access points to tunnels and the backbone connection.
Customer router	represents the router element and its access point to the tunnel and its customer interfaces.
Site	represents a collection of customer site access points to one or more router elements.
VPN	represents the entire customer VPN and includes all associated customer routers and sites.

**Figure 14**  
**RFC 2764 service clusters**



### RFC 2764 provider edge network service views

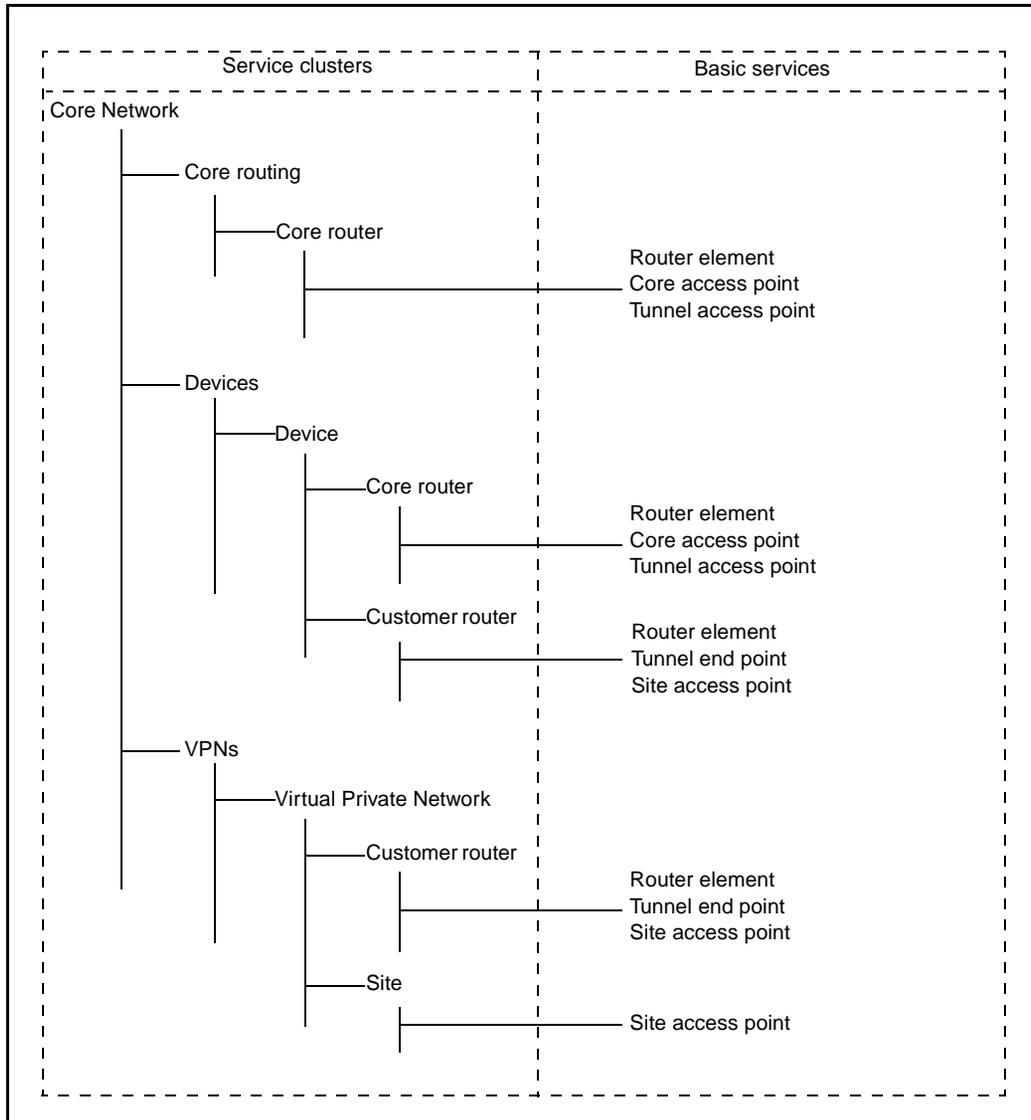
The VPN Monitor uses basic service and service cluster data to construct and display VPN information in an hierarchical, or service view, arrangement. RFC 2764 has the following service views:

- Core Routing
- Devices

- VPNs

For details about service views, see “RFC 2764 provider edge network service views” (page 186).

**Figure 15**  
**RFC 2764 provider edge network service views**



## RFC 2547

VPN Monitor supports RFC 2547. For details, see the following sections:

- “RFC 2547 basic services” (page 187)
- “RFC 2547 service clusters” (page 189)
- “RFC 2547 provider edge network service views” (page 191)

### RFC 2547 basic services

The table “RFC 2547 basic service descriptions” (page 187) lists RFC 2547 basic services and their description. The figure “RFC 2547 basic service schema” (page 188) shows these basic services in an RFC 2547 IP VPN.

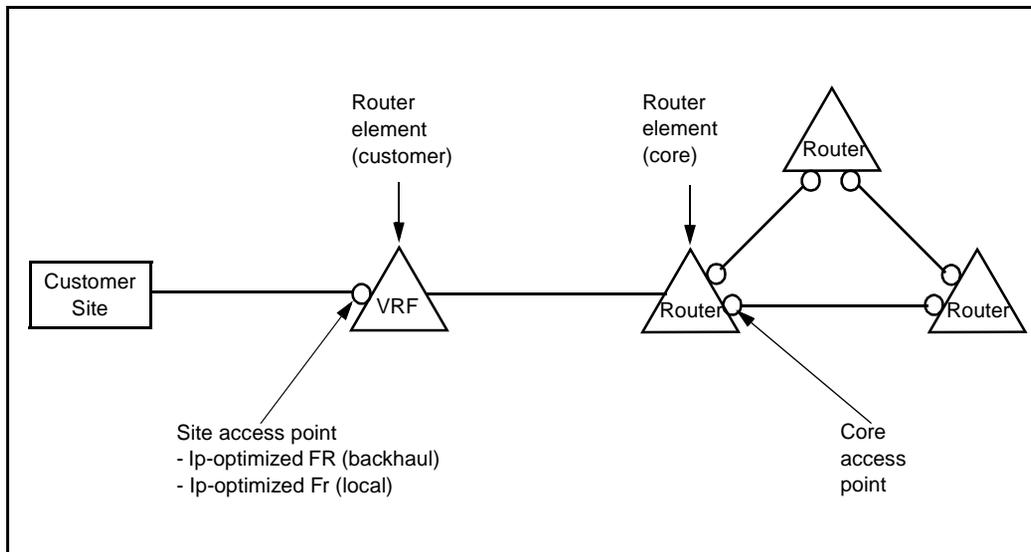
**Table 25**  
**RFC 2547 basic service descriptions**

Basic service	Description
Router element	represents a Passport router or a VPN routing function.
Core access point	represents the access to the backbone that interconnects router elements.
Site access point	represents an instance of customer access to a customer router element on the Passport device.

#### Basic service creation conventions

Logical interfaces associated with a loopback address (for example, rtr/ if/ lb) have a basic service type of core access point.

**Figure 16**  
**RFC 2547 basic service schema**



The table “RFC 2547 basic service components” (page 188) details the Passport components that comprise each of the basic services.

**Table 26**  
**RFC 2547 basic service components**

Basic services	Components
Router element	
Customer	EM/ Rtr/ Vrf/
Core	EM/ Rtr/ EM/ Vr/ Ldp 1
Core access point	EM/ Rtr/ If/ EM/ Rtr/ If/ <Media component> <sup>2</sup>
(Sheet 1 of 2)	

**Table 26 (continued)**  
**RFC 2547 basic service components**

Basic services	Components
<p>Site access point</p> <p>IP-optimized FR (backhaul)</p> <p>IP-optimized FR (local)</p> <p>1 May differ depending on MPLS type.            2 Media component may change depending on the backbone.            3 One for each IPCos.</p> <p><b>Note:</b> Where applicable, Fruni can be replaced by Frnni.</p> <p><b>Note:</b> For backhaul scenarios, there may be more than one Fruni with Dlcis. In this case, these Frunis and their associated Dlcis, Lmi, and Framers components are included in the basic service</p>	<p>at the Fruni connection end point node:            EM/A Fruni/            EM/A Fruni/ Lmi            EM/A Fruni/ Framers            EM/A Fruni/ Dlcis<sup>3</sup></p> <p>at the router node:            EM/B Fruni/x            EM/B Fruni/y            EM/B Rtr/ Vrf/ If/            EM/B Rtr/ Vrf/ If/ IpODlcis</p> <p>EM/ Fruni/            EM/ Fruni/ Framers            EM/ Fruni/ Lmi            EM/ Fruni/ Dlcis<sup>3</sup>            EM/ Rtr/ Vrf/ If/            EM/ Rtr/ Vrf/ If/ IpODlcis</p>
(Sheet 2 of 2)	

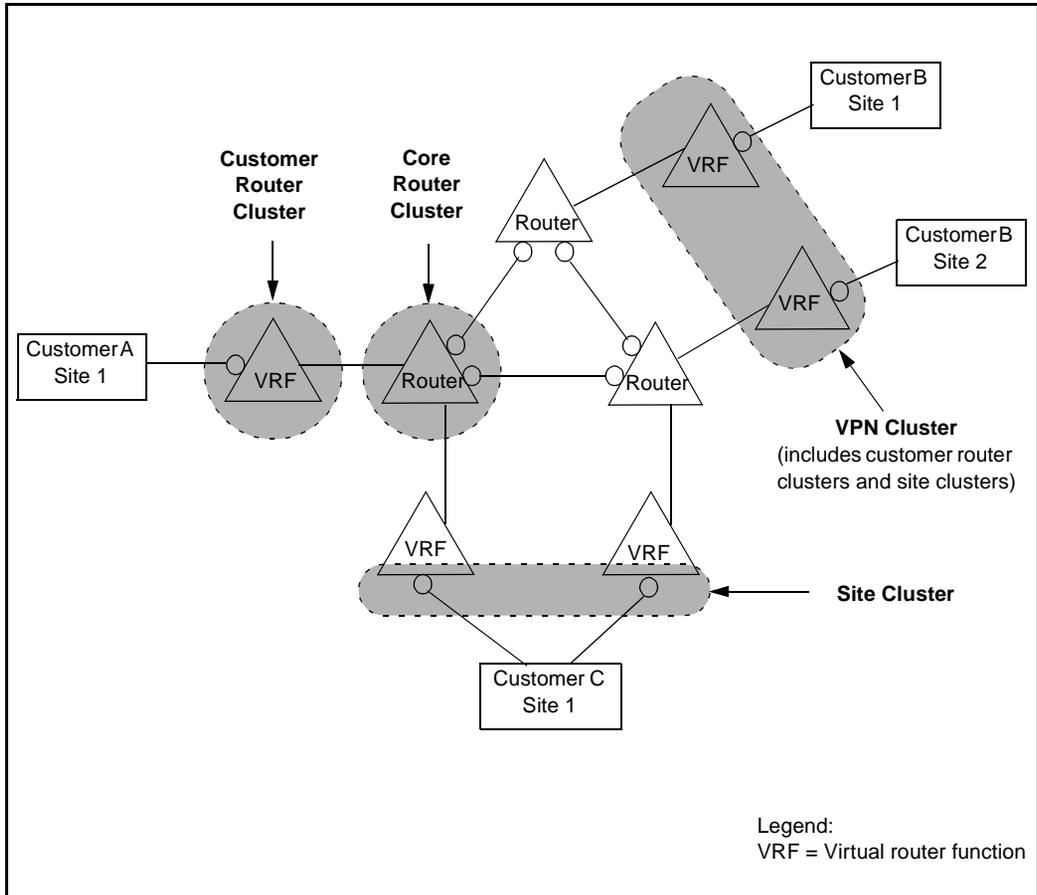
## RFC 2547 service clusters

The table “RFC 2547 service cluster descriptions” (page 190) lists RFC 2547 service clusters and their descriptions. The figure “RFC 2547 service clusters” (page 191) shows sample service clusters.

**Table 27**  
**RFC 2547 service cluster descriptions**

<b>Service cluster</b>	<b>Description</b>
Core router	represents the router and its interfaces to the backbone.
Customer router	represents the VPN routing function and its customer site access points.
Site	represents a collection of customer site access points to one or more virtual routers.
VPN	represents the entire customer VPN and includes VPN routing functions on different Passports and all of their corresponding site access points.

**Figure 17**  
**RFC 2547 service clusters**



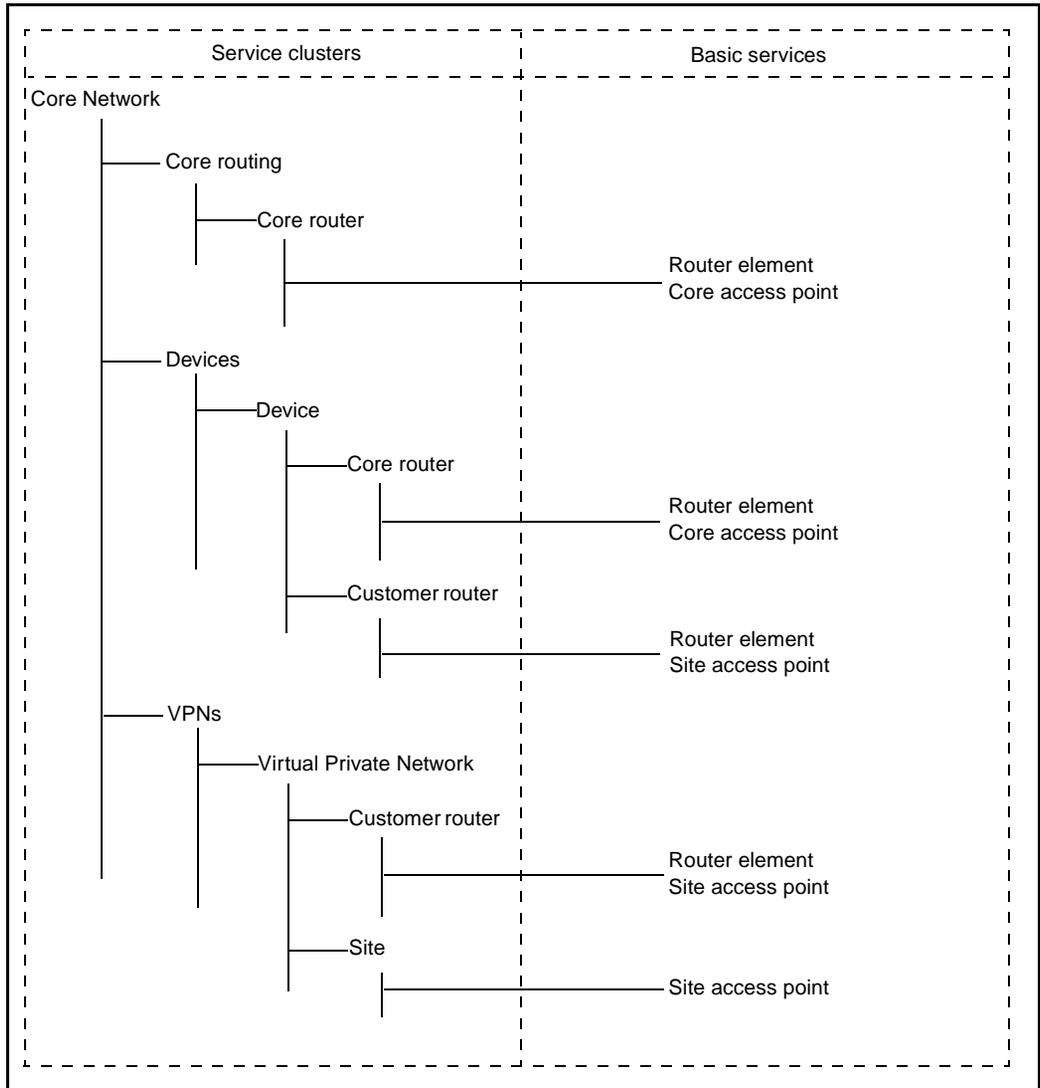
### RFC 2547 provider edge network service views

The VPN Monitor uses basic service and service cluster data to construct and display VPN information in an hierarchical, or service view, arrangement. RFC 2547 has the following service views:

- Core Routing
- Devices
- VPNs

For details about service views, see “RFC 2547 provider edge network service views” (page 192).

**Figure 18**  
**RFC 2547 provider edge network service views**



## Direct virtual router to virtual router

VPN Monitor supports direct virtual router to virtual router (VR-VR) VPNs. For details, see the following sections:

- “Direct VR-VR basic services” (page 193)
- “Direct VR-VR service clusters” (page 196)
- “Direct VR-VR VPN views” (page 197)

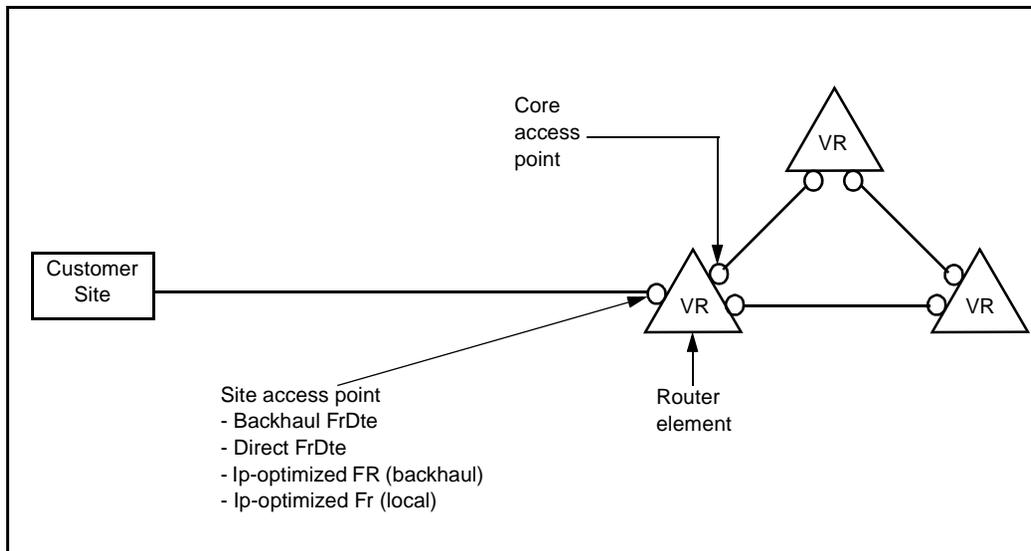
### Direct VR-VR basic services

The table “Direct VR-VR basic service descriptions” (page 193) lists direct VR-VR basic services and their description. The figure “Direct VR-VR VPN schema” (page 194) details the Passport components that comprise each of the basic services.

**Table 28**  
**Direct VR-VR basic service descriptions**

Basic service	Description
Router element	represents the Passport software entity that emulates a physical router and is used for a virtual router.
Core access point	represents the access to the backbone that interconnects router elements and is a peer to other core access points on other router elements in the VPN.
Site access point	represents an instance of customer access to a router element on the Passport device.

**Figure 19**  
**Direct VR-VR VPN schema**



The table “Direct VR-VR VPN basic service components” (page 194) details the Passport components that comprise each of the basic services.

**Table 29**  
**Direct VR-VR VPN basic service components**

Basic services	Components
Router element	EM/ Vr/ EM/ Vr/ Ip/
Core access point	EM/ Vr/ Pp/ EM/ Vr/ Pp/ IpPort EM/ Vr/ Pp/ IpPort LogicalIf/ EM/ AtmMpe/
(Sheet 1 of 3)	



**Table 29 (continued)**  
**Direct VR-VR VPN basic service components**

Basic services	Components
IP-optimized FR (local)	EM/ Fruni/x EM/ Fruni/ Framer EM/ Fruni/ Lmi EM/ Fruni/ Dlci/ <sup>1</sup> EM/ Vr/ Pp/ EM/ Vr/ Pp/ IpPort EM/ Vr/ Pp/ IpPort LogicalIf/ EM/ IpDlciGroup/
<sup>1</sup> One for each IPCos.	
<b>Note:</b> Where applicable, Fruni can be replaced by Frnni.	
<b>Note:</b> For backhaul scenarios, there may be more than one Fruni with Dlci's. In this case, these Frunis and their associated Dlci, Lmi, and Framer components are included in the basic service.	
(Sheet 3 of 3)	

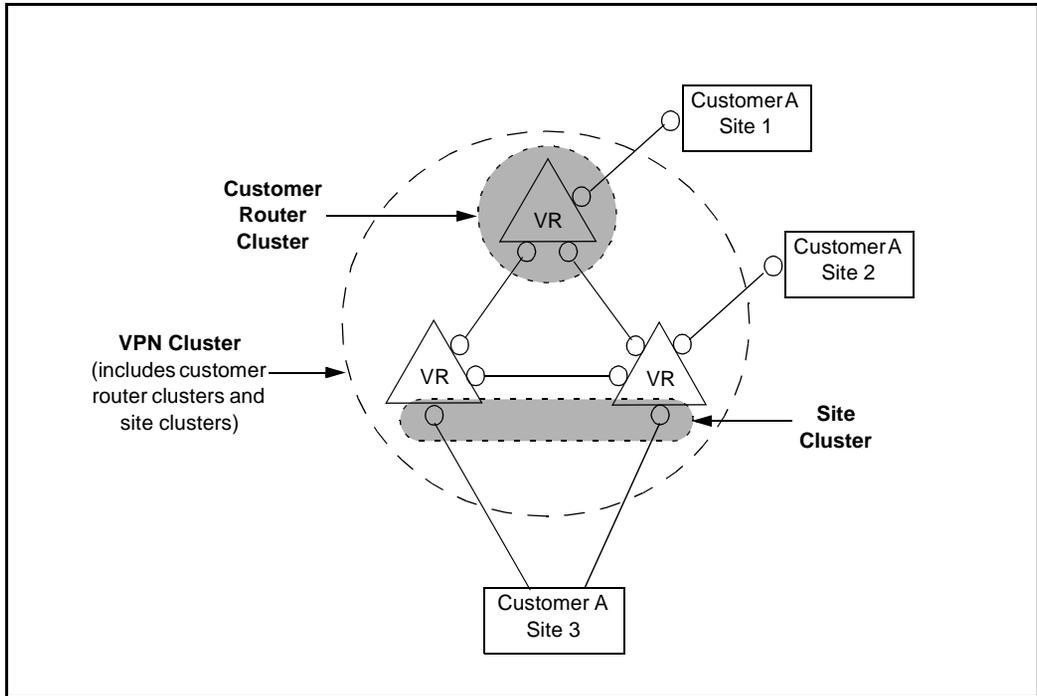
## Direct VR-VR service clusters

The table “Direct VR-VR service descriptions” (page 196) lists direct VR-VR basic services and their description. The figure “Direct VR-VR service clusters” (page 197) shows sample service clusters.

**Table 30**  
**Direct VR-VR service descriptions**

Basic service	Description
Customer router	represents a virtual router and its interfaces.
Site	represents a collection of customer site access points to one or more virtual routers.
VPN	represents the entire customer VPN and includes customer virtual routers on different Passports, the core access points that connect to these virtual routers, and all site access points.

**Figure 20**  
**Direct VR-VR service clusters**



### Direct VR-VR VPN views

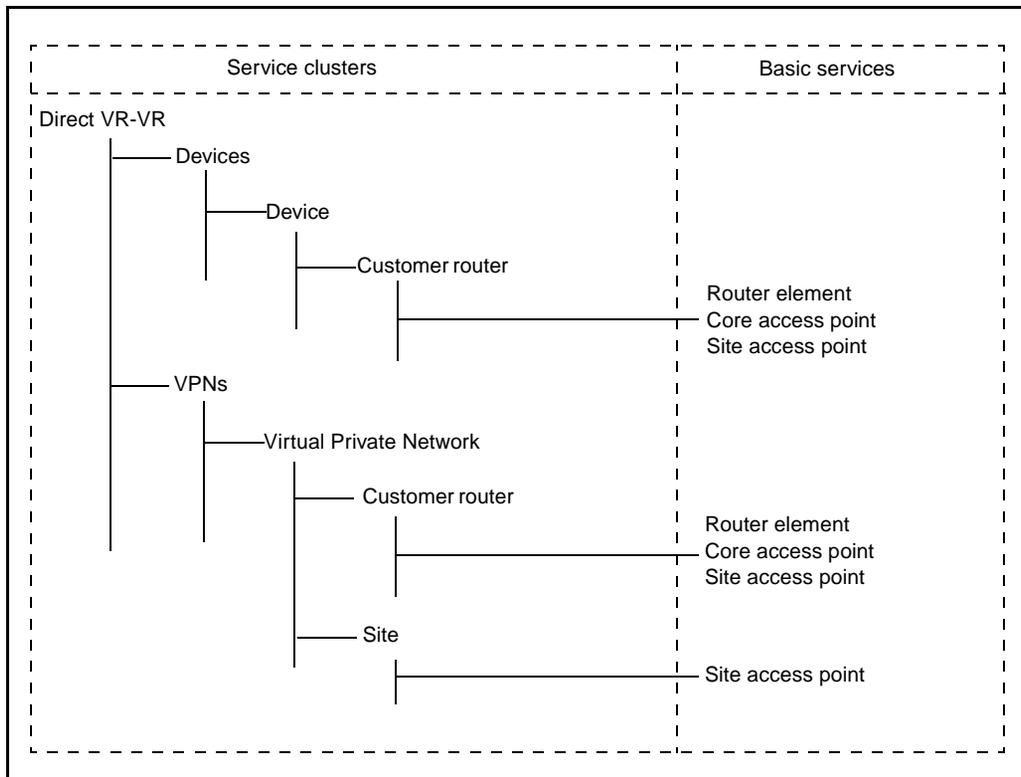
The VPN Monitor uses basic service and service cluster data to construct and display VPN information in an hierarchical, or service view, arrangement.

Direct VR-VR has the following views:

- Devices
- VPNs

For details about service views, see “Direct VR-VR VPN views” (page 198).

**Figure 21**  
**Direct VR-VR VPN views**



## VPN state color conventions

The VPN Monitor tool uses standard MDM color conventions to indicate the network model states of components. For a description of the default MDM state colors and their meaning, see the following tables:

- “Basic service states” (page 199)
- “Service cluster states” (page 199)
- “Core networks and view states” (page 200)

These tables list MDM states from the most severe (critical) to the least severe (normal).

## Basic service states

VPN Monitor computes the states of a basic services based on the states of their components. The table “Basic service states” (page 199) lists basic service colors, their associated MDM states, and rules for state determination.

**Table 31**  
**Basic service states**

Background color	MDM state	Description
Red	Critical	At least one component is out-of-service (OOS).
Grey	Unmanaged	All components are unknown (UNK). This state may occur during server startup when the server has fully retrieved its data.
Yellow	Troubled	At least one component is in-service—troubled (ISTB), other components are INSV or UNK. Or, at least one component is ISTB or UNK, other components are INSV or NA.
Green	Normal	At least one component is in-service (INSV). The state of other components, if any, are not available from the NDAM server.

## Service cluster states

The states of service clusters are based on the states of basic services or other service clusters that comprise the service clusters. The table “Service cluster states” (page 200) lists service cluster colors, their associated MDM states, and rules for state determination.

**Table 32**  
**Service cluster states**

<b>Background color</b>	<b>MDM state</b>	<b>Description</b>
Red	Critical	All basic services and service clusters have a critical state.
Yellow	Troubled	At least one basic service or service clusters is troubled, critical, or unmanaged.
Green	Normal	All basic services and service clusters have a normal state.

## Core networks and view states

The states of provider edge (PE) networks and views are based on the most severe status of the service clusters that comprise the PE networks or views. The order of severity is critical, unmanaged, troubled, and normal. The table “Service cluster states” (page 200) lists PE network and view state colors, their associated MDM states, and rules for state determination.

**Table 33**  
**Core network and view states**

<b>Background color</b>	<b>MDM state</b>	<b>Description</b>
Red	Critical	One or more clusters are critical.
Grey	Unmanaged	One or more clusters are unmanaged. Other clusters may be troubled or normal.
Yellow	Troubled	One or more clusters are troubled. Other clusters may be normal.
Green	Normal	All service clusters are normal.

## VPN Monitor window

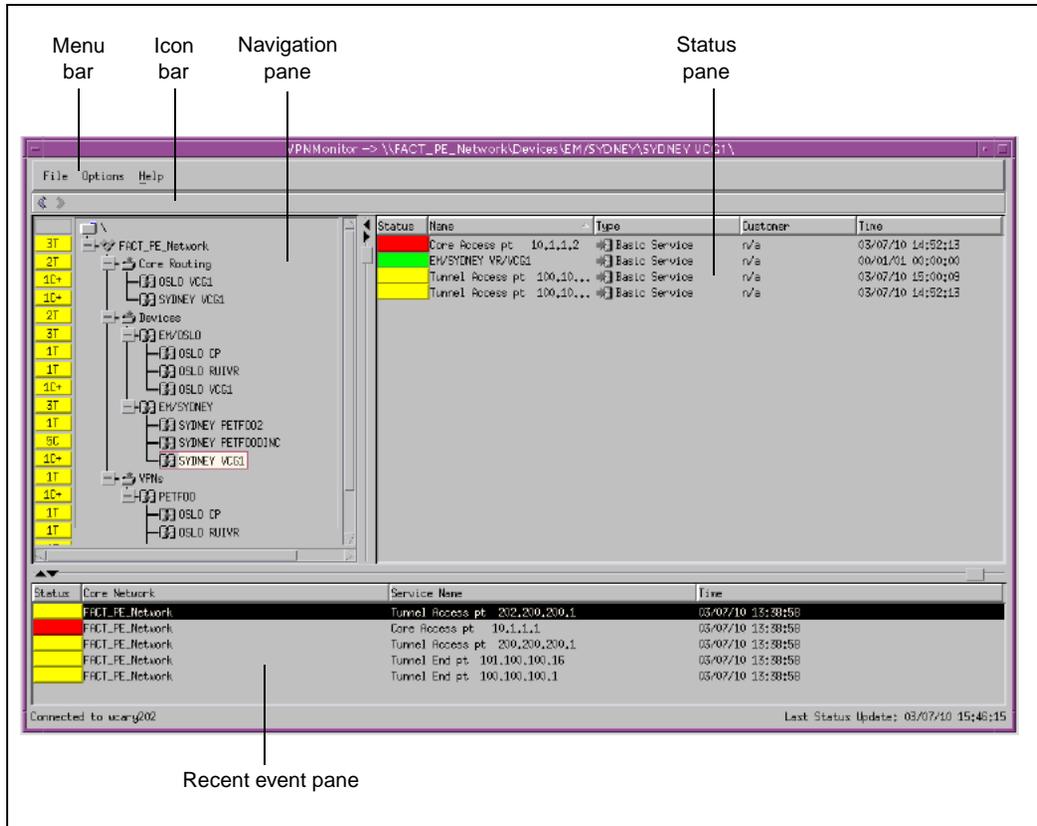
The VPN Monitor tool displays VPN services and the status of those services in a single window. VPN Monitor facilitates the diagnosis of IP VPN services and components in the Passport network.

The VPN Monitor window contains the following items:

- “Menu bar” (page 202)
- “Tool bar” (page 203)
- “Navigation pane” (page 203)
- “Status pane” (page 205)
- “Recent event pane” (page 205)

The figure “VPN Monitor window” (page 202) shows a sample VPN Monitor window with an RFC 2764 VPN network.

**Figure 22**  
**VPN Monitor window**



## Menu bar

The menu bar contains the following menus:

- “File” (page 203)
- “Options” (page 203)
- “Help” (page 203)

### File

The File menu contains the following command:

- **Exit** closes the window and exits the tool. See the procedure “Quitting VPN Monitor” (page 210).

### Options

The Options menu contains the following command:

- **StandardToolbar** displays or hides the standard tool bar. See the procedure “Displaying or hiding the tool bar” (page 214).

### Help

The Help menu contains the following commands:

- **On Context** displays information about a selected area of the VPN Monitor window. See the procedure “Displaying VPN Monitor online help” (page 211).
- **On Window** displays descriptive information about the VPN Monitor window components. See the procedure “Displaying VPN Monitor online help” (page 211).

## Tool bar

The standard tool bar contains icons that let you move backward or forward through the selections in the navigation pane. Selecting the back icon changes the display in the navigation pane to the previous selection. VPN Monitor keeps a history of the previous 10 selections in the tree. Selecting the forward icon changes the display to the next most recent selection in the navigation pane.

## Navigation pane

The navigation pane contains 2 columns. The first column indicates the computed state of all items in the navigation tree. For details about how the state is derived, see “VPN state color conventions” (page 198). As well as the state color indicator, the column also displays the number of critical or troubled subcomponents. See the figure “VPN Monitor states” (page 204).

The second column displays the navigation tree which defines the hierarchical structure of VPN provider edge (PE) networks and their associated views. For RFC 2764 and RFC 2547, the top level of the VPN

hierarchy in the navigation pane is the PE network. This PE network element corresponds to the PE network entity in the MDM. The next level shows the service views—core routing, devices, and VPNs.

**Figure 23**  
VPN Monitor states

OSLO\_VCG1 service cluster has a status of 1C+ indicating one of its basic services is critical (1C). The plus (+) indicates at least one other basic service is troubled.

The status pane shows which basic service is critical and which is troubled

Status	Core Network	Service Name	Time
1C+	Christina_PE_Network	Site Access pt 100.100.122.1	03/07/11 09:10:27
1C+	Christina_PE_Network	Tunnel End pt 100.100.100.1	03/07/11 09:10:27
1C+	Christina_PE_Network	Tunnel End pt 100.100.100.8	03/07/11 09:10:27
1C+	Christina_PE_Network	Site Access pt 100.100.33.33	03/07/11 09:10:27
1C+	Christina_PE_Network	Site Access pt 100.100.222.2	03/07/11 09:10:27
1C+	Christina_PE_Network	Site Access pt 100.100.150.1	03/07/11 09:10:27

For direct VR-VR VPNs, the top level of the VPN hierarchy is direct VR-VR. This entity is created in VPN Monitor. The next level shows the service views—VPNs and devices.

The navigation pane supports a pop-up menu. Right-clicking a service cluster in the navigation pane opens a pop-up menu that lets you search for all occurrences of the selected service in the PE network. See the procedure “Finding basic services or service clusters in the provider edge network” (page 218).

## Status pane

The contents of the status pane depend on what you select in the navigation pane. When you make a selection in the navigation pane, the status pane displays the components that make up the selected service. For each component, the status pane also displays the associated status, service type, customer name, and status time stamp.

The status pane supports pop-up menus. For basic services and service clusters the pop-up menu lets you search for all occurrences of the selected service in the provider edge network. See the procedure “Finding basic services or service clusters in the provider edge network” (page 218). The pop-up menu for basic services also lets you show all components of the selected service. See “Displaying basic service components” (page 217).

## Recent event pane

The recent event pane displays service status changes generated by the VPN Monitor Server. Events display in chronological order.

The recent event pane supports pop-up menus. For basic services the pop-up menu lets you search for all occurrences of the selected service in the provider edge network. See the procedure “Finding basic services or service clusters in the provider edge network” (page 218). The pop-up menu also lets you show all components of the selected service. See “Displaying basic service components” (page 217).

## VPN Monitor dialogs

VPN Monitor also contains the following dialogs:

- “Find” (page 205)
- “Component” (page 206)

### Find

Use the Find dialog to display all occurrences of a specific basic service or service cluster in the provider edge (PE) network.

The Find dialog contains the following fields:

- **Service Name** displays the selected basic service or service cluster.
- **Scope** indicates the PE network of the selected component. By using the associated drop-down menu, you can extend the scope to another PE network or all available PE networks.
- **Matches** lists all occurrences of the selected VPN service. If you select a specific entry from this list, the associated container expands in the navigation pane and the item is made available in the status pane.

The Find dialog also contains the following buttons:

- **Close** closes the dialog.
- **Help** displays online help for the Find dialog.

## Component

The Component dialog displays the selection of Passport components that make up the selected basic service and the state of each of those components.

The Component dialog contains the following fields:

- **State** displays the state of each component as it is computed and propagated by the VPN Monitor Server. The VPN Monitor Server maintains the propagated states for basic service components using the NDAM state of the component and any parent components.
- **Component Name** displays the components of the selected basic service.

The Component dialog also contains the following buttons:

- **Close** closes the dialog.
- **Help** displays online help for the Component dialog.

Selecting a component in this dialog puts the component in context for use with other MDM tools that also support context.

Right-clicking a component opens a pop-up menu that lets you start other MDM fault, performance, and system tools in context of the selected component.

## Procedures

The VPN Monitor tool lets you monitor Passport IP VPN services. The tool monitors, calculates, and displays the status of basic services. Based on these state values, you can further diagnose problems and take corrective action. This section contains the following VPN Monitor procedures:

### Starting and stopping the VPN Monitor tool

- “Starting VPN Monitor from the MDM toolset” (page 208)
- “Starting VPN Monitor from the command line” (page 209)
- “Quitting VPN Monitor” (page 210)

### Getting online help

- “Displaying VPN Monitor online help” (page 211)

### Modifying the VPN Monitor window

- “Opening pop-up menus” (page 212)
- “Adjusting pane sizes” (page 213)
- “Displaying or hiding the tool bar” (page 214)

### Working with basic services and service clusters

- “Navigating the VPN” (page 215)
- “Displaying service view components” (page 216)
- “Displaying basic service components” (page 217)
- “Finding basic services or service clusters in the provider edge network” (page 218)

### Starting other MDM tools

- “Starting other MDM tools from VPN Monitor” (page 219)

## Starting VPN Monitor from the MDM toolset

VPN Monitor lets you monitor Passport IP virtual private network (VPN) services.

When the VPN Monitor client starts, it uses the server on the host specified in the Service Selection dialog box. For situations where you need to restart VPN Monitor, ensure the appropriate host is specified in the Server Selection dialog box before you start VPN Monitor.

### Prerequisites

Before you can start VPN Monitor, the following items must be up and running:

- MDM Administration Database  
For details, see 241-6001-400 *Preside MDM Administration Database User Guide*.
- VPN Monitor Extractor  
For details, see 241-6001-310 *Preside MDM Server Reference Guide*.
- VPN Monitor Server  
For details, see 241-6001-310 *Preside MDM Server Reference Guide*.

### Procedure steps

- 1 In the Preside Multiservice Data Manager window, select **Fault** and then **VPN Monitor**.  
  
The **Configuration Synchronizing** dialog opens and displays the status of the configuration loading process.
- 2 When the **Configuration Synchronizing** dialog indicates that the configuration has finished loading (configuration loaded), click **OK**.  
  
The dialog closes and the **VPN Monitor** window is populated with VPN information.

## Starting VPN Monitor from the command line

VPN Monitor lets you monitor Passport IP virtual private network (VPN) services.

When the VPN Monitor client starts, it uses the server on the host specified in the Service Selection dialog box. For situations where you need to restart VPN Monitor, ensure the appropriate host is specified in the Server Selection dialog box before you start VPN Monitor.

### Prerequisites

Before you can start VPN Monitor, the following items must be up and running:

- MDM Administration Database  
For details, see 241-6001-400 *Preside MDM Administration Database User Guide*.
- VPN Monitor Extractor  
For details, see 241-6001-310 *Preside MDM Server Reference Guide*.
- VPN Monitor Server  
For details, see 241-6001-310 *Preside MDM Server Reference Guide*.

### Procedure steps

- 1 From the UNIX command line, type the following command:  

```
/opt/MagellanNMS/bin/VPNMonitorClient
```

The Configuration Synchronizing dialog opens and displays the status of the configuration loading.
- 2 When the **Configuration Synchronizing** dialog indicates that the configuration has finished loading (configuration loaded), click **OK**.  

The dialog closes and the **VPN Monitor** window is populated with VPN information.

## Quitting VPN Monitor

Use this procedure to quit the VPN Monitor tool.

### Procedure steps

- 1 From the **File** menu, select **Exit**.  
The VPN Monitor window closes.

## Displaying VPN Monitor online help

Use this procedure to view online help for the VPN Monitor tool. You can display various types of online help.

### Procedure steps

#### Help On Context

Help on Context displays online information about a specific area of the VPN Monitor window.

- 1 From the **Help** menu, select **On Context**.

The mouse pointer changes to a question mark (?).

- 2 Move the mouse pointer onto an area of the window for which you want help and click the mouse button.

The online help window opens with information specific to the area you selected.

#### Help on Window

Help on Window provides a description of the elements of the VPN Monitor window.

- 1 From the **Help** menu, select **Help on Window**.

The online help window opens with a description of the Passport Shelf View window.

## Opening pop-up menus

Pop-up menus are visible when you right-click on services in the VPN Monitor window. These pop-up menus provide additional commands that are specific to the selected area of the window. Use this procedure to open a pop-up menu.

### Procedure steps

- 1 Right-click any basic service or service cluster in the navigation, status, or recent events pane.  
A pop-up menu opens.
- 2 Select a command from the pop-up menu.  
The command executes and the pop-up menu closes.

## Adjusting pane sizes

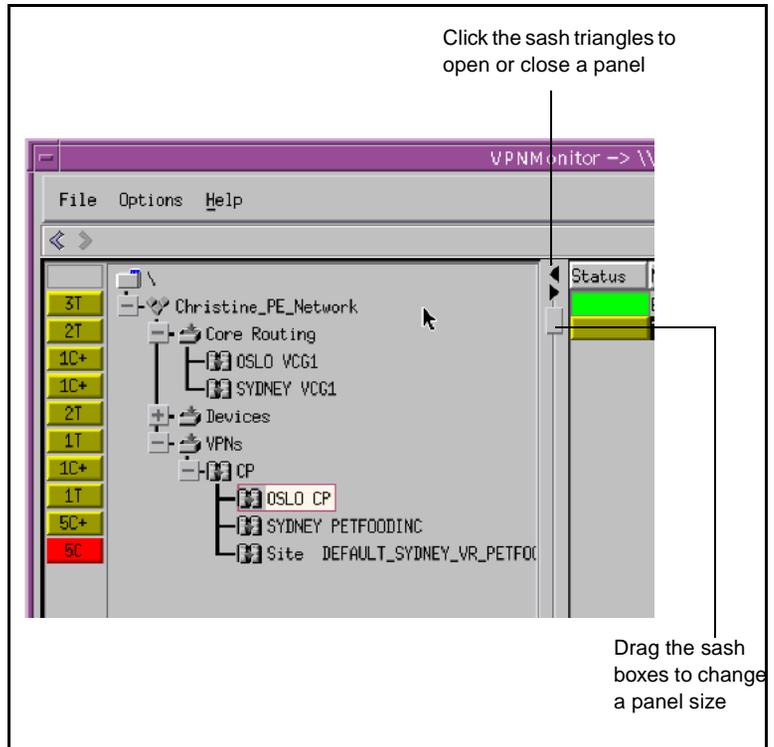
The VPN Monitor contains various panes. You can adjust these pane sizes. Any adjustments that you make remain in effect until you readjust the settings or until you close the window. Use this procedure to adjust the sizes of these panes

### Procedure steps

- 1 To adjust the height or width of a pane, drag the box in the sash to the desired location.

When you move a sash to increase the amount of space in one pane, the space for the other panes decreases correspondingly.

- 2 To open or close a pane, click the triangles in the sash.



## Displaying or hiding the tool bar

You can display or hide the VPN Monitor tool bar.

### Procedure steps

- 1 Use one of the following methods:
  - To hide the tool bar, from the **Options** menu, click to select the **Standard Tool bar** option.
  - To display the hidden tool bar, from the **Options** menu, click to clear the **Standard Tool bar** option.

## Navigating the VPN

The navigation pane represents the hierarchical structure of the VPN. Use this procedure to navigate the VPN service views.

### Procedure steps

- 1 All unexpanded components in the navigator pane display with a plus (+) sign. To expand the component, click the plus sign (+) adjacent to the component you want to expand.

When the component expands, the plus sign changes to a minus sign (-).

- 2 To compress subcomponents, click the minus sign (-) adjacent to the parent component.

## Displaying service view components

You can display the components and their associated states of views, service clusters, and basic services.

### Procedure steps

- 1 Select any entry in the navigation panel.

The states for the selected entry and its associated subcomponents display in the status pane.

## Displaying basic service components

You can display the Passport components that comprise a basic service.

### Procedure steps

- 1 Select an entry from the navigation panel that displays basic services in the status pane.
- 2 In the status pane, right-click the basic service for which you want to display Passport components.

A pop-up menu opens.

- 3 From the pop-up menu, select **Show Components**.

The Components dialog opens and displays the Passport components that comprise the basic service as well as the state of each component.

## Finding basic services or service clusters in the provider edge network

You can search for all occurrences of a specific basic service or service cluster in the provider edge (PE) network.

### Procedure steps

- 1 Use any of the following methods:
  - In the navigation pane, right-click any entry in the core routing, devices, or VPNs service view.
  - In the status pane, right-click a basic or service cluster.
  - In the recent event pane, right-click a basic serviceA pop-up menu opens.
- 2 From the pop-up menu, select **Find**.

The Find dialog opens and displays the selected service name, the scope, and all occurrences of the selected service in the PE network
- 3 Optionally, you can search another PE networks or search all PE networks by selecting an entry from the drop-down list in the **Scope** field.

## Starting other MDM tools from VPN Monitor

The VPN Monitor tool provides a selection of fault capabilities. To perform additional fault, configuration, and performance tasks, you can start other tools from the Passport Shelf View.

### Procedure steps

- 1 From the navigation panel, select an entry that displays basic services in the status pane.
- 2 Right-click a basic service entry in the status pane and from the resulting pop-up menu, select **Show Components**.

The **Components** dialog opens and displays a list of the basic service components.

- 3 Select an entry in the **Components** dialog and then right-click to open a popup menu.
- 4 From the pop-up menu, select an MDM fault, performance, or system tool.

The MDM tool opens in the context of the selected component.



---

## Chapter 5

# Alarm Display

---

This section describes the Alarm Display and provides you with instructions on how to use this tool. The following information is included:

- “Alarm Display overview” (page 222)
- “Alarm Display formats” (page 222)
- “Common alarm format” (page 222)
- “Viewing alarms in the Active mode” (page 226)
- “Clearing active alarms for DPN” (page 229)
- “Clearing active alarms for Passport” (page 230)
- “Viewing alarms in the Log mode” (page 236)
- “Displaying Customer Database Information” (page 242)
- “Keyboard shortcuts” (page 244)
- “Filtering alarms” (page 245)
- “Setting alarms by effects” (page 254)
- “Starting another tool” (page 256)
- “Customizing Alarm Display Start Tool submenus” (page 256)
- “Saving and viewing Alarm Display files” (page 259)
- “Customizing resources” (page 262)
- “Command line arguments” (page 264)

## Alarm Display overview

The Alarm Display provides a list of logs and active alarms in the network. It lets you view alarms received from Passport, DPN and selected SNMP devices in a single window. You can use the Alarm Display in conjunction with other surveillance tools to isolate faults in your network.

You access the Alarm Display tool from the Fault toolset in the Preside MDM window. The Alarm Display provides two modes of operation: Active and Logs. The Alarm Display displays all alarms (notably those from Passport and DPN switches) in a common format. You can launch Alarm Display with an Active Alarm List or a window that displays a log of all alarms received.

## Alarm Display formats

Although alarms sent by Passport and DPN switches differ, the Alarm Display can display alarms from both networks. The Alarm Display displays active alarms and logs for Passport and DPN in common format.

The following example illustrates the different alarm formats in terse mode.

### Common format:

```
CRITICAL SET 09990001 98-03-03 16:57:16 EM/NODER8.
```

## Common alarm format

Passport switch alarms are shown in common format. The table “Common alarm severity mapping” (page 222) shows the mapping between the Preside Multiservice Data Manager (MDM) Alarm Display common alarm severities and Passport switch severities.

**Table 34**  
**Common alarm severity mapping**

MDM Alarm Display common alarm severity label	Passport switch severity label	DPN switch severity label
CRITICAL	Critical	Major
MAJOR	Major	Minor
(Sheet 1 of 2)		

**Table 34 (continued)**  
**Common alarm severity mapping**

MDM Alarm Display common alarm severity label	Passport switch severity label	DPN switch severity label
MINOR	Minor	
CLEAR	Clear	Wildcard
WARNING	Warning	Degrade, Overload
UNKNOWN	Indeterminate	others
(Sheet 2 of 2)		

## Syntax styles

You can control the amount of information each alarm displays on the screen. The Alarm Display offers three syntax styles: terse, normal and full.

### Terse

Terse syntax displays alarm information on a single line. Long component identifiers are truncated to fit on the single line. Terse format contains the following fields:

- common severity (see the table “Common alarm severity mapping” (page 222))
- event (SET, MSG, or CLR)
- fault code
- date
- time
- component identifier (long component identifiers are terminated with ‘...’ to indicate a truncated line)

The format for terse format is as follows:

```
<severity><event><fault code><date><time><comp ID>
```

#### Example

```
CRITICAL SET 09990001 98-03-03 16:57:16 EM/NODER8.
```

**Normal**

Normal syntax style displays an intermediate amount of alarm information on multiple lines.

The first part of normal syntax contains all of the fields of terse syntax. However normal syntax does not truncate long component identifiers and, as a result, may occupy more than one line.

The second part of normal syntax contains the notification ID, alarm type, and probable cause of the alarm.

The last part of normal syntax contains lines with the labeled comment data and the operator data fields. These lines may, or may not, be present depending on the availability of this information.

The format for normal syntax is as follows:

```
<severity><event><fault code><date><time><comp ID>  
<n lines wrapped for component identifier if necessary>  
<ID:notification ID><TYPE:type><CAUSE:probable cause>  
[CO:<commentData>] [OP:<operatorData>]
```

**Example**

```
CRITICAL SET 09990001 98-03-03 16:57:16 EM/NODER8  
ID: FFFFFFFF TYPE:equipment CAUSE: equipmentFailure  
CO: NMS:bcary9b0 has lost connectivity to this node.
```

**Full**

Full syntax displays complete information on alarms. This syntax style displays a variable number of lines depending on the origin of the alarm (DPN or Passport) and the specific content of the received alarm (for example, the presence or absence of expert, comment, and operator data).

The first part of full syntax contains all of the fields of terse syntax. However, full syntax does not truncate long component identifiers and, as a result, may occupy more than one line.

The second part of full syntax contains the notification ID, alarm type, and probable cause of the alarm.

The last part of full syntax contains lines with labeled fields. These lines may, or may not, be present.

The format for full syntax is as follows:

```
<severity><event><fault code><date><time><comp ID>
<n lines wrapped for component identifier if necessary>
<ID:notification ID><TYPE:type><CAUSE:probable cause>
[CO:<commentData>] [OP:<operatorData>]
[EX: <expertData>]
RAW: <raw>
ADMIN:<admin state> OPER:<operational state>
USAGE:<usage state>
AVAIL:<availability> PROC:<procedural status>
CNTRL:<control status>
ALARM:<alarm status> STBY:<standby status> UNKNW:
<unknown status>
[REL COMP:<related component identifier one line per
related component>]
[INT:<process id>; <filename>; <line number>;
<version>]
[CDB:<customer database information>]
```

#### Example

```
CRITICAL SET 09990001 98-03-03 16:57:16 EM/NODER8
ID: FFFFFFFF TYPE:equipment CAUSE: equipmentFailure
CO: NMS:bcary9b0 has lost connectivity to this node.
RAW:unk ADMIN:unlocked OPER:disable USAGE:idle
      AVAIL:          PROC:          CNTRL:
      ALARM:          STBY:notSet UNKNW:
INT: ;;;;
```

## Alias substitution for component names

The Alarm Display provides an option that lets you substitute an alias for the component name when displaying alarms. This function is an extension of the Customer Database (CDB) support. To use the alias function, you need to customize the tool's Motif resources. To enable alias substitution set the `cdbSupportAlias` resource to a value of `True`. For details, see "Resources for color control of common alarm formats by Alarm Display" (page 263).

When you enable support for alias substitution, the CDB Preferences Dialog box opens with an additional checkbox—Display component ID alias from CBC server. Use this checkbox to turn alias substitution on or off in Alarm Display.

When alias substitution is turned on, the component name is replaced by the alias in the Customer Database's Related Component field. The alias displays in all alarm formats. However, a new second line displays in the normal and full formats to indicate the real component name. For more information, see "Displaying Customer Database Information" (page 242).

## Viewing alarms in the Active mode

The Active mode shows the SET alarms for which there is no corresponding CLEAR. The display is auto refreshed at a default rate of once every minute; it removes cleared alarms and inserts new SET alarms. You can turn the auto refresh off and refresh the display as needed by pressing the *Refresh* button.

*Note:* If more than 500 SET alarms are received with the *Auto Refresh* turned off, it automatically resets to *On* and forces a refresh of the display.

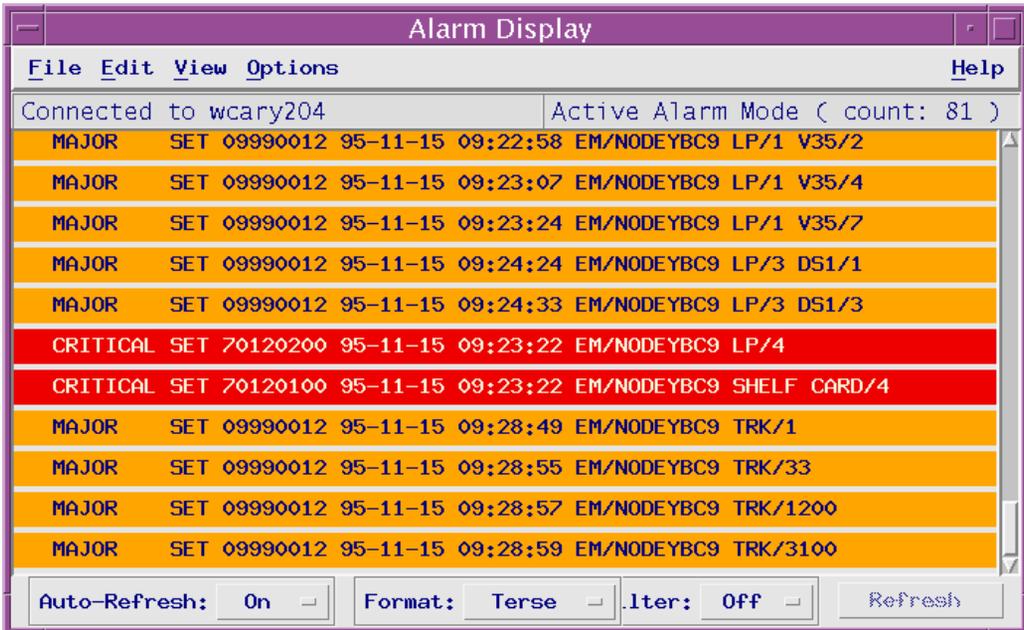
You can perform the following actions in Active mode:

- Double click on an alarm to change the alarm display format. For details on alarm displays, see "Syntax styles" (page 223).
- Press the Shift key and double click on an alarm to change the alarm display format to full syntax. For details on full syntax, see "Syntax styles" (page 223).
- Press the Control key and double click on an alarm to acknowledge or unacknowledge an alarm. For details on acknowledging and unacknowledging alarms, see "Acknowledging and Unacknowledging Alarms" (page 238).
- Select an alarm and press the up or down arrow key to scroll through the list of alarms displayed on the screen.

## Viewing alarms in the Active Alarm mode

- 1 In the Preside MDM window, select Fault -> Alarm Display: Active.

The Alarm Display main window opens. The main window contains a menu bar, an alarm scrolling window, and a set of toggle buttons at the bottom of the window. Below the menu bar, the name of the host to which you are connected and the number of active alarms are displayed. A Refresh button at the bottom of the window lets you refresh the display manually at any time.



- 2 Select *Auto-Refresh: Off* if you do not want to refresh the display automatically.
 

**Note:** Accelerator keys are available for all display toggle buttons. See the table “Accelerator keys” (page 245).
- 3 Select *Set Full Format*, *Set Normal Format*, or *Set Terse Format* to view selected alarms in the format you want; or choose a format from the option menu that appears when you click the *Format* button at the bottom of the display. If you use the option menu to set the format, all displayed and new alarms are reformatted in the new format (see “Full” (page 224), “Normal” (page 224), and “Terse” (page 223)).
- 4 Select *Filter: On* to filter Active incoming alarms (see “Filtering alarms” (page 245)).

- 5 To view the alarm in the log mode select *Select Log Mode* from the View menu.
- 6 To paste selected alarm information to a text editor, select *Copy* from the *Edit* menu.  
**Note:** To select multiple alarms, press the *Shift* key and hold the left mouse button to drag the cursor over the alarms you want.
- 7 Click *Refresh* to manually refresh the display.

## Clearing active alarms for DPN

You can clear DPN alarms locally and globally from the Alarm Display clear them out DMDR and GMDR databases locally on the workstation and/or globally through the DMA servers.

### Procedure

- 1 In the Preside MDM window, click **Fault**. Click **Alarm Display: Active**.  
The **Alarm Display** displays the current active alarms from the network.
- 2 Click on the alarms you want to clear. To select multiple alarms, hold down the *Control* key while you click the alarms.  
The selected alarms are highlighted.
- 3 Right-click and hold to display the **Alarm Menu** pop-up menu.
- 4 You can clear alarms from several different menu selections:
  - While holding down the right-mouse button, select **Local Clear** or **Global Clear** and then release the mouse button.
  - While holding down the right-mouse button, select **Start Tool -> Fault-> Global Clear of Alarm** and then release the mouse button.

If you are globally clearing alarms, a dialog box is displayed asking “Are you sure you want to clear the alarm(s)?” Select *Yes* if you are sure you want to globally clear the alarm. Select *No* if you do not want to clear the alarm

**Note:** **Global Clear** only clears DPN and Passport alarms.

- 5 Click **Refresh** or wait for the next refresh period for alarms to disappear.  
If one or more requests failed, a dialog box opens with the error messages.

### Expected results

- If you clicked **Local Clear**, the alarm is cleared from the GMDR/DMDR/FMDR/SMDR/IMDR database.
- If you clicked **Local Clear** or **Global Clear**, your userID, hostname, and the “DISPLAY” environment variable value will be displayed in the comment data of the resulting **Clear Alarm**.

- If you clicked **Global Clear**, the alarm is cleared from the GMDR/DMDR database and from the active alarm list stored on the OA in the network.

## Clearing active alarms for Passport

You can clear Passport alarms locally and globally from the Alarm Display and clear them out of the FMDR and GMDR databases locally on the workstation and/or globally from the devices. See the following procedures:

- “Clearing a Passport alarm using Local Clear” (page 231)
- “Clearing a Passport alarm using Global Clear” (page 232)
- “Clearing a Passport alarm using the Global Clear tool” (page 233)

## Clearing a Passport alarm using Local Clear

You can clear Passport alarms locally from the Alarm Display to clear them from the MDM servers. This procedure is intended for any MDM operator and multiple alarms can be cleared at one time.

### Prerequisites

- The GMDR server must be up and running.

### Procedure

- 1 In the Preside MDM window, click **Fault**. Click **Alarm Display: Active**.

The **Alarm Display** displays the current active alarms from the network.

- 2 Click on the alarms you want to clear. To select multiple alarms, hold down the *Control* key while you click the alarms.

The selected alarms are highlighted.

- 3 Right-click and hold to display the **Alarm Menu**

- 4 pop-up menu.

- 5 Select **Local Clear** and then release the mouse button.

A Confirmation dialog box is displayed asking “You are about to clear the selected alarm(s) locally from MDM. Are you sure you want to clear the alarm(s)?” Select *Yes* if you are sure you want to locally clear the alarms. Select *No* if you do not want to clear the alarms.

- 6 Click **Refresh** or wait for the next refresh period for alarms to disappear.

### Expected results

- The alarm is cleared from the GMDR/FMDR databases.
- Your userID, hostname, and the “DISPLAY” environment variable value will be displayed in the comment data of the resulting **Clear Alarm**.

## Clearing a Passport alarm using Global Clear

You can clear Passport alarms globally from the Alarm Display to clear them out of the MDM servers and the on-switch databases. This procedure is intended for any MDM operator and multiple alarms can be cleared at one time.

### Prerequisites

- Passport Global alarm clearing must be configured on the DMA server.
- The GMDR servers must be up and running.
- The GMDR server must be able to access a DMA server through its configuration.

### Procedure

- 1 In the Preside MDM window, click **Fault**. Click **Alarm Display: Active**.  
The **Alarm Display** displays the current active alarms from the network.
- 2 Click on the alarms you want to clear. To select multiple alarms, hold down the *Control* key while you click the alarms.  
The selected alarms are highlighted.
- 3 Click the right mouse button and hold to display the **Alarm** pop-up menu.
- 4 Select **Global Clear** and then release the mouse button.  
A Confirmation dialog box is displayed asking “You are about to clear the selected alarm(s) globally from MDM and the device(s). Are you sure you want to clear the alarm(s)?” Select *Yes* if you are sure you want to globally clear the alarms. Select *No* if you do not want to clear the alarms.
- 5 Click **Refresh** or wait for the next refresh period for alarms to disappear.  
If one or more requests failed, a dialog box opens with the error messages.

### Expected results

- Your userID, hostname, and the “DISPLAY” environment variable value will be displayed in the comment data of the resulting **Clear Alarm**.
- The alarm is cleared from the GMDR/FMDR databases and from the active alarm list stored on the Passports in the network.

## Clearing a Passport alarm using the Global Clear tool

You can clear a Passport alarm globally from the Alarm Display to clear it out of the MDM servers and the on-switch database. This procedure requires that the MDM operator set up connection authentication first. Only one alarm can be cleared at a time.

### Prerequisites

- The Host Group Directory Services (HGDS) server and the Passport Comms Mgr server (FDTM) must be up and running.

### Procedure

- 1 In the Preside MDM window, click **Fault**. Click **Alarm Display: Active**.

The **Alarm Display** displays the current active alarms from the network.

- 2 Click on the alarm you want to clear.

The selected alarm is highlighted.

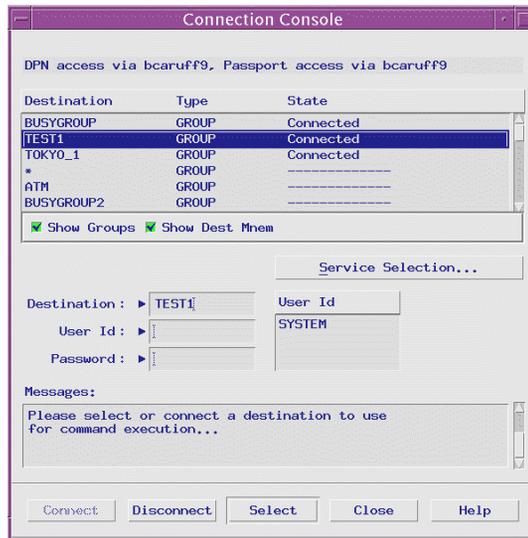
- 3 Click the right mouse button and hold to display the **Alarm** pop-up menu.

- 4 Select **Start Tool -> Fault -> Global Clear of Alarm** and then release the mouse button.

A Confirmation dialog box is displayed asking “You are about to clear the selected alarm(s) globally from MDM and the device(s). Are you sure you want to clear the alarm(s)?” Select *Yes* if you are sure you want to globally clear the alarm. Select *No* if you do not want to clear the alarm.

The **Connection Console** dialog box opens and displays the first Passport group to which the node belongs. The **Connection Console**

dialog box does not display if you are already connected to a group that contains the Passport.



- 5 Connect to a destination. Use the default selected destination or select another destination.
- 6 Type a valid user ID in the **User Id** text box.
- 7 Type a valid password in the **Password** text box.  
You can repeat steps 5-7 as often as needed.
- 8 Click **Connect**.
- 9 Select a connected destination using one of the following steps:
  - Double-click on a connected network destination in the **Destination** list.
  - Select a connected network destination in the **Destination** list and then click **Select**.
  - Select the Passport wild-card route (\*). The wild card lets you direct commands to Passport nodes in any of the connected groups without having to know which group the node belongs to.

If the request failed, a dialog box opens with the error message.

**Expected results**

- Your userID, hostname, and the “DISPLAY” environment variable value will be displayed in the comment data of the resulting **Clear Alarm**.
- The alarm is cleared from the GMDR/FMDR databases and from the active alarm list stored on the Passport in the network.

## Viewing alarms in the Log mode

When the Alarm Display tool is in the Log mode, the SET, CLR, and MSG alarms are shown as they are asynchronously received.

Passport babbler alarms are always kept by Preside Multiservice Data Manager (MDM). A babbler alarm is defined as a SET alarm generated by the switch, without a corresponding CLR alarm. The babbler alarms carry a different notification ID but the same component ID, the same fault code, and the same alarm severity as the previous SET alarms they are duplicating. In the case of successive SET alarms, FMDR retains the latest received alarm, and previous alarms become historical alarms. By default, DPN babbler alarms are discarded by MDM. To enable DPN babbler alarms, run the DMDR server with the -B option. For information on the DMDR server startup options, see 241-6001-310 *Preside MDM Server Reference Guide*.

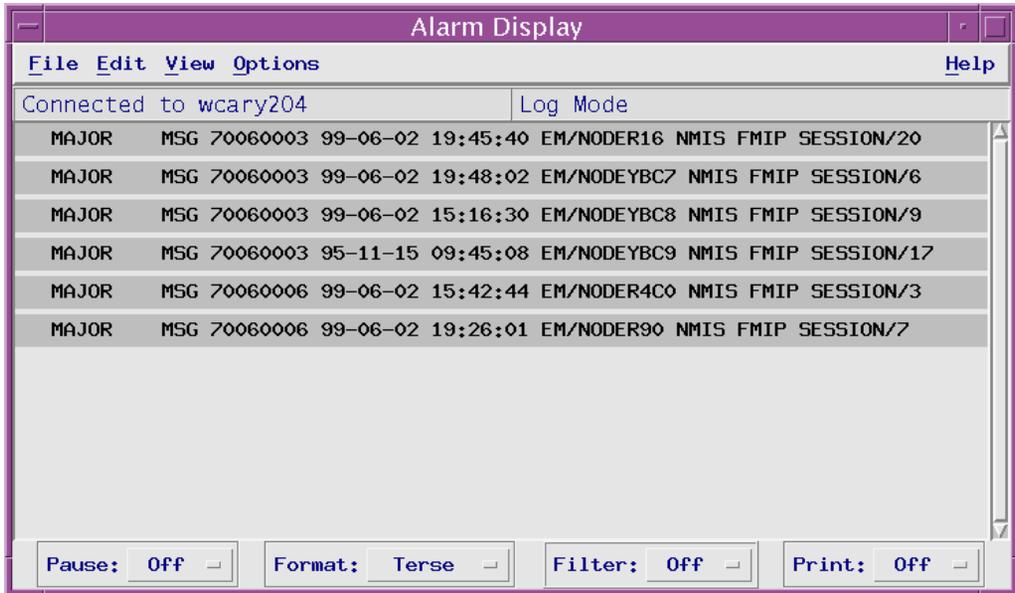
You can perform the following actions in Log mode:

- Double click on an alarm to change the alarm display format. For details on alarm displays, see “Syntax styles” (page 223).
- Press the Shift key and double click on an alarm to change the alarm display format to full syntax. For details on full syntax, see “Syntax styles” (page 223).
- Press the Control key and double click on an alarm to acknowledge or unacknowledge an alarm. For details on acknowledging or unacknowledging alarms, see “Acknowledging and Unacknowledging Alarms” (page 238).
- Select an alarm and press the up or down arrow key to scroll through the list of alarms displayed on the screen.

## Viewing alarms in Log mode

- 1 In the Preside MDM window, select Fault -> Alarm Display: Log.

The Alarm Display window opens.



- 2 To turn the display of incoming messages on or off, click the Pause button and select On or Off from the popup menu.
- 3 Set the alarm format display using one of the following methods:
  - a. Double-click on an alarm to change its format. All subsequent alarms display in the selected format.
  - b. Right-click on an alarm to open the popup Log Menu. From the Log menu, select Set Terse Format, Set Normal Format, or Set Full Format. All subsequent alarms display in the selected format.
  - c. Click the Format button and select Terse, Normal, or Full format. All subsequent alarms display in the selected format.
- 4 To turn alarm filters on or off, click the Filter button and select On or Off from the popup menu.
- 5 To print alarms as they are received at the workstation, click the Print button and select On or Off from the popup menu.
- 6 To view alarms in active mode, from the View menu, select Select Active Alarm Mode.

- 7 To paste selected alarm information to a text editor, from the Edit menu, select Copy.

**Note:** To select multiple alarms, press the *select* mouse button and drag the cursor over the alarms. To select non-contiguous alarms, hold down the *Control* key and use the *select* mouse button.

## Acknowledging and Unacknowledging Alarms

You can acknowledge or unacknowledge a set of selected active alarms from the Alarm Display by invoking the *Acknowledge/Unacknowledge Alarm(s)* Dialog from the *Active Alarm List* pop-up menu. Acknowledging and unacknowledging alarms is permitted only in the Active mode.

### Acknowledging active alarms

- 1 From the *Active Alarm List* pop-up menu, select a set of alarms to be acknowledged.
- 2 Using the *select* mouse button, invoke the alarm pop-up menu and choose the *Acknowledge Alarms...* option.
- 3 When the *Alarm Acknowledgment* Dialog appears, enter a reason for the action and a userid (if the system administrator enables changes to this value). The default is `<UnixUserID>@<Hostname>`.
- 4 Ensure that you select only those alarms that you wish to acknowledge, then select the *Ack* button.

Acknowledged alarms are displayed with a checkmark icon on the left, both in Active mode and Log mode, even though alarms can only be acknowledged from Active mode. The date/time of the acknowledgment, the userid, and the reason associated with each alarm are shown when displaying alarms in full format.

### Unacknowledging active alarms

- 1 From the *Active Alarm List* pop-up menu, select a set of alarms to be unacknowledged using the *select* button.
- 2 Using the *menu* button, open the alarm pop-up menu and choose the *Unacknowledge Alarms...* option.
- 3 When the *Alarm Acknowledgment* Dialog appears, enter a reason for the action and a userid (if the system administrator enables changes to this value). The default is `<UnixUserID>@<Hostname>`.
- 4 Ensure that you select only those alarms that you wish to unacknowledge; then select the *Unack* button.

Unacknowledged alarms are displayed with a crossed out checkmark icon on the left, both in Active mode and Log mode, even though alarms can only be unacknowledged from Active mode. The date/time of the unacknowledgement, the userid, and the reason text associated with each alarm are shown when displaying alarms in full format.

For information on the dialog used for acknowledging or unacknowledging alarms, see “Alarm acknowledgement and unacknowledgement” (page 275).

The figure “Active Alarm Display” (page 240) illustrates an example of the *Active Alarm Display* mode of the Alarm Display that contains acknowledged and unacknowledged alarms.

**Figure 24**  
Active Alarm Display



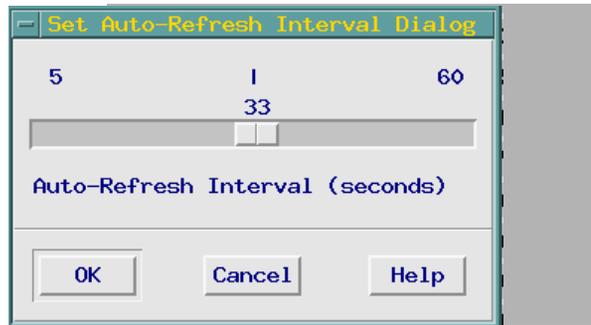
## Setting the Auto-Refresh interval

In the Active mode you can set the interval between display refreshes. This setting controls the time when new Active alarms are inserted or cleared alarms are removed from the display.

### Setting the Auto-Refresh interval

- 1 From the Options menu, select Set Auto-Refresh Interval.

The Set Auto-Refresh Interval dialog appears.



- 2 Use the slider to set the interval and press the *OK* button.

The Set Auto-Refresh Interval dialog disappears. The display is automatically refreshed at the chosen interval if you press the *Auto-Refresh On* toggle button.

## Sorting by time and by component id

You can choose to sort the alarm list in the Active Alarm display mode by component identification or by time.

### Sorting the Active Alarm List

- 1 If you want the list ordered by component id, press *menu* on *View* in the Alarm Display main window and choose *Sort by Component Id*.

The alarm list is sorted by component id. New incoming alarms are inserted into the list in component id order.

If you want to sort the alarm list by time with the most recent alarms appended at the bottom of the list, press *menu* on *View* in the Alarm Display main window, and choose *Sort by Time*.

The Active Alarm List is sorted by time with the most recent alarms appearing at the bottom of the list. After the initial sorting, new alarms are

simply appended at the bottom of the display with no sorting. You can use the Resort Displayed Alarms item from the View menu to resort the alarms in time order.

## Displaying Customer Database Information

By default, the Alarm Display does not display customer database information. You can, however, override this default and control the display of customer data in alarms by using the Set CDB Preferences Dialog. See “Setting customer database preferences” (page 242).

Enabling the display of customer data in alarms can help you diagnose faults. When you do enable the display, the Alarm Display shows information on an alarm’s component ID from a customer database server. You can view this information in the full common alarm format (for both the Active and Logs mode) in the “CDB:” tagged field. For more information on common alarms, see “Common alarm format” (page 222). For details on how to setup and populate a customer database server, see 241-6001-804 *Preside MDM Workstation Utilities User Guide*, “Customer Data Tool”.

**Note:** Populate the customer database with information in the display component ID format. For example, use the format EM/NODE1 LP/0 rather than EM NODE1 LP 0.

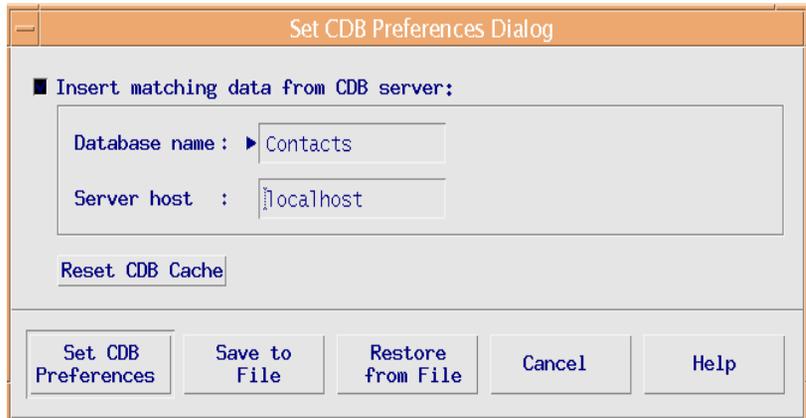
Alarm Display provides an option that lets you use alias substitution for component names. To do so, you must first turn on the support for this capability by modifying the Motif resource files (see “Alias substitution for component names” (page 225)). When support has been enabled, you can use the CDB Preferences Dialog control whether or not to display the alias in Alarm Display.

### Setting customer database preferences

- 1 From the Options menu, select Set CDB Preferences.

The Set CDB Preferences dialog opens.

**Figure 25**  
**Set CDB Preferences Dialog**



- 2 Click *Insert matching data from CDB server* to enable the option.  
 The Database name and Server host fields are enabled.
- 3 If you have enabled support for alias substitution, an additional checkbox displays in the dialog—Display component ID alias from CDB server. Select the checkbox to turn on the alias function. To turn off the alias function, click to clear the checkbox.
- 4 Enter a customer database name in the Database name field; enter a server host name in the Server host field.
- 5 Click *Save to File* to preserve the CDB preferences for later use.  
 The Alarm Display saves the settings to the file `$HOME/MagellanNMS/IADCdbPrefs.cfg`.  
 The next time Alarm Display is started, these settings will be used.
- 6 Click *Set CDB Preferences* to activate the preferences.  
 The Set CDB Preference Dialog closes and the Alarm Display activates the preferences. If you have enabled the display of customer database information and the Alarm Display is able to communicate with the server, the Alarm Display displays the database name and host in the Alarm Display's connection status field.

### Restoring customer database preferences

If you have previously saved your preferences in a file, you can restore them for later use.

- 1 In the Set CDB Preferences Dialog, click *Restore from file*.

The Alarm Display restores the last saved preferences from the file *\$HOME/MagellanNMS/IADCdbPrefs.cfg*.

- 2 Click *Set CDB Preferences* to activate the preferences.

The Set CDB Preference Dialog closes and the Alarm Display activates the preferences. If you have enabled the display of customer database information and the Alarm Display is able to communicate with the server, the Alarm Display displays the database name and host in the Alarm Display's connection status field.

### Resetting the customer database information cache

To reduce the communication costs with the Customer Database server, the Alarm Display maintains a cache of the latest information fetched. This cache may need to be reset if, for example, the Customer Database has been updated with new information.

- 1 In the Set CDB Preferences Dialog, click *Reset CDB Cache* to reset the customer database information cache.

The customer database information cache is reset.

### Exiting without saving customer database preferences

- 1 Click *Cancel*.

The dialog closes without saving any changes to the current CDB preferences.

### Displaying help on Set CDB Preferences Dialog

- 1 Click *Help* to display information on the Set CDB Preferences Dialog.

Online help is displayed.

## Keyboard shortcuts

The table “Accelerator keys” (page 245) lists the accelerator keys for the Alarm Display.

**Table 35**  
**Accelerator keys**

Mode	Function			
Logs Mode	Pause	Format	Filter	Print
	Ctrl+s (on)	Ctrl+t (terse) Ctrl+m (normal)	Ctrl+y (on)	Ctrl+p (on)
	Ctrl+q (off)	Ctrl+u (full)	Ctrl+n (off)	Ctrl+o (off)
Active Alarm Mode	AutoRefresh	Format	Filter	
	Ctrl+s (off)	Ctrl+t (terse) Ctrl+m (normal)	Ctrl+y (on)	
	Ctrl+q (on)	Ctrl+u (full)	Ctrl+n (off)	

## Filtering alarms

The Alarm Display Filter Dialog defines the conditions that alarms need to meet to be reported in the Alarm Display main display. Use the filter dialog to define filter characteristics, save or restore filter settings, and apply defined filter characteristics to the Alarm Display main display.

### Defining filters

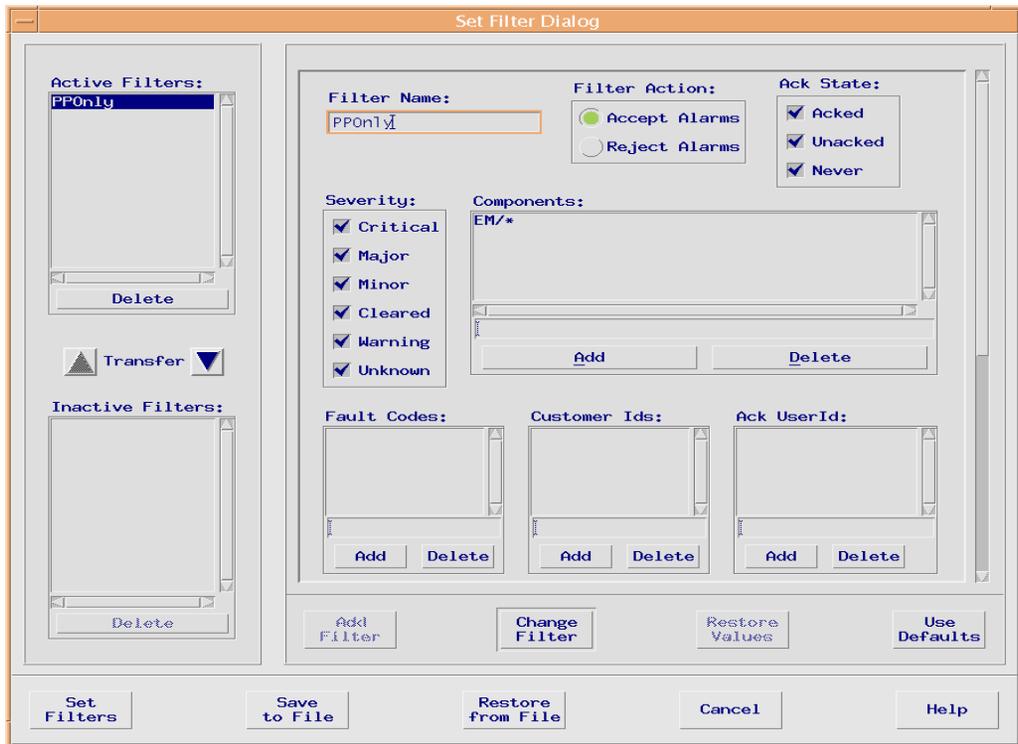
You can define alarm filters according to severity, component ID, fault code, and customer ID. Filter action is defined as either Accept or Reject. Alarms are reported through Accept filters if they meet defined criteria; Reject filters block the display of alarms having the characteristics you define. For example, you can filter the Alarm Display main display by accepting critical and major alarms from component PM/R66, and rejecting minor and cleared alarms from this component or other specified components. You can combine up to 10 accept and reject filters to screen alarms.

#### Defining your first filter

- 1 From the Options menu, select Set Filter.

The Set Filter Dialog opens.

**Figure 26**  
**Set Filter Dialog**



- 2 In the Filter Name field, enter a filter name.
- 3 In the Filter Action area, click *Accept* or *Reject*.  
 Accept passes alarms matching the criteria you specify to other control areas of this dialog. Reject blocks the display of alarms matching the criteria you specify.
- 4 In the Ack State area, click the acknowledge states that you want.
- 5 In the Severity area, click the alarm severities that you want.  
 The alarm severities are displayed or blocked, based on the selected Filter Action.
- 6 In the Components field, enter a component identifier (ID) and click *Add* to add components to the list. To delete a component from the list, select the component ID that you want to delete and click *Delete*.

**Note 1:** The Alarm Display supports two wildcard characters for the component ID—the asterisk (\*) and the question mark (?). The \* matches any string including a null string. For example, the component pattern PM/R66\* retrieves alarms from all modules and their subcomponents whose names start with R66. This wildcard might include such modules as R66WEST, R662, and R66A. The ? matches any single character. For example, the component pattern PM/R66? retrieves alarms from all modules and their subcomponents whose names start with R66 and are 4 characters long. This wildcard might include such modules as R662 and R66A.

To get alarms for a single module and its subcomponents, you need to use two patterns. For example, to get alarms for PM/R66 and its subcomponents, the first pattern, PM/R66, retrieves the alarms on the module. The second pattern, PM/R66 \*, retrieves alarms on the subcomponents. Note the presence of the blank space in the second pattern.

You can use more than one pattern matching character in the component ID field. For example, you can use the component ID pattern PM/R66\* PO/\* to filter the port alarms on PM/R66. You need to use the display name of the component ID, for example PM/R66, since the Alarm Display does not accept PM R66.

**Note 2:**

You can use up to 40 patterns in the *Components* list. Set this maximum by changing the following resource in your resource file:  
*IAD\*maxNumberOfComponentPatternsPerFilter.*

- 7 In the Fault Codes field, enter a fault code name and click *Add* to add a fault code value to the list. To delete fault code values from the list, select the fault code name that you want to delete and click *Delete*.

**Note 1:** The Alarm Display supports two wildcard characters for the Fault Code. The asterisk (\*) matches any string including a null string. The question mark (?) matches any single character. For example, the fault code pattern 30\* retrieves all alarms with a fault code beginning with 30. You can use more than one pattern matching character in the fault code field.

**Note 2:** You can use up to 40 patterns in the Fault Code lists. To set this maximum, change the following resource in your resource file:  
*IAD\*maxNumberOfFaultCodePatternsPerFilter.*

- 8 In the Customer IDs field, enter a customer ID and click *Add* to add a customer ID to the list. To delete a customer ID from the list, select the customer ID that you want to delete and click *Delete*.

**Note:** You can use up to 40 numbers in the *Customer Ids* list. To set this maximum, change the following resource in your resource file:  
*AD\*maxNumberOfCustomerIdNumbersPerFilter.*

- 9 In the Ack Userid field, enter a userid and click *Add* to enter a userid. To delete an ack userid from the list, select the userids you want to delete and click *Delete*.

**Note 1:** The Alarm Display supports two wildcard characters for the Ack Userid. The asterisk (\*) matches any string including a null string. The question mark (?) matches any single character. For example, the Ack userid pattern *dmei\** retrieves all alarms that are acked or unacked by user *dmei*, regardless of which workstation is used. The default Ack Userid is *<UnixUserID>@<Hostname>*. You can use more than one pattern matching character in the Ack Userid field.

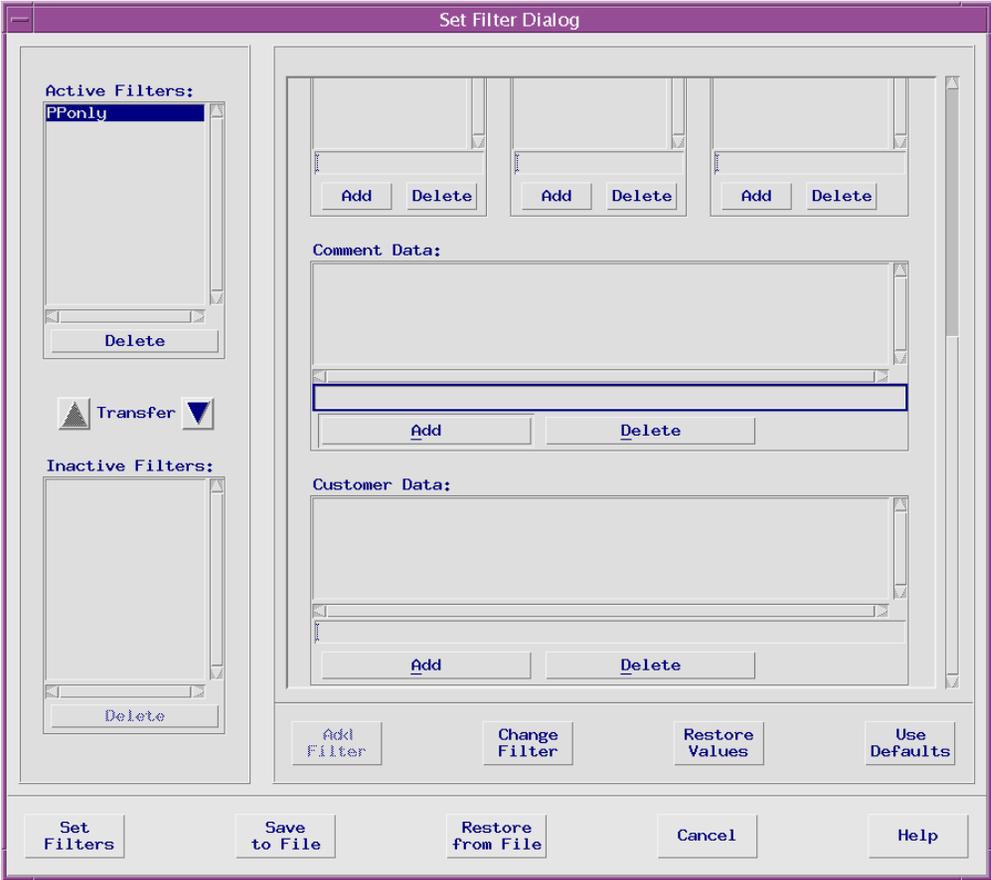
**Note 2:** You can use up to 40 patterns in the *Ack Userid* list. To set this maximum, change the following resource in your resource file:  
*IAD\*maxNumberOfAckUserIdsPerFilter.*

- 10 Click *Add Filter* to add your new filter. You can also change the values for your filter. See “Changing a filter” (page 250).

The filter name appears in the Inactive Filters list area on the left side of the dialog. An inactive filter is one that is not used by the Alarm Display when you select the filtering option.

- 11 Scroll down the Set Filter Dialog to see the remainder of the dialogue.

Figure 27  
Set Filter Dialog (Continued)



- 12 In the Comment Data field, enter a pattern and press *Add* to add comment text patterns to the list. To delete a pattern from the list, select the pattern you want to delete and click *Delete*.

**Note 1:** The Alarm Display supports two wildcard characters for Comment Data. The asterisk (\*) matches any string including a null string. The question mark (?) character matches any single character.

**Note 2:** You can use up to 40 patterns in the Comment Data list. Set this maximum by changing the following resource in your resource file: *IAD\*maxNumberOfComponentPatternsPerFilter*.

- 13 In the Customer Data field, enter a pattern and click *Add* to add customer data patterns to the list. To delete a pattern from the list, select the pattern you want to delete and click *Delete*.

**Note 1:** The Alarm Display supports two wildcard characters for Customer Data. The asterisk (\*) matches any string including a null string. The question mark (?) matches any single character.

**Note 2:** You can use up to 40 patterns in the Customer Data list. Set this maximum by changing the following resource in your resource file:  
*IAD\*maxNumberOfComponentPatternsPerFilter*.

- 14 Click *Save to File* to save your filters.
- 15 Select the filter that you want from the *Inactive Filters* list and click the left transfer arrow to make the filter active.

The filter moves to the Active Filters list and is used to filter alarms.

- 16 Click *Set Filters* to close the dialog and apply the filter.

The Set Filter Dialog closes. If the Filter On option is enabled in the Alarm Display main dialog, the filter settings are applied.

### Changing a filter

- 1 From the Options menu, select Set Filter.

The Set Filter Dialog opens.

- 2 Select a filter from the *Active Filters* or *Inactive Filters* list.

The Filter Name field updates with the name of the selected filter. The corresponding filter attributes are displayed

- 3 Change any attributes and click *Change Filter*.

- 4 Click *Set Filters*.

If you change an active filter, the changes are applied to this session. If you change an inactive filter, the changes are not applied to this session. An inactive filter is not used by the Alarm Display when the filtering option is enabled.

**Note:** Active filter settings apply when the *Filter On* option of the Alarm Display main window is enabled. If the *Filter Off* option is enabled, active filters are not applied to the current session.

- 5 Click *Save to File* to save your filters to a file.

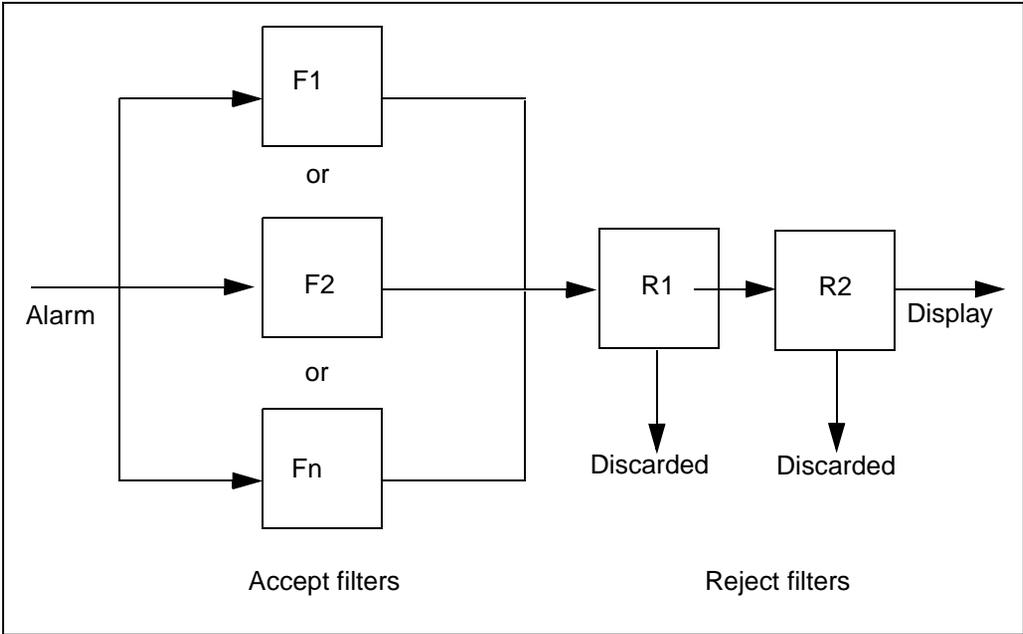
All filters are saved to a file. The next time the Alarm Display is started, alarms are filtered accordingly.

### Applying filters

You can apply your filters to the Alarm Display main display after you define them.

The figure “Filtering process” (page 251) illustrates the filtering process. The Alarm Display shows an alarm if it matches the conditions of at least one Accept filter; it blocks the display of an alarm if it matches the conditions of one Reject filter. Alarm Display uses a two-stage filtering process. First, accept the alarm types you want displayed, and then reject a subset of the accepted alarms that you do not want to see in the Alarm Display main display.

**Figure 28**  
**Filtering process**



You can combine up to 10 Active filters in any combination of Accept or Reject filters. To set this maximum, change the *AD\*maxNumberActiveFilters* resource in your resource file.

### Applying filters

- 1 From the Options menu, select Set Filter.

The Set Filter Dialog opens. The Active Filters area displays the names of any filters currently running.

- 2 To remove filters from the *Active Filters* or *Inactive Filters* lists, select them and press the *Delete* button.
- 3 To change the attributes of a filter, select it and press the *Change Filter* button.

The Filter Name field is updated with the name of the selected filter, and the other selector fields show the attributes of this filter. Change the attributes for your filter by repeating the procedure in “Defining your first filter” (page 245).

- 4 If you make changes to a filter and want to see the original parameters, press the *Restore Values* button.

The filter appearing in the Filter Name area reverts to its original specifications.

- 5 Use the *Transfer* arrow buttons to move selected filters between the *Active Filters* and *Inactive Filters* lists.

- 6 If you want to save your new filter set to a file, press the *Save to File* button.

The filters you define are saved to file; filters appearing in the *Active Filter* area control the Alarm Display the next time you invoke the Alarm Display tool. For more information about Alarm Display filter files, see “Saving filters” (page 253).

- 7 Press the *Set Filters* button to run the filters named in the *Active Filters* list.

Alarms in the Alarm Display main display are filtered based on the criteria you define. If the Alarm Display is running in Logs mode, only new incoming alarms are displayed using your selected filters. If the Alarm Display is running in the Active Alarms mode, the Alarm Display main display is refreshed using your selected filters.

- 8 Press *Close* if you do not want to save your changes.

The main Alarm Display display is shown. If the filter option is On, the display is filtered by the filter set in the Active Filters list.

---

## Saving filters

After you define a set of filters, you can save them to a file. Saved filters are automatically restored when you start the Alarm Display. Filters are stored in your *\$HOME/MagellanNMS* directory under the following names: *ADActiveModeFilterDpn.cfg* (outdated), *ADActiveModeFilter.cfg*, *ADLogModeFilterDpn.cfg* (outdated), and *ADLogModeFilter.cfg*. Each filter is defined by a separate record and each record is separated by a blank line. A filter must contain a filter name, the action it performs, and its activity.

This is an example of a filter set in the Log mode:

```
FILTERNAME: x
ACTION: ACCEPT
ACTIVE: TRUE
SEVERITY:CRITICAL
SEVERITY: MAJOR
SEVERITY: MINOR
SEVERITY: CLEARED
COMPONENT: PM/R66*
FAULTCODE:1*
CUSTOMERID:1
ACKSTATE: acked
ACKUSERID: dmei

FILTERNAME: xx
ACTION: REJECT
ACTIVE: TRUE
SEVERITY: CRITICAL
SEVERITY: MAJOR
SEVERITY: MINOR
SEVERITY: CLEARED
COMPONENT: PM/R66 PE/2*
FAULTCODE: 1*
CUSTOMERID: 1
ACKSTATE: acked
ACKUSERID: dmei
```

### Maintaining a filter library

- 1 Use the *Save to File* button to save filters named in the *Active Filters* and *Inactive Filters* lists to your user config file.

The next time you run the Alarm Display, alarms are filtered accordingly. To run your new set of filters immediately, press the *Apply Filters* button. The main Alarm Display is shown and your filters determine the information that appears there.

- 2 If you make changes to your filter set and want to see which filters were running the Alarm Display when you started, press the *Restore from File* button.

The Alarm Display Set Filter dialog is refreshed to show your original Active and Inactive filter sets.

- 3 To clone the attributes of a filter, select it.

The filter name appears in the *Filter Name* field, and its attributes are displayed in the other control fields of the dialog.

- 4 Enter a new name for the filter in the *Filter Name* field and change the attributes.

- 5 Press the *Add Filter* button.

The filter from which you clone the attributes appears in the *Inactive Filters* list under the new name. The original filter is preserved in the list from which you select it.

- 6 Press the *Save to File* button if you want to save your new filter.

## Setting alarms by effects

Alarm conditions may be set for specific visual effects or audible effects. You can modify these settings through the *Set Effects* dialog.

### Setting alarm effects for visual and audible monitoring

- 1 From the Options menu, select *Set Effects*.

The Set Effects Dialog opens.



- 2 Select from the *Bell* area the values required for an alarm to sound the bell.

**Note:** The bell selector is not available in the *Active* mode.

- 3 Select from the *Highlight* area the values required to have an alarm displayed with a colored background.

- 4 Select *Save to File* to save the selected settings to file.

The settings are saved. The changes are not applied and the dialog remains open.

- 5 Select *Set Effects* to apply the changes.

The dialog is closed. The selected filter settings are applied to the main window display if you select the *Bell Effect On* or *Highlight Effect On* in the menu bar *View* menu.

Depending on the operational mode, the effects settings are applied as follows:

- In the *Active* Mode, the effect settings are applied to both existing and incoming set alarms.
- In the *Log* Mode, only incoming set alarms are affected.

**Note:** To activate or deactivate *Highlight* or *Bell* mode, select from the *View* menu.

- 6 To display the effects you saved, use the *View* menu. *Turn Bell On* or *Turn Highlight On* for a display of the saved effects.
- 7 If you want to update the dialog with the contents of the last saved effect settings select *Restore from File*.

- 8 Select *Cancel* to dismiss the dialog.

Any changes that you make to the effect settings are lost if you do not save before choosing this action.

- 9 Select *Help* to receive online help for any dialog setting.

## Starting another tool

- 1 Position the mouse pointer on any alarm in the Alarm Display alarm list and press the mouse menu button.

A pop-up menu opens.

- 2 From the pop-up menu, select *Start Tool*.

A submenu opens listing the categories of tools from which you can make a selection.

- 3 From the submenu, select an appropriate category.

A list of available tools and utilities for that category opens.

- 4 From the list, select a tool or utility.

The selected item opens.

For details on individual tools and utilities, see the appropriate Preside Multiservice Data Manager (MDM) documentation.

## Customizing Alarm Display Start Tool submenus

You can customize the contents of the Start Tool menu in the active and log mode. For procedures on customizing the Start Tool menu, see the section on customizing the toolsets and Start Tool menus section in 241-6001-301 *Preside MDM Customization Administrator Guide*.

When you modify the Start Tool menu file, use one of the following substitution variables in the command line:

- \$COMP: the component's internal representation
- \$DCOMP: the component's display name
- \$SEVERITY: the Common severity, which can be UNKNOWN, CRITICAL, MAJOR, MINOR, WARNING, or CLEARED
- \$DPNSEV: the DPN severity, which can be DEGRADE, OVERLOAD, MINOR, MAJOR, WILDCARD, CRITICAL, or OTHER

- **\$EVENT:** CLEAR, SET, or MSG
- **\$DPNMNEM:** the Network Control System (NCS) condition mnemonic, which can be TRAPDATA, ACTIVATE, INVALID, MISSING, DUPLICAT, MEMORY, CONJEST, FAILED, REFUSED, TIME\_OUT, CRITICAL, OOS, THRESHLD, ENABLED, DISABLED, PROBE, CALL\_BLK, or DISCARD
- **\$DPNACTION:** the NCS action value, which can be ncsServiceData, ncsHardwareFault, ncsSoftwareFault, ncsSecurityViolation, ncsProtocolViolation, ncsDebugInfo, ncsNetwork, ncsEngineering, ncsUnclassified, or ncsOperations. This value is an empty string for Passport-originated alarms.
- **\$FCODE:** the alarm fault code. The fault code is an 8-digit code used to specify the alarm. The first 4 digits are used to identify the source of the alarm, and the last 4 digits are used to identify the alarm.
- **\$DATE:** the date information in the format 'year:month:day'
- **\$TIME:** the time information in the format 'hour:min:sec'
- **\$DTYPE:** the DPN device type. This value is an empty string for Passport-originated alarms.
- **\$FORMAT:** the present format of an alarm, which can be TERSE, NORMAL, or FULL
- **\$RAWSTATE:** the Raw state, which can be insv, oos, trb, unk, nex, or nea. This value is an empty string for DPN-originated alarms.
- **\$TYPE:** the alarm type, which can be communications, qualityOfService, processing, equipment, environment, security, operator, debug, or unknown. This value gives a general explanation of the cause of the alarm.
- **\$CMT:** the operator comment data text
- **\$OPER:** the operator data text

**Example:**

If you want to invoke the tool called Customer Tool Kit Script with the component id and the fault code contained in the alarm, add the following two lines to the `/opt/MagellanNMS/IADAlarm.menu` file. The CustomerToolKitScript script is called with this information when you use the Start Tool submenu and select the Customer Tool Kit Script:

- `labelString: Customer Tool Kit`
- `tMCommandLine: CustomerToolKitScript COMP:"$COMP"  
DCOMP:" FAULTCODE:"$FCODE"`

## Passing component information from Alarm Display to Component Information Viewer

You can pass component context information from the Alarm Display to the Component Information Viewer.

- using the *Start Tool* command
- using the *Auto Context* function from the Component Information Viewer

### Passing component information if the Component Information Viewer is not already running

- 1 In the Preside MDM window, select Fault -> Alarm Display.

The Alarm Display window opens, displaying the current alarms or logs from the network.

- 2 Position the mouse pointer over the alarm you want to investigate from the list shown and press the mouse menu button.

A pop-up menu opens.

- 3 On the pop-up menu, select Start Tool -> Fault -> Component Information Viewer.

The component is identified from the selected alarm information. A new Component Information Viewer window with Auto Context active is created with the component ID information. You can investigate further using the Component Information Viewer functions.

### Passing component information if the Component Information Viewer is running with Auto Context on

- 1 Select the alarm in the Alarm Display that you want.

The information for the component in the selected alarm is pasted into the Component Information Viewer window.

**Note:** In a drag selection, only the last selected alarm is passed to the Component Information Viewer.

### **Passing component information if the Component Information Viewer is running with Auto Context off**

- 1 Select the alarm in the Alarm Display that you want.

The selected alarm is highlighted.

**Note:** In a drag selection, only the last selected alarm is passed to the Component Information Viewer.

- 2 Switch to Component Information Viewer, position the mouse pointer on the *Related Components for or Information for* text field selector and press the mouse menu button.

A pop-up menu opens.

- 3 From the pop-up menu, select *Get Context*.

The component is identified from the selected alarm information and is pasted into the Component Information Viewer window.

## **Saving and viewing Alarm Display files**

You can save the information displayed by the Alarm Display to a file and also view saved files. The appearance and control areas differ slightly depending on whether you are in Active Alarms or Logs mode.

For situations in which you do not wish to have an operator logged in to the Alarm Display Tool, there is another way to extract alarms from **Preside Multiservice Data Manager (MDM)** with the *rnclarm* utility. For information about this utility, see the section on extracting alarms in text format in 241-6001-301 *Preside MDM Customization Administrator Guide*.

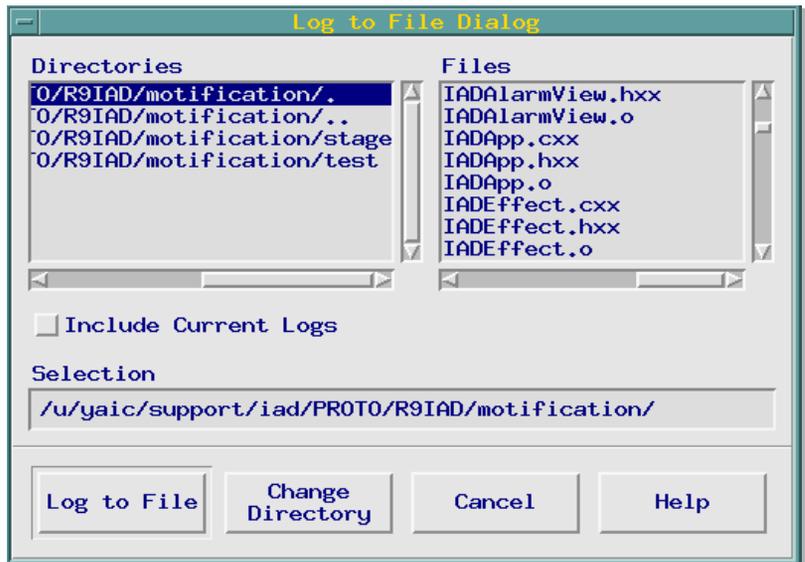
See the following procedures:

- “Saving Alarm Display information to a file” (page 260)
- “Viewing an Alarm Display log file in active mode” (page 260)
- “Viewing an Alarm Display log file in log mode” (page 261)

## Saving Alarm Display information to a file

- 1 From the Active mode File menu, select Save Active Alarms to File... or from the Log mode File menu, select Log to File....

A file selection dialog opens.



- 2 Select a directory and file from the lists in the dialog, or type a filename in the Selection field.
- 3 In active mode, click the Save Active Alarms button, or in log mode click the Log to File button.
- 4 From log mode, you have the option of saving new logs to your file. To do so, click the Include Current Logs button.

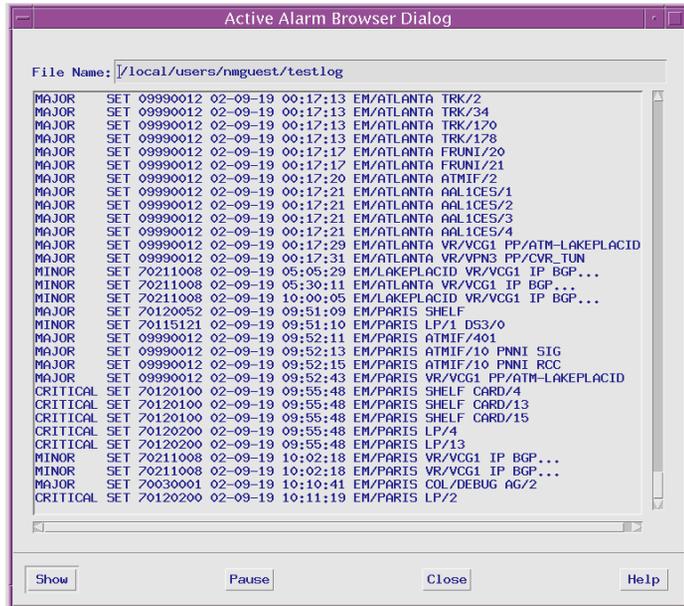
## Viewing an Alarm Display log file in active mode

- 1 From the active alarm mode File menu, select View Active Alarms File.

The View Active Alarms File Dialog opens.

- 2 In the View Active Alarms File Dialog, select the appropriate directory and file name from the lists, or type the complete path name in the Selection field.
- 3 Click View Active Alarms File.

The **Active Alarm Browser Dialog** opens.



- 4 To pause the display of incoming alarms, click **Pause**.

A red outline surrounds the log information and the label on the **Pause** button changes to **Resume**.

- 5 To resume the display of paused alarms, click **Resume**.

- 6 To refresh the display of alarms with the current content of the log file, click **Show**.

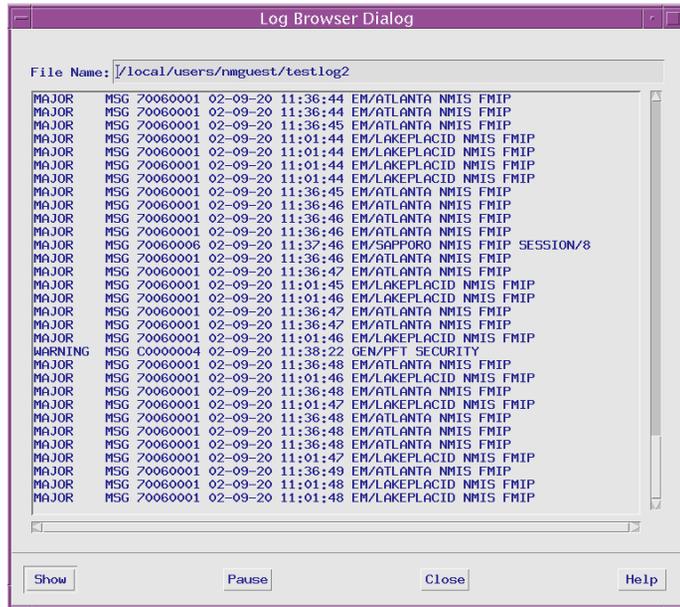
## Viewing an Alarm Display log file in log mode

- 1 From the log mode **File** menu, select **View Log File**.

The **View Log File Dialog** opens.

- 2 In the **View Log File Dialog**, select the appropriate directory and file name from the lists, or type the complete path name in the **Selection** field.
- 3 Click **View Log File**.

The **Log Browser Dialog** opens.



- 4 To pause the display of incoming alarms, click **Pause**.

A red outline surrounds the log information and the label on the **Pause** button changes to **Resume**.

- 5 To resume the display of paused alarms, click **Resume**.

- 6 To refresh the display of alarms with the current content of the log file, click **Show**.

## Customizing resources

You can customize the resources to control the colors of the alarm format by severity. You can also customize the resources to control whether the problem states are shown in the related components list, and to control whether the bell rings upon error.

The table “Resources for color control of common alarm formats by Alarm Display” (page 263) lists the resources you use to control the colors associated with the common alarm format severity displayed by the Alarm Display components.

**Table 36**  
**Resources for color control of common alarm formats by Alarm Display**

Resource	Description	Legal value
*BackgroundColorUnknown *ForegroundColorUnknown *BackgroundColorCritical *ForegroundColorCritical *BackgroundColorMajor *ForegroundColorMajor *ForegroundColorMinor *BackgroundColorMinor *BackgroundColorWarning *ForegroundColorWarning *BackgroundColorCleared *ForegroundColorCleared *BackgroundColorDefault *ForegroundColorDefault	Specifies the background and foreground color-to-severity mappings for the common alarm formats.	Any legal X windows color or specification. See 241-6001-301 <i>Preside MDM Customization Administrator Guide</i> .
IAD*cdbSupportAlias	Enables support for Customer Database component name aliasing.	True to enable alias support, False (default) to prevent alias support

The table “Resources for customizing the Acknowledge/Unacknowledge Alarms Dialog” (page 264) lists the resources you use to customize the *Acknowledge Alarms* Dialog and the *Unacknowledge Alarms* Dialog.

**Table 37**  
**Resources for customizing the Acknowledge/Unacknowledge Alarms Dialog**

Resource	Description	Legal value
*AckAlarmDlog*userIdFieldField.editable	If True, the <i>User</i> field in the dialog used for acknowledging or unacknowledging alarms can be modified. The default is False.	True or False
*AckAlarmDlog*commentData.maxLength	The maximum length of <i>Reason</i> text that can be specified when acknowledging or unacknowledging alarms. The default length is 256.	Any legal <i>Motif</i> value associated with the <i>MaxLength</i> resource.

## Command line arguments

The table “Command line arguments” (page 264) lists the Command line arguments for the Alarm Display.

**Table 38**  
**Command line arguments**

Command line	Description
[ -h <host> ]	The name of the remote host on which the General Manager Data Router (GMDR) is running. If a surveillance service selection exists, the default is the selected host; otherwise, the default is the local host.
[ -c ]	If you are in the Active mode, the initial sorting is by component id. The default is by time.
[ -s <GMDR> ]	The name of the GMDR server from which you want to extract data. The default is GMDR.
(Sheet 1 of 2)	

**Table 38 (continued)**  
**Command line arguments**

Command line	Description
[ -r <number> ]	The maximum number of active alarms that the Alarm Display buffers when the <i>Auto-Refresh</i> option is deactivated. The default is 500.
[ -b <number> ]	The maximum number of logs that the Alarm Display buffers while the <i>Pause</i> option is activated. The default is 500.
[ -a <number> ]	The maximum number of logs that Alarm Display keeps in the Log mode window. The default is 500.
[ -o <DPN> ]	DPN mode only. It displays DPN alarms in NCS format. The default is Passport- and DPN-originated alarms in <i>common</i> format. This is now outdated.
[ -m [ACTIVE   LOG] ]	Can be Log or Active mode. The default is Log mode.
[ -w <number> ]	The time interval between refreshes of the Log display. The default is two seconds.
(Sheet 2 of 2)	



## Chapter 6

# Alarm Help

---

This section describes Alarm Help, a utility that lets you view alarm code descriptions on the workstation. This chapter contains the following:

- “About Alarm Help” (page 267)
- “Alarm help window” (page 268)
- “Starting Alarm Help” (page 269)
- “Stopping Alarm Help” (page 269)
- “Searching for an alarm code” (page 270)
- “Searching for a text string” (page 270)
- “Viewing alarm codes from Alarm Display or Component Information Viewer” (page 271)
- “Adding and editing alarm codes” (page 271)

### About Alarm Help

Alarm Help is a utility that lets you view alarm code descriptions for the following:

- DPN devices
- Passport devices
- Preside Multiservice Data Manager (MDM) proxy alarms
- SNMP-supported devices

In addition, you can use Alarm Help to add and edit your own user-defined alarm code descriptions.

The documents that are available in Alarm Help are:

- 241-1001-506 *DPN-100 Alarm Console Indications* contains DPN alarms
- 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms* contains Passport alarms
- 241-6001-501 *Preside MDM Proxy Alarms Reference Guide* contains MDM proxy alarms
- 241-6001-502 *Preside MDM Device Alarms Reference Guide* contains alarms for SNMP devices supported by MDM

See also...

- “Alarm help window” (page 268)
- “Starting Alarm Help” (page 269)
- “Searching for an alarm code” (page 270)
- “Searching for a text string” (page 270)
- “Viewing alarm codes from Alarm Display or Component Information Viewer” (page 271)
- “Adding and editing alarm codes” (page 271)

## Alarm help window

When you start Alarm Help, a Netscape browser opens and displays the alarm in context. The alarm in context is the last alarm that was selected from the Alarm Display or Component Information Viewer tool. If no alarm is in context when you start Alarm Help, the top of the Alarm Console Indications document displays in the window. After you start Alarm Help, the contents of the window update automatically as the alarm in context changes.

Alarm Help has the following buttons:

- **Reset**  
returns you to the top of the Alarm Console Indications document when you have been doing other viewing or searching.

**Note:** By default the word Introduction is displayed in the text entry field because that is the first text found.

- Text entry field  
lets you type in an alarm code or other text that you want searched.
- Search Alarm  
initiates a search for an alarm code.
- Search Text  
initiates a search through the alarm documents for a specific text string.
- Add/Edit  
lets you add you own alarm code descriptions to Alarm Help and edit them.

The Alarm Help window has the following areas:

- a navigation area on the left that contains a table of contents.
- a view area on the right that contains the text of the alarm documents.

See also...

- “Searching for an alarm code” (page 270)
- “Searching for a text string” (page 270)
- “Adding and editing alarm codes” (page 271)

## Starting Alarm Help

- 1 On the Preside MDM window, select Fault -> Alarm Help

The Alarm Help window opens with the Introduction of the Alarm Console Indications document.

## Stopping Alarm Help

- 1 Use one of the following methods to stop Alarm Help:
  - Close the Netscape browser. Minimizing the window does not stop the alarm help display.
  - Select any context-sensitive help menu item.
  - Click any help button.

## Searching for an alarm code

You can search for a particular alarm code in Alarm Help. To do so, you need to specify all characters in the 8-digit code. You cannot search based on partial matches or wildcards.

- 1 Enter the 8-digit alarm code in the text entry field.

The fault code is eight hexadecimal digits entered as XXXX XXXX or XXXXXXXX.

- 2 Click the Search Alarm button.

If the alarm code is matched with one or more occurrences, all the occurrences are displayed in the navigation area. If no alarm code is matched, the words No matches is displayed.

You can replace any of the eight hexadecimal digits in the fault code with a wildcard character. Type the wildcard characters in the text entry field.

Valid wildcard characters are n, x, y, and z. These can take on the hexadecimal values of 0 (zero) through F. You can also use the question mark (?) as a wildcard character to replace a single digit, and the asterisk (\*) to replace a number of digits at the end of the alarm code.

See also...

- “Searching for a text string” (page 270)

## Searching for a text string

- 1 Type the text string, enclosed by single quotes, in the text entry field.

- 2 Click the Search Text button.

If the string is matched with one or more occurrences, all the occurrences of the text string will appear in the navigation area. If the text string cannot be matched, the phrase No Matches is displayed in the view area.

**Note:** Matched strings can occur both in headings and in any other text within a document.

See also...

- “Searching for an alarm code” (page 270)

---

## Viewing alarm codes from Alarm Display or Component Information Viewer

- 1 If Alarm Help is not running, open Alarm Help:
  - a. Select an alarm in Alarm Display or Component Information Viewer.
  - b. With the right mouse button, select Start Tool.
  - c. From the Start Tool menu, select Alarm Help.
- 2 Select the alarm code you want to view.

The text for the selected alarm code will be displayed in Alarm Help.

## Adding and editing alarm codes

Alarm Help allows you to add alarm code descriptions. You can add a new alarm code or you can reuse an existing alarm code. You can also edit or delete alarm code descriptions.

*Note:* If you add or modify alarm code descriptions in the Online Documentation (UNIX) and then switch to Online Documentation (Web), the revisions may not be available to Online Documentation (Web). If this occurs, use the following procedure:

- 1 Type

```
/etc/init.d/jtomcatctl404 stop
/etc/init.d/jtomcatctl404 start
```
- 2 Restart MDM.

See also...

- “Adding a description for a new alarm code” (page 271)
- “Adding a description using an existing alarm code” (page 272)
- “Editing an alarm code description” (page 273)
- “Deleting an alarm code description” (page 273)

### Adding a description for a new alarm code

- 1 Enter a new alarm code in the text entry field.

The code should consist of eight hexadecimal digits. Make sure the code does not conflict with any other alarm codes.

The SNMP Surveillance Adapter has a CD (customer-defined) labelling feature. If you enter only six digits, CD is automatically added to the start of the six-digit code. For example, **123456** becomes **CD 123456**. This CD label helps to ensure that the alarm code will not conflict with any other alarm code.

If you enter eight digits, CD is not added to the start of the alarm code. Make sure the code does not conflict with any other alarm codes.

**Note 1:** The CD labelling feature is unique to the SNMP Surveillance Adapter. This feature does not apply to the SNMP Integrator.

**Note 2:** The first two numbers should match the device type value for the device being managed.

- 2 Click the Add/Edit button.

The Edit Alarm Text window is displayed with the new alarm code in the title bar of the window.

- 3 Type the text of the alarm code description in the window.
- 4 Click the Apply button.

The new alarm code is added to the end of the list in the navigation area.

## Adding a description using an existing alarm code

- 1 Select an existing alarm code:

Select an existing alarm code one of the following ways:

- Enter an existing alarm code in the text entry field as an eight hexadecimal digit. For example, enter **CD12 3456**, or **5004 0100**.
- Select an alarm code in the navigation area.

- 2 Click the Add/Edit button.

The Edit Alarm Text window is displayed with the existing alarm code in the title bar of the window.

- 3 Type the text of the alarm code description in the window.
- 4 Click the Apply button.

**Note:** You can only add user-defined alarm codes. If you use this procedure to edit an existing alarm code that was provided to you, a duplicate alarm code description will be created.

The new alarm code is added to the end of the list in the navigation area.

## Editing an alarm code description

- 1 Select an existing alarm code:

Select an existing alarm code one of the following ways:

- Enter the alarm code in the text entry field as an eight hexadecimal digit. For example, enter **CD12 3456**, or **5004 0100**.

Select an alarm code in the navigation area.

- 2 Click the Add/Edit button.

The Edit Alarm Text window is displayed with the existing alarm code in the title bar of the window.

- 3 Edit the text of the alarm code description in the window.
- 4 Click the Apply button.

## Deleting an alarm code description

- 1 Select an existing alarm code:

Select an existing alarm code one of the following ways:

- Enter the alarm code in the text entry field as an eight hexadecimal digit. For example, enter **CD12 3456**, or **5004 0100**.
- Select an alarm code in the navigation area.

- 2 Click the Add/Edit button.

The Edit Alarm Text window is displayed with the existing alarm code in the title bar of the window.

- 3 Click the Delete button.

A warning is displayed asking if you want to delete the alarm code description.

- 4 Click the Yes button to confirm you want to delete the alarm code description.

**Note:** You can only delete user-defined alarm code descriptions.



# Chapter 7

## Alarm acknowledgement and unacknowledgement

---

This section describes the alarm acknowledgement and unacknowledgement tools and includes procedures on how to use these tools. The following information is included:

- “Alarm Acknowledgement and Unacknowledgement overview” (page 275)
- “Acknowledging and unacknowledging single or multiple alarms” (page 276)
- “Changing state by acknowledging all active alarms on a component” (page 277)
- “Displaying Alarm Acknowledgment and Unacknowledgement information” (page 277)
- “Acknowledge Alarm(s) Dialog” (page 278)
- “Unacknowledge Alarm(s) Dialog” (page 279)
- “Alarm acknowledgement/unacknowledgement procedures” (page 281)
- “Customizing the Alarm Acknowledgment Dialog” (page 286)

### Alarm Acknowledgement and Unacknowledgement overview

The Alarm Acknowledgment tool lets you notify others that you are investigating a problem associated with one or more active alarms. When you no longer need alarms acknowledged, use the Alarm Unacknowledgement

tool. Rather than removing acknowledgement, the Alarm Unacknowledgement tool changes the acknowledged status to unacknowledged.

Alarm acknowledgment and unacknowledgement behave as a SET/REPLACE. For example, a previously unacknowledged alarm can be acknowledged using the SET operation; a currently acknowledged or unacknowledged alarm can be changed using the REPLACE operation.

For more details about Alarm Acknowledgement and Unacknowledgement, see, the following topics:

- “Acknowledging and unacknowledging single or multiple alarms” (page 276)
- “Changing state by acknowledging all active alarms on a component” (page 277)
- “Displaying Alarm Acknowledgment and Unacknowledgement information” (page 277)
- “Acknowledge Alarm(s) Dialog” (page 278)
- “Unacknowledge Alarm(s) Dialog” (page 279)
- “Alarm acknowledgment/unacknowledgement procedures” (page 281)
- “Customizing the Alarm Acknowledgment Dialog” (page 286)

## Acknowledging and unacknowledging single or multiple alarms

You can acknowledge or unacknowledge a selection of active alarms and you can acknowledge all alarms for a given component. To acknowledge and unacknowledge one or more active alarms, use the following commands available from MDM alarm-based fault management tools (for example, Alarm Display and Component Information Viewer):

- **Acknowledge Alarms** to acknowledge one or more selected active alarms
- **Unacknowledge Alarms** to remove acknowledgement from one or more selected acknowledged alarms

To acknowledge and unacknowledge all active alarms for a selected component, and optionally its related subcomponents, use the following commands from MDM state-based fault management tools (for example, Network Viewer and Component Information Viewer):

- **Acknowledge Alarms on Component** to acknowledge all active alarms for a selected component, and optionally its subcomponents.
- **Unacknowledge Alarms on Component** to unacknowledge any currently acknowledged alarms for a selected component.

For alarm acknowledgement and unacknowledgement procedures, see

- “Acknowledging selected active alarms” (page 282)
- “Unacknowledging selected active alarms” (page 284)
- “Acknowledging active alarms on selected components” (page 283)
- “Unacknowledging active alarms on selected components” (page 284)

## Changing state by acknowledging all active alarms on a component

The Alarm Acknowledgement and Unacknowledgement tool provides a link between alarm-based and state-based surveillance. Acknowledging all active alarms on a component masks the component state during propagation. When you acknowledge all active alarms on a component from an alarm-based tool such as Alarm Display, the propagated state of the component becomes acknowledged. The effect is similar to manually acknowledging a component state from a state-based tool such as the Network Viewer, where the raw state remains unchanged. For details, see the section on the General Management Data Router (GMDR) in 241-6001-310 *Preside MDM Server Reference Guide*.

## Displaying Alarm Acknowledgment and Unacknowledgement information

When you acknowledge or unacknowledge alarms, a dialog opens and displays the user ID from which the acknowledge or unacknowledge request was made and prompts for the reason for the request. Displaying alarm information in full format from the Alarm Display or Component Information Viewer tool includes the user ID, time, and reason for acknowledgement or

unacknowledgement. Acknowledged alarms in Alarm Display and Component Information Viewer display with checkmark to the left of the alarm. Unacknowledged alarms display with an X on top of the checkmark.

## Acknowledge Alarm(s) Dialog

The Acknowledge Alarm(s) Dialog is used to acknowledge one or more active alarms.

The figure “Acknowledge Alarm(s) Dialog for selected active alarms” (page 278) illustrates an Acknowledge Alarm(s) Dialog for selected active alarms.

**Figure 29**  
Acknowledge Alarm(s) Dialog for selected active alarms



The data entry fields for the Acknowledge Alarm(s) Dialog are as follows:

- *User* indicates the identifier stored as part of the alarm (the person associated with the acknowledgment or unacknowledgement). This value is non-editable (by default) but can be made editable through the resource modification described in “Customizing the Alarm Acknowledgment Dialog” (page 286).

- *Reason* specifies the reason for the acknowledgment and is stored as part of the alarm. You can enter text description of up to 256 characters (maximum allowable length by default). You can alter the maximum allowable length for the reason text through the resource modification described in “Customizing the Alarm Acknowledgment Dialog” (page 286). If you select a single alarm that was previously acked or unacked, the reason text associated with that alarm automatically appears by default. You can delete this text by typing new text, or you can modify it by clicking the text using the left mouse button.

The Acknowledge Alarms Dialog has the following buttons:

- *Ack Alarms* sends an *ackAlarm* request to the General Management Data Router (GMDR) server for each selected active alarm (if this dialog is invoked from an alarm list menu item) or for every active alarm for the current component (if this dialog is invoked from a toolset menu item)
- *Cancel* ignores the request and pops down the dialog.
- *Help* displays information about Alarm Acknowledgment and Unacknowledgement.

The following button is displayed only when you acknowledge all active alarms on a selected component using the Start Tool menu item:

- *Also ack all alarms on related sub-components* allows you to perform a hierarchical alarm acknowledgment to acknowledge all active alarms on the component you select and on any of its subcomponents.

## Unacknowledge Alarm(s) Dialog

The UnAcknowledge Alarm(s) Dialog is used to unacknowledge one or more active alarms.

The figure “UnAcknowledge Alarm(s) Dialog for selected active alarms” (page 280) illustrates a sample Unacknowledge Alarm(s) Dialog for selected active alarms.

**Figure 30**  
**UnAcknowledge Alarm(s) Dialog for selected active alarms**



The data entry fields for the Unacknowledge Alarm(s) Dialog are as follows:

- *User* indicates the identifier stored as part of the alarm (the person associated with the acknowledgment or unacknowledgement). This value is non-editable (by default) but can be made editable through the resource modification described in “Customizing the Alarm Acknowledgment Dialog” (page 286).
- *Reason* specifies the reason for the unacknowledgement and is stored as part of the alarm. You can enter text description of up to 256 characters (maximum allowable length by default). You can alter the maximum allowable length for the reason text through the resource modification described in “Customizing the Alarm Acknowledgment Dialog” (page 286). If you select a single alarm that was previously acked or unacked, the reason text associated with that alarm automatically appears by default. You can delete this text by typing new text, or you can modify it by clicking the text using the left mouse button.

The Unacknowledge Alarms Dialog has the following buttons:

- *UnAck Alarms* sends an *ackAlarm* request to GMDR for each selected active alarm (if this dialog is invoked from an alarm list menu item) or for every active alarm for the current component or subcomponent (if this dialog is invoked from a toolset menu item).
- *Cancel* ignores the request and pops down the dialog.
- *Help* displays information about Alarm Acknowledgment and Unacknowledgement.

The following is displayed only when you unacknowledge all active alarms on a selected component using the Start Tool menu item:

- *Also unack all alarms on related sub-components* allows you to perform a hierarchical alarm unacknowledgement to unacknowledge all the active alarms on the component you select and on any of its subcomponents.

## Alarm acknowledgment/unacknowledgement procedures

To perform other Alarm Acknowledgment tasks, see

- “Acknowledging selected active alarms” (page 282))
- “Acknowledging active alarms for selected components” (page 282))
- “Unacknowledging selected active alarms” (page 284))
- “Unacknowledging active alarms on selected components” (page 284))

### Starting Alarm Acknowledgment

Alarm Acknowledgment is started from the Acknowledge Alarm(s) Dialog under the following conditions:

- on a set of selected active alarms from within the Alarm Display. See “Alarm Display” (page 221).
- on a set of selected active alarms from within the Component Information Viewer. See “Acknowledging active alarms” (page 369).
- on a selected component from within the Network Viewer. See “Network Viewer” (page 51).
- on a selected component from within the Component Status Display. See “Component Status Display” (page 397).

- on a selected component from within the Network Status Bar. See “Network Status Bar” (page 289).
- on a selected component from within the Component Information Viewer. See “Acknowledging active alarms” (page 369).

These scenarios cause an *ackAlarm* request to be issued to the GMDR server to perform the required acknowledgment. For additional information, see 241-6001-303 *Preside MDM Administrator Guide*, and the section on Inbound Alarm API in 241-6001-203 *Preside MDM Alarm and Status API Reference Guide*.

## Acknowledging selected active alarms

In Alarm Acknowledgment, you can acknowledge a previously unacknowledged alarm, and you can re-acknowledge a currently acknowledged alarm with a different user (if this field is configured to be editable) or reason, or both.

The figure “Acknowledge Alarm(s) Dialog for selected active alarms” (page 278) illustrates an Acknowledge Alarm(s) Dialog for selected active alarms.

### Acknowledging selected active alarms

- 1 When the Acknowledge Alarms Dialog opens, enter a reason or modify the existing reason.
- 2 If the dialog is configured to allow the *User* value to be changed, modify it if required.
- 3 Click on *Ack Alarm(s)*.

The dialog closes.

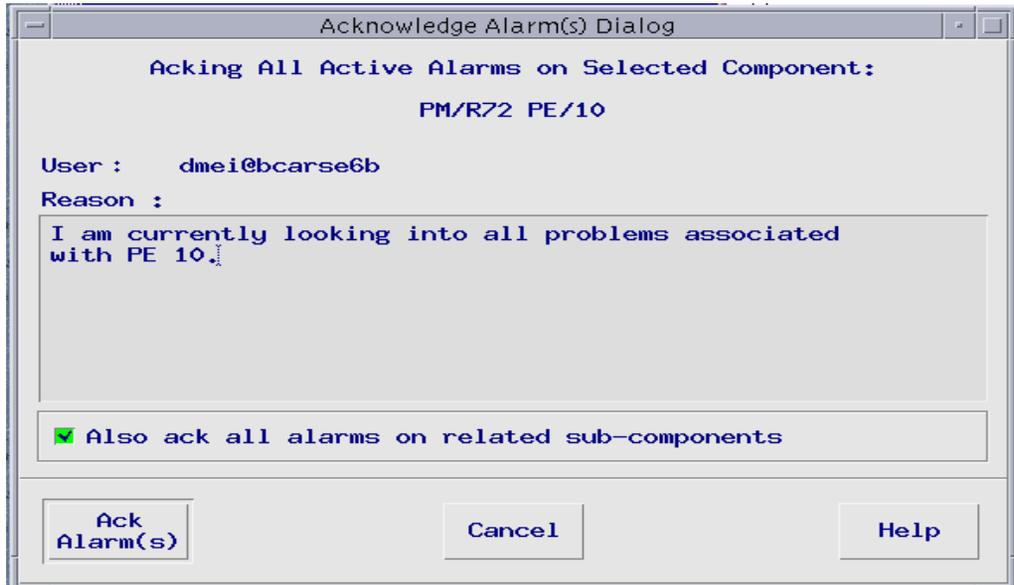
An attempt is made to acknowledge each alarm. If a given alarm fails to be acknowledged, other alarms are not affected; they can still be acknowledged.

## Acknowledging active alarms for selected components

Active alarms for selected components from within the Network Viewer, Component Status Display, Network Status Bar, and Component Information Viewer can be acknowledged.

The figure “Acknowledge Alarm(s) Dialog for selected components” (page 283) shows the Acknowledging Alarm(s) Dialog.

**Figure 31**  
**Acknowledge Alarm(s) Dialog for selected components**



### Acknowledging active alarms on selected components

- 1 When the Acknowledge Alarms Dialog opens, enter a reason or modify the existing reason.
- 2 If the dialog is configured to allow the *User* value to be changed, modify it if required.
- 3 Click on *Also ack all alarms on related sub-components*.

*This acknowledges all active alarms for all subcomponents of the selected component.*

- 4 Click on *Ack Alarm(s)*.

The dialog closes.

An attempt is made to acknowledge each alarm. If a given alarm fails to be acknowledged, other alarms are not affected; they can still be acknowledged.

## Unacknowledging selected active alarms

In Alarm Unacknowledgement, you can unacknowledge a previously acknowledged alarm, and you can unacknowledge a currently unacknowledged alarm to change the owner or reason, or both. You cannot unacknowledge an alarm that has never been acknowledged or unacknowledged.

The figure “UnAcknowledge Alarm(s) Dialog for selected active alarms” (page 280) illustrates a sample Unacknowledge Alarm(s) Dialog for selected active alarms.

### Unacknowledging selected active alarms

- 1 When the Unacknowledge Alarms Dialog opens, enter a reason or modify the existing reason.
- 2 If the dialog is configured to allow the *User* value to be changed, modify it if required.
- 3 Click on *Unack Alarm(s)*.
- 4 To unacknowledge all active alarms on a selected component and all its subcomponents, click on the toggle button.

The dialog immediately closes.

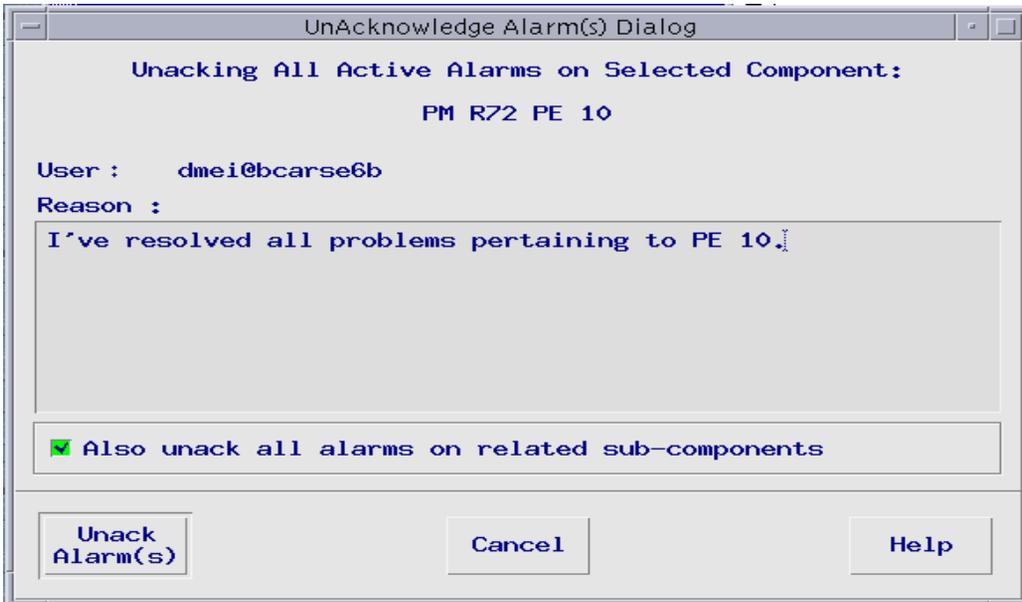
An attempt is made to unacknowledge each alarm. If a given alarm fails to be unacknowledged, other alarms are not affected; they can still be unacknowledged.

## Unacknowledging active alarms on selected components

Active alarms for selected components from within the Network Viewer, Component Status Display, Network Status Bar, and Component Information Viewer can be unacknowledged.

The figure “UnAcknowledge Alarm(s) Dialog for selected component” (page 285) shows the Unacknowledge Alarm(s) Dialog.

**Figure 32**  
**UnAcknowledge Alarm(s) Dialog for selected component**



### Unacknowledging active alarms on selected components

- 1 When the Unacknowledge Alarms Dialog opens, enter a reason or modify the existing reason.
- 2 If the dialog is configured to allow the *User* value to be changed, modify it if required.
- 3 Click on *Also unack all alarms on related sub-components*.  
This unacknowledges all active alarms for all subcomponents belonging to the selected component.
- 4 Click on *Unack Alarm(s)*.  
The dialog immediately closes.

An attempt is made to unacknowledge each alarm. If a given alarm fails to be unacknowledged, other alarms are not affected; they can still be unacknowledged.

## Customizing the Alarm Acknowledgment Dialog

The dialogs used for acknowledgment/unacknowledgement of alarms use resources to control their functional and visual aspects. You can customize some of these resources.

The table “Resources for customizing the Acknowledge/Unacknowledge Alarms Dialog” (page 286) lists the alarm acknowledgment resources that you can customize. These resources apply to both the Acknowledge Alarm(s) Dialog and the Unacknowledge Alarm(s) Dialog.

**Table 39**  
**Resources for customizing the Acknowledge/Unacknowledge Alarms Dialog**

Resource	Description	Legal value
*AckAlarmDlog*userld FieldField.editable	If True, the <i>User</i> field in the dialog used for acknowledging or unacknowledging alarms, can be modified. The default is False.	True or False
*AckAlarmDlog* commentData.max Length	The maximum length of <i>Reason</i> text that can be specified when acknowledging or unacknowledging alarms. The default length is 256.	Any legal <i>Motif</i> value associated with the <i>MaxLength</i> resource.

### Resource Files

The following files contain resources for the Acknowledge and Unacknowledge Alarm(s) Dialogs:

- */opt/MagellanNMS/lib/app-defaults/C/CIV* contains resources for the dialog when invoked from selected alarms in the Component Information Viewer.
- */opt/MagellanNMS/lib/app-defaults/C/IAD* contains resources for the dialog when invoked from selected alarms in Alarm Display.

- `/opt/MagellanNMS/lib/app-defaults/C/ACKALARM` contains resources for the dialog when invoked from selected components in Network Viewer, Component Status Display, Component Information Viewer, and Network Status Bar.

You can make resource changes to the Alarm Acknowledgment Dialogs that affect a particular application or all applications that provide Alarm Acknowledgment. For example, you can change the following resource:

```
IAD*AckAlarmDlog*UserIdFieldField.editable: True
```

This enables the *user* field to be editable when acknowledging or unacknowledging alarms from the Alarm Display. If you omit the *IAD* prefix, all applications are affected.

See the section on customizing resources used by MDM tools in 241-6001-301 *Preside MDM Customization Administrator Guide*, for more information on setting and overriding resources.



---

## Chapter 8

# Network Status Bar

---

This section describes the Network Status Bar and provides you with instructions on how to use this tool. The following information is included:

- “Network Status Bar overview” (page 289)
- “Network Status Bar main window” (page 290)
- “Keyboard shortcuts” (page 294)
- “NSB Dialogs” (page 294)
- “NSB procedures” (page 296)
- “Customizing resources in the Network Status Bar” (page 299)

### Network Status Bar overview

The Network Status Bar provides you with a high-level view of the current network status. The Network Status Bar monitors a set of statistical indicators gathered from the General Management Data Router (GMDR) database. Some of these indicators quantify troubled elements of the network, including the number of active alarms and the number of out-of-service components.

The Network Status Bar supports the following capabilities:

- global network status monitoring and indicator thresholding
- a Troubled Components Dialog that displays troubled components from the network model
- service selection of the network model
- service selection of the GMDR servers

You can perform the following procedures using the Network Status Bar:

- start the Network Status Bar, see “Starting the Network Status Bar” (page 296)
- acknowledge the current indicator values, see “Acknowledging the current indicator values” (page 297)
- view the Troubled Components Dialog, see “Troubled Components Dialog” (page 294)
- start other Preside Multiservice Data Manager (MDM) tools, see “Starting other tools” (page 298)

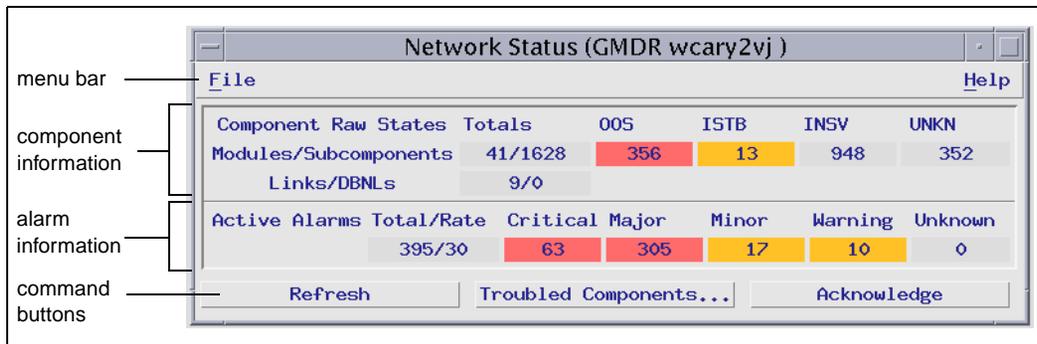
## Network Status Bar main window

The Network Status Bar main window contains the following areas:

- “Menu bar” (page 291)
- “Component information” (page 291)
- “Alarm information” (page 292)
- “Command buttons” (page 293)

See the figure “Network Status Bar window” (page 290) for a sample Network Status Bar window.

**Figure 33**  
**Network Status Bar window**



Active alarms and out-of-service components indicate troubled network elements. Troubled elements display with a colored background: red for major trouble and orange for minor trouble. This puts emphasis on their values if a customizable threshold is crossed. If no threshold is crossed, their background remains a neutral color.

The information displayed is refreshed on a regular basis, typically every 60 seconds. The time interval can be set by using the *refreshPeriod* resource or the *-refresh* command line option. For additional information, see “Customizing resources in the Network Status Bar” (page 299).

## Menu bar

The menu bar contains the following menus:

- “File menu” (page 291)
- “Help menu” (page 291)

### File menu

The File menus contains the following command:

- **Exit** closes the window and exits the tool.

### Help menu

The Help menu contains the following commands:

- **On Context** displays information about a selected area of the Network Status Bar window.
- **On Window** displays descriptive information about the Network Status Bar window components.

## Component information

The components section displays information on the total number of components managed by GMDR and its breakdown into per state counts (the states here are raw states, as opposed to those visible from a Network Model base tool). Counts are shown for both modules/subcomponents and plain and dynamic links (DBNL):

<b>State</b>	<b>Description</b>
Totals	The total number of modules or subcomponents
* OOS	The number of out-of-service components (modules and subcomponents) (threshold resource: compOOSThresh)
+ ISTB	The number of in-service components that are troubled (threshold resource: compISTBThresh)
INSV	The number of in-service components.
UNKN	The number of components in other states (unknown to GMDR)
+ Totals	The total number of plain and dynamic links (for example, DBNL) known to GMDR to be active (threshold resource: dbnlCountThresh for dynamic links)

## Alarm information

The alarm section displays information on the number of active alarms in the GMDR database. This count is broken down in terms of (common format) alarm severities and the alarm arrival rate in alarms per minute.

<b>State</b>	<b>Description</b>
* Critical	The number of active alarms of severity CRITICAL (threshold resource: critAlmThresh)
* Major	The number of active alarms of severity MAJOR (threshold resource: majorAlmThresh)
+ Minor	The number of active alarms of severity MINOR (threshold resource: minorAlmThresh)
+ Warning	The number of active alarms of severity WARNING (threshold resource: warnAlarmThresh)

<b>State</b>	<b>Description</b>
Unknown	The number of active alarms of severity INDETERMINATE (or other)
Total/Rate	The number of active alarms or the alarm arrival rate (alarms per minute)

**Note:** The ‘\*’ indicates a major trouble indicator displaying a red background when its value is above threshold.

**Note:** The ‘+’ indicates a minor trouble indicator displaying an orange background when its value is above threshold. For links, the number of DBNLs is checked.

## Command buttons

The Network Status Bar provides the following buttons:

### **Refresh**

The *Refresh* button updates the dialog with the latest information from the GMDR database. Acknowledgment is removed and thresholded background colors are displayed as required.

### **Troubled Components...**

The *Troubled Components...* button starts the Troubled Components Dialog to show what components are currently in the Troubled state (OOS or ISTB) as indicated by the Network Model.

### **Acknowledge**

The *Acknowledge* button acknowledges the current status values by changing the background color of the trouble indicator fields (aquamarine) on the display. As the values of these indicators change, their background color reverts to either the OK color (gray) or the trouble-indicating color (red or orange). This enables you to ignore the current issues in the network but be informed of any change in the indicators. Pressing the Refresh button forces all indicators to display their unacknowledged background color.

## Keyboard shortcuts

The Network Status Bar provides the following command shortcuts:

- *Ctrl+E* exits from the Network Status Bar tool.
- *Shift+Help* displays help information for the dialog, menu item, or button that the cursor is currently on. When you press Shift+Help, the cursor changes to a question mark. Move the cursor to the item for which you want help and press the Select button to display help information for the item.

## NSB Dialogs

The Network Status Bar provides the following dialogs:

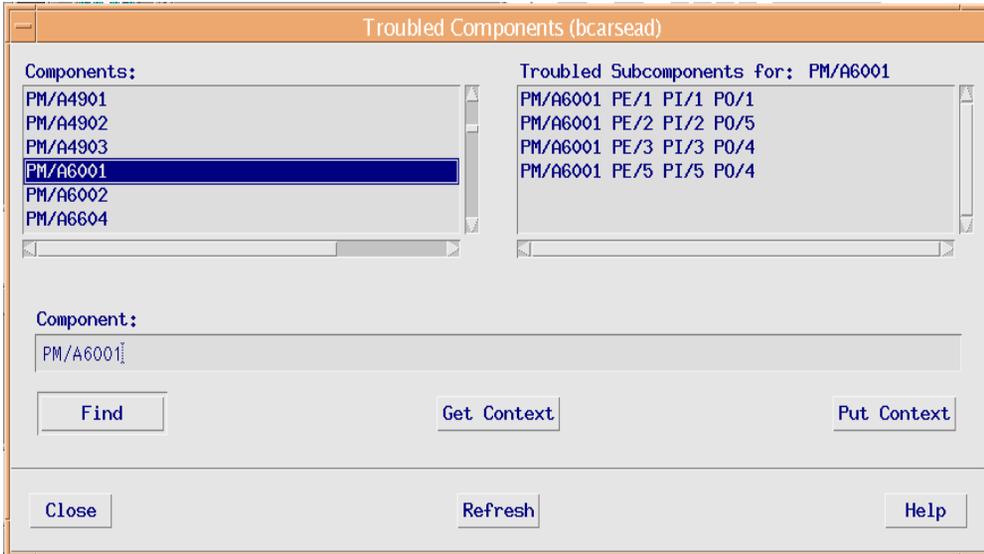
- “Troubled Components Dialog” (page 294)
- “Error Dialogs” (page 296)
- “Warning Dialogs” (page 296)

### Troubled Components Dialog

The Troubled Components Dialog, shown in the figure “Troubled Components Dialog” (page 295), displays the troubled components in the Network Model. A list on the left shows all components and links known to the Network Model to have a Troubled state (out-of-service or in-service–troubled) or to have subcomponents with a Troubled state. It also displays all Dial Backup Network Links (DBNLs) known to be active. When a component in this list is selected, the list on the right is updated to include the troubled subcomponents for the selected component module or link (for links, both endpoints are shown as in the Component Information Viewer's Related List).

Note that the contents of the dialog are not updated automatically as that of the main window. To update the information in the dialog, select the Refresh button.

**Figure 34**  
**Troubled Components Dialog**



The subcomponents in the troubled subcomponents list support a pop-up start tools menu that lets you to start another Preside Multiservice Data Manager (MDM) tool in the context of the selected component. For details on the Start Tool menu, see “Start Tool” (page 39). Start tool menus can be customized. For information about customizing start tools, see the section on customizing the toolsets and Start Tools menu in 241-6001-301 *Preside MDM Customization Administrator Guide*.

The component text field can be populated in these ways:

- by dropping a component from another tool onto the dialog
- by selecting a component in the module or component list
- by entering a component name from the keyboard
- by selecting the Get Context button

**Note:** You can also drag the components of the dialog and drop them (component name) onto other tools.

Components selected with the *select* mouse button in the subcomponents list (rinh) are also automatically put into (Hot) context as if the *Put Context* command had been issued.

Buttons in the dialog are as follows:

- The *Find* button displays the component in the component list and the subcomponent in the subcomponent list. The lists are scrolled so that the component is visible. A standard warning dialog is displayed if the entered component is not found.
- The *Get Context* button performs the Find Component operation, for the component in context.
- The *Put Context* button puts the current component in context.
- The *Refresh* button updates the dialog with the latest information from the database.

## Error Dialogs

Error dialogs warn you of an error condition. You need to respond before you can proceed. Click on OK to return to the application at the point before the error condition occurred.

## Warning Dialogs

Warning dialogs warn of possible danger. You need to respond before you can proceed. Click on OK to proceed, or click on Cancel to return to the application at the point before the dialog appeared.

## NSB procedures

You can perform the following tasks using the Network Status Bar:

- “Starting the Network Status Bar” (page 296)
- “Acknowledging the current indicator values” (page 297)
- “Using the Troubled Components Dialog” (page 297)

## Starting the Network Status Bar

You can leave the Network Status Bar open continuously, so that changes in the network can be monitored while you use the workstation for other applications.

## Starting the Network Status Bar

- 1 From the Preside MDM window, select Fault -> Network Status Bar.

The Network Status window opens.

Component Raw States Totals	005	ISTB	INSV	UNKN	
Modules/Subcomponents	41/1628	356	13	948	352
Links/DBNLs	9/0				

Active Alarms Total/Rate	Critical Major	Minor	Warning	Unknown	
395/30	63	305	17	10	0

- 2 Select *Refresh* to view the latest information from the GMDR database.

The dialog is Updated with the latest information from the GMDR database.

## Acknowledging the current indicator values

When you acknowledge the current indicator values, the background color changes. This visible feedback helps you to identify future changes in indicator values.

### Acknowledging the current indicator values

- 1 From the Network Status menu, select Acknowledge.

The background color of the trouble indicator fields changes to aquamarine.

As the values of these indicators change, their background color reverts to either the OK color (gray) or to the trouble-indicating color (red or orange).

- 2 Select *Refresh* if you want to force all indicators to display their unacknowledged background color.

## Using the Troubled Components Dialog

The following procedure explains how to use the Troubled Components Dialog.

### **Opening and navigating into the Troubled Components Dialog**

**1** In the Network Status window, click the Troubled Components button.

The Troubled Components Dialog opens and displays those components that are currently in trouble as indicated by the network model.

**2** To identify specific troubled components, perform one of these actions:

- Select a module or link in the list on the left of the display so that its troubled subcomponent or endpoints are displayed in the list on the right of the display.
- Type in the name of the component and select *Find*.
- Select *Get Context* to perform the Find Component operation for the component in context.
- Use Drag and Drop onto this dialog to select the source component.

### **Using the Troubled Components Dialog information for other tools**

**1** Navigate to identify the components you want, using the procedure “Opening and navigating into the Troubled Components Dialog” (page 298).

**2** Perform one of these actions:

- Select *Put Context* to put the current component in context.
- Use Drag and Drop to drag the source component to its destination tool.
- Use the *Start Tool* command on selected components as described in “Starting other tools” (page 298).

### **Starting other tools**

The subcomponents in the component lists of the Troubled Dialog support a pop-up menu that allows you to start another Preside Multiservice Data Manager (MDM) tool in the context of the selected component (for example, invoking the Component Information Viewer for the selected subcomponent).

### **Starting a tool from the Troubled Components Dialog**

**1** Position the mouse pointer on a component or subcomponent and press the mouse menu button.

A pop-up menu opens.

- 2 Select a toolset in the pop-up menu and then point to the tool that you want to start.

## Customizing the Network Status Bar

The NSB lets you customize the following items:

- Troubled Components pop-up menu
- NSB resources

### Customizing the Troubled Components pop-up menu

For procedures on customizing the pop-up menu in the *Troubled Components* Dialog, see the section on customizing the toolsets and Start Tools menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

When you modify the menu, use one of the following substitution variables substitution variables in the command line:

- \$COMP: The internal component name of the target
- \$DCOMP: The display component name of the target

### Customizing resources in the Network Status Bar

The *Network Status Bar* uses resources to describe certain functional and appearance aspects. Some of these aspects can be customized. Others must not be tampered with without affecting the functionality of the Network Status Bar.



#### **CAUTION**

##### **Risk of altering the functionality of the NSB**

Do not modify resources that are not listed in the following table. Changing unlisted resources may negatively affect the appearance and functionality of the Network Status Bar.

For details about customizing resources, see the section on customizing resources used by MDM tools in 241-6001-301 *Preside MDM Customization Administrator Guide*. The original resource file for the Network Status Bar is */opt/MagellanNMS/lib/defaults/C/StatsBar*.

The table “Resources in the Network Status Bar that you may customized” (page 300) lists the Network Status Bar resources that you may customize.

**Table 40**  
**Resources in the Network Status Bar that you may customized**

Resource	Description	Legal values
compOOSThresh dbnlCountThresh critAlmThresh majorAlmThresh minorAlmThresh warnAlarmThresh	Indicator thresholds	Integer (def: 0)
refreshPeriod	Main window refresh interval	Integer (def: 60s)
errorColor	Major indicators' background color	Color
warningColor	Minor indicators' background color	Color
plainColor	Non-threshold background color	Color
ackedColor	Acked indicators' background color	Color

## Chapter 9

# Component Information Viewer

---

This section provides an overview and window description for the Preside Multiservice Data Manager (MDM) Component Information Viewer tool. This section contains the following topics:

- “Component Information Viewer overview” (page 301)
- “Component Information Viewer window” (page 303)
- “Customizing the Component Information Viewer display” (page 318)
- “Diagnostic commands” (page 325)
- “Procedures” (page 342)
- “Errors and warnings” (page 381)

### Component Information Viewer overview

The Component Information Viewer is the primary Multiservice Data Manager (MDM) tool for diagnosing network faults. This tool provides in-depth information on components and subcomponents of a network element. You can view surveillance information for a component and navigate to other components, subcomponents, or associated links. The Component Information Viewer uses information from active and recent alarms to assess the cause of a fault. The tool also determines the impact of a fault by providing state information for related components.

Using the Component Information Viewer, you can perform the following tasks:

- put a component into acknowledge or maintenance state

- acknowledge, unacknowledge, or clear active alarms
- start other tools
- set preferences for parameters such as automatic context, automatic refresh interval, alarm format, and customer database server identification
- set component filters
- obtain management information including active alarms, recent alarms, status records (DPN only), model data, and customer data
- execute diagnostic commands

## Component Information Viewer data

The tool facilitates fault diagnosis by providing access to the following management and diagnostic information:

### Management data

The information panel provides various types of management data information on a component including active alarm, recent alarms, status, model data, and customer data.

- Active alarm information includes active alarms for the target component extracted from the General Management Data Router (GMDR).
- Recent alarms information includes recent alarms, active or not, for that component extracted from the GMDR buffer.
- Status information includes the most recent status record received for the target component extracted from the GMDR.
- Model information includes information on the component that is stored in the Network Model.
- Customer Database includes information for the component. The information is retrieved from the Customer Database server identified in the Preference Settings Dialog.

### Diagnostic information

The Component Information Viewer provides commands that let you directly access information to diagnose network faults without having to start other fault management tools.

Before you can access diagnostic information, you need to specify a component and the type of diagnostic information you want to retrieve. Diagnostic information displays in the Component Information Viewer window or, in some cases, another window. For details about the available diagnostic commands, see “Diagnostic commands” (page 325).

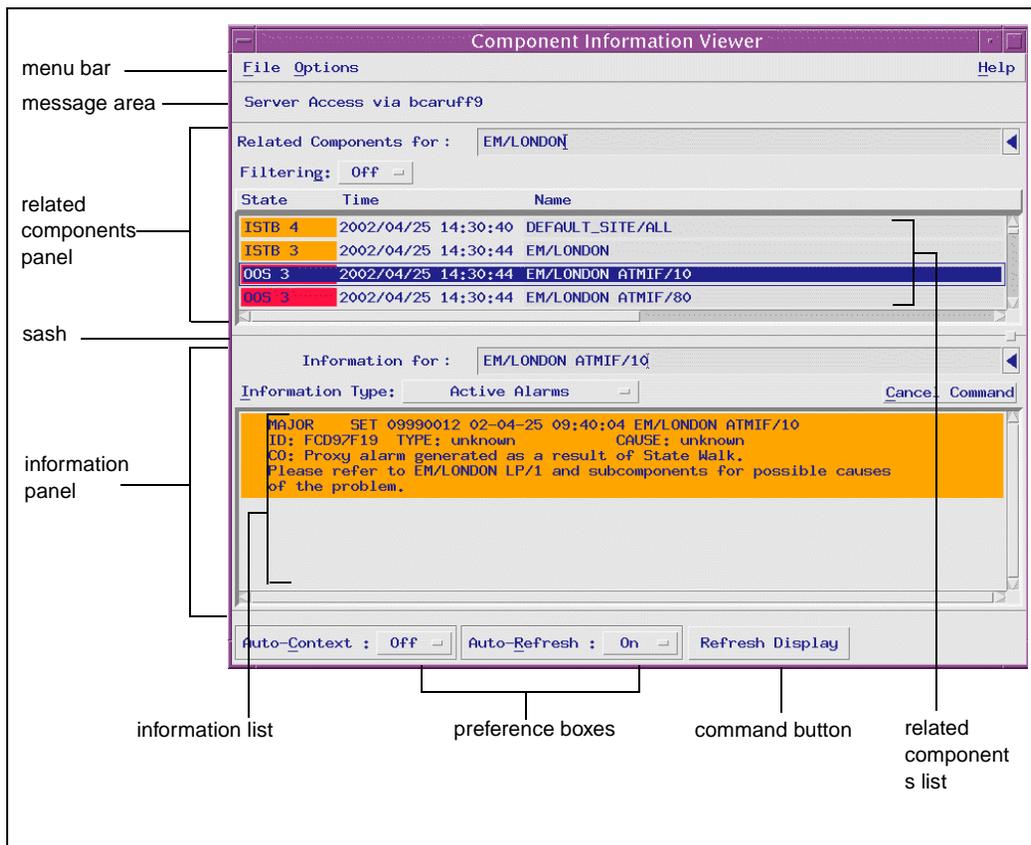
## Component Information Viewer window

The Component Information window contains the following areas:

- “Menu bar” (page 306)
- “Message area” (page 307)
- “Related components panel” (page 307)
- “Sash” (page 310)
- “Information panel” (page 310)

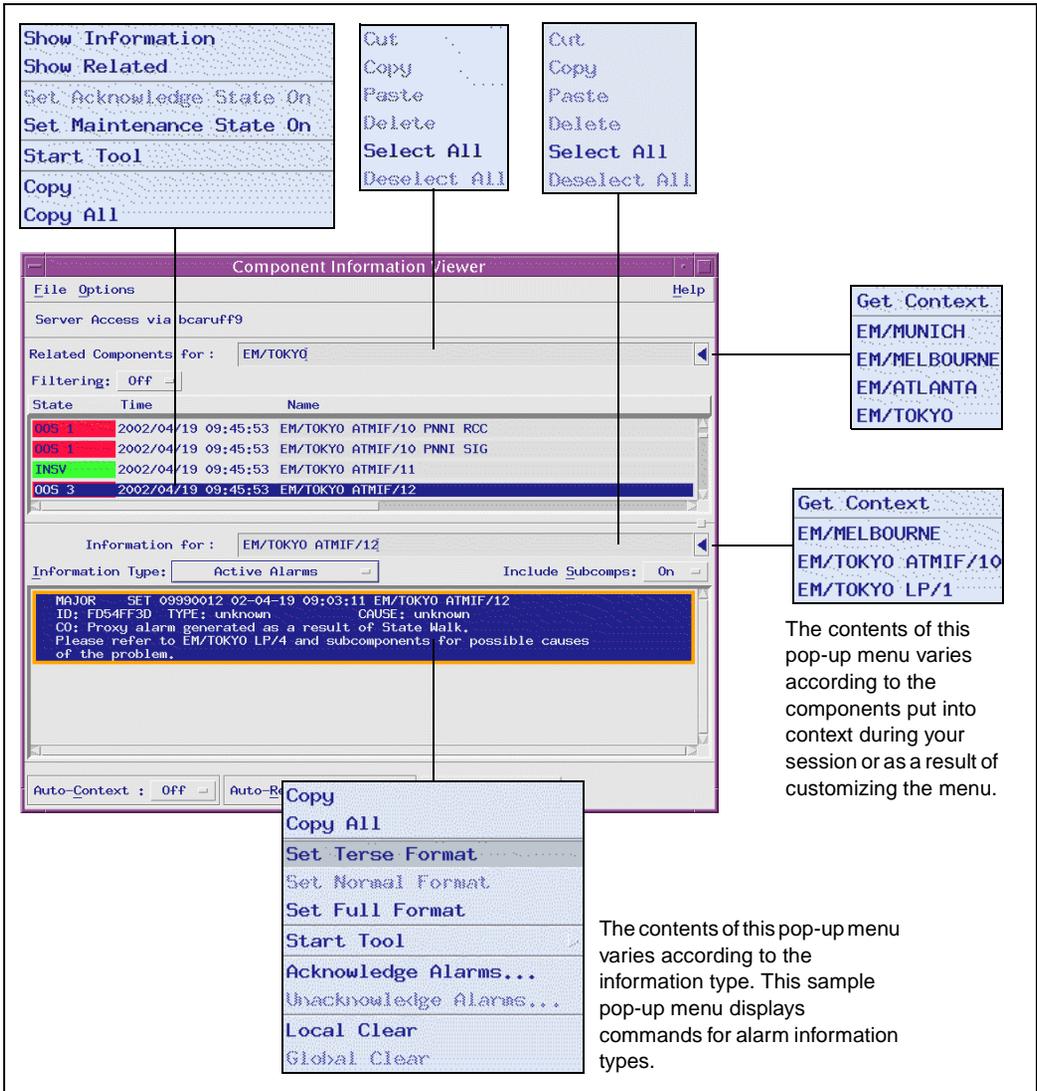
The figure “Sample Component Information Viewer window” (page 304) shows a sample Component Information Viewer window.

**Figure 35**  
**Sample Component Information Viewer window**



The figure “Component Information Viewer pop-up menus” (page 305) shows commands that are available from pop-up menus in the Component Information Viewer tool.

**Figure 36**  
**Component Information Viewer pop-up menus**



## Menu bar

The Component Information Viewer menu bar contains the following menus:

- “File menu” (page 306)
- “Options menu” (page 306)
- “Help menu” (page 306)

### File menu

The File menu contains the following command:

- **Exit** closes the Component Information Viewer tool. If you modified preferences or filter settings, a dialog box opens and prompts for the appropriate course of action for these changes before the session closes.

### Options menu

The Options menu contains the following commands:

- **Change Component Filter Settings...** opens the Component Filter Settings dialog box where you can modify, save, and restore component filter settings. For the procedure to change filter settings, see [“Setting component filters”](#) (page 348).
- **Change Preference Settings...** opens the Preference Settings Dialog where you can modify, save, and restore Component Information Viewer preferences. For the procedure the change preference settings, see [“Setting Preferences”](#) (page 350).

### Help menu

The Help menu contains the following commands:

- **Help on Context** displays information about a selected area of the Component Information Viewer window.
- **Help on Window** displays general information about the Component Information Viewer tool.

For details about using these help commands, see [“Displaying Component Information Viewer online help”](#) (page 347).

## Message area

The message area displays the name of the servers used by the Component Information Viewer. This area also displays a message when a command returns a non-zero error code.

## Related components panel

The related components panel lets you view the impact of a component failure and the name and state of any related components. From this panel, you can start other MDM tools and interact with the Information Panel to find the cause of a particular fault.

The related components panel contains the following items:

- “Related Components for” (page 307)
- “Filtering box” (page 308)
- “Related components list” (page 308)

### Related Components for

Use the Related Components for field to specify the component name for which you want related component information. Related component information displays in the related components list.

The Related Components for field supports two pop-up menus. One pop-up menu collects the names of components that you target during a session. You can select an entry from this list of components to populate the field. To open this menu, right-click on the triangle at the right of the Related Components for field. The other pop-up menu lets you edit existing text in the field. To open this pop-up menu, right-click in the field. The figure “Component Information Viewer pop-up menus” (page 305) shows these pop-up menus.

You can use various methods to specify a component name in the Component Information Viewer window.

- Typing an entry.  
If you type the component name in a format other than the display format, the Component Information Viewer reformats the component name to the display format.

- Using component context  
To use component context, right-click on the left pointing triangle at the end of the Related Components for field and select the an appropriate entry from the **Get Context** pop-up menu. For more information about component context, see “Context” (page 38).
- Selecting an item from the target component pop-up menu  
The Component Information Viewer tool maintains a list of the last 10 components that you have targeted during your session. To recall a targeted component, right-click on the triangle to the right of the Related Components for field and select an entry from the Get Context pop-up menu.

### **Filtering box**

You set filters by using the Change Component Filter Settings... command in the Options menu. The Filtering box contains a drop-down list that lets you turn filtering on or off for related components. When filtering is on, only those components matching the current component filter settings display in the related components list. When filtering is off, all related components display.

The Component Information Viewer saves the value specified in the Filtering box as a preference setting. Therefore, the filter setting applies each time the Component Information Viewer tool opens. For more information on preference settings, see “Setting Preferences” (page 350).

### **Related components list**

The related components list displays the parents, children, related links, and any special relationships of the component specified in the Related Components for field. This list also supports a pop-up menu that lets you perform tasks on selected entries in the list.

The list displays the propagated state, time, and name of each related component. For a description of the propagated states, see the table “Propagated states” (page 309).

**Table 41**  
**Propagated states**

Propagated state	Description
UNKNOWN	The component is unknown.
INSV	The component is in service and working properly.
ISTB	The component is in service but has a non-fatal fault, or one of its subcomponents is ISTB or OOS. The number represents the criticality of the faulty component.
OOS	The component is out of service because of a fatal fault or one of its parents is OOS. The number represents the criticality of the faulty component.
MTCE	The component is in maintenance state.
HIER MTCE	The component is in a hierarchical maintenance state. This state occurs when a parent of the component is in maintenance state.
ACKED	The component is in acknowledged state and no other faults are apparent.

The time shown in the list is the time of the last state change. The time displays in *yy-mm-dd hh:mm:ss* format. If the component has never had a state change, the text “Never Changed” displays.

### Related components pop-up menu

The related components pop-up menu lets you perform tasks on selected entries in the related components list. To open the pop-up menu, right-click on an entry in the related components list. The figure “Component Information Viewer pop-up menus” (page 305) shows the related components pop-up menu. This pop-up menu contains the following commands:

- **Show Information** updates the Information Panel to show information on the selected component.
- **Show Related** updates the Related Components Panel to show the related components of the selected component.

- **Set Acknowledge State On/Off** sets the acknowledged state of a selected component. For more information, see “Setting the acknowledge state for a component” (page 356).
- **Set Maintenance State On/Off** sets the maintenance state of a component and the hierarchical maintenance for all its subcomponents. For more information, see “Setting the maintenance state for a component” (page 357).
- **Start Tool** allows you to start other MDM tools. For details, see “Starting other MDM tools from Component Information Viewer” (page 358).
- **Copy** copies the text of the selected item to the Primary selection and the clipboard.
- **Copy All** copies the text of all the related components to the Primary selection and the clipboard.

## Sash

The sash is positioned between the related components and information panels. Moving the sash up or down changes the amount of space each panel occupies. For example, if you move the sash down to increase the amount of space for the related components panel, the amount of space for the information panel decreases. To move the sash, drag the box on the right side of the sash up or down.

## Information panel

Use the information panel to display additional management data for a component including alarms, network model data, customer data, and diagnostics.

The Information Panel contains the following items:

- “Information for” (page 311)
- “Information type” (page 313)
- “Include subcomps” (page 314)
- “Commands” (page 314)
- “Information list” (page 316)

**Information for**

To view additional information about a component, you need to specify the component name in the Information for field and specify the type of information you want in the Information Type box. For information about the types of information you can display, see “Information type” (page 313). This field also supports a pop-up menu that lets you edit the text in the field.

The Information for field supports two pop-up menus. One pop-up menu collects the names of components that you target for information during a session. You can use this pop-up menu to populate the field. To open this menu, right-click on the triangle at the right side of the Information for field. The other pop-up menu lets you edit existing text in the field. To open this pop-up menu, right-click in the field. The figure “Component Information Viewer pop-up menus” (page 305) shows these pop-up menus.

To specify a component name in this field, you can use the following methods:

- **Typing an entry**  
If you type the component name in a format other than the display format, the Component Information Viewer reformats the component name to the display format.
- **Using the field’s pop-up menus**  
There are two pop-up menus in the Information for field. One provides commands to edit the text in the field, the other pop-up menu provides access to component context and a list of components from which you can select. You can use the second pop-up menu to target a component. To open this pop-up menu, right-click on the triangle at the end of the Information for field. You can then target the component in context by selecting the Get Context command, or you can target a component by selecting from a list of the ten most recently targeted components. For more information about component context, see “Context” (page 38). If you frequently use the same component names, you can customize the entries in this pop-up menu. For details, see “Customizing the Component Information Viewer display” (page 318).
- **Using the related components list**  
Selecting an entry in the related components list, populates the Information for field with the selected component name.

- Using search patterns  
You can use search patterns for active alarm and recent alarm information types. Patterns of components have a vertical bar ('|') in the name, typically the first character if there is only one pattern. All alarms matching the specified patterns display in the information panel. The pattern language is the same as extended GREP style patterns.

A search pattern is first matched to the component ID in canonical format (blank separated). Then the pattern is matched to the component ID in display format (/ separated), then to the fault code, and finally to the comment text of the alarms.

When you specify a search pattern, information is not automatically refreshed. Refresh the display manually by clicking the Refresh button or by pressing the Return key in the text field.

The table “Sample search patterns” (page 312) provides sample search patterns and a description of their function.

**Table 42**  
**Sample search patterns**

Search pattern	Function
EM .* SONET .* EM .* DS3 .*	Reports all alarms in the network for Passport DS3 and SONET port-interfaces
EM .* SONET .*	Reports only SONET alarms. The vertical bar at the beginning distinguishes the specification from a plain component name:
^7039....\$ ^7041....\$ ^7001....\$	Displays all Passport ATM and Frame Relay related alarms. The caret (^) indicates the beginning of the string to match. The \$ character indicates the end of the string to ensure occurrences of these numbers are not matched in the middle of another string

**Pop-up menu**

To edit the text in the Information for field, use the field's pop-up menu. To open the pop-up menu, right-click in the Information for field. The pop-up menu contains commands that let you cut, copy, paste, delete, select or deselect text in this field. This pop-up menu is the same as the Related Components for pop-up menu.

**Information type**

The Information Type: box lets you select the type of information to display in the information panel. The table "Component Information Viewer Information types" (page 313) lists the available information types.

**Table 43**  
**Component Information Viewer Information types**

<b>Information type</b>	<b>Description</b>
Active Alarms	Displays the currently active alarms for the specified component
Status	Displays the most recent status record received from the specified component (DPN only)
Recent Alarms	Displays the alarm history for the specified component
Model Data	Displays the information about the specified component, as started in the network model.
Customer Data	Displays customer database information matching the specified component. This information is retrieved from the Customer Database server identified in the Preferences dialog. See "Setting Preferences" (page 350)
Diagnostics	Displays diagnostic information based on the type of information selected with the Command button. For details about available diagnostic commands, see "Diagnostic commands" (page 325)

The Component Information Viewer saves the value in the Information Type box as a preference setting. Therefore, the information type applies each time the Component Information Viewer application opens. For more information on preference settings, see “Setting Preferences” (page 350).

### **Include subcomps**

The Include Subcomps box is available only when the current information type is Active Alarms. This box lets you choose whether or not to display active alarms for all subcomponents of a specified component.

The Component Information Viewer saves the value in the Include Subcomps box as a preference setting. Therefore, the setting for this option applies each time the Component Information Viewer application opens. For more information on preference settings, see “Setting Preferences” (page 350).

### **Commands**

The Commands box is available only when the current information type is Diagnostics. Clicking on the box opens a menu of diagnostic commands. The commands vary depending on the available tools and whether the menu of diagnostic commands has been customized at your installation. You may see the following items:

- commands to select a command route, start the Command Console tool, and display online help
- Passport and DPN commands to
  - help diagnose components
  - send inventory reports to the Information Panel
- Passport commands to execute Passport tests

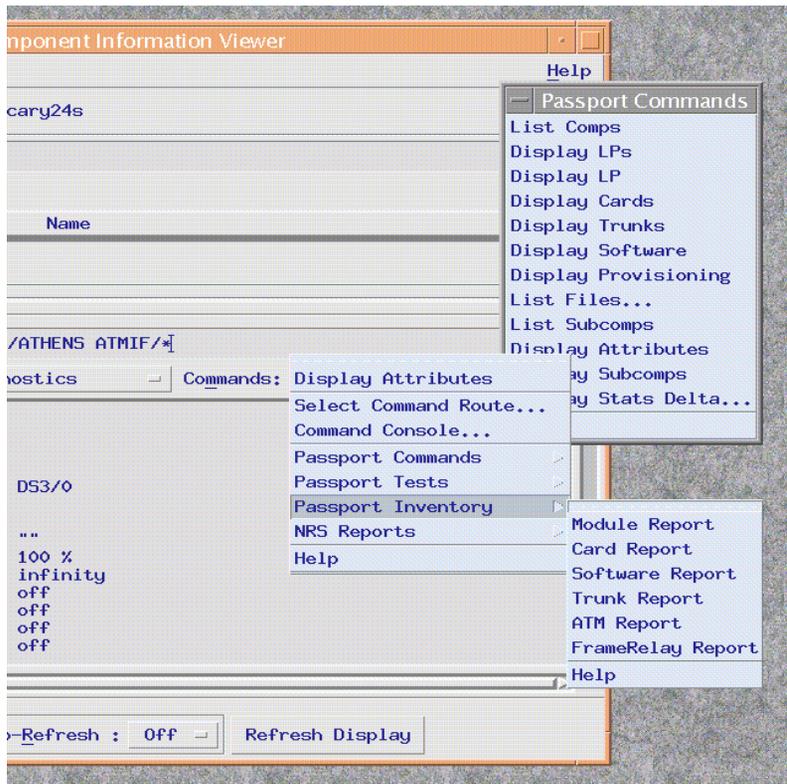
Output from these diagnostic commands display in the Information panel.

For a list of default Component Information Viewer Diagnostic commands, see “Diagnostic commands” (page 325). For details about customizing the diagnostic menu, see the section on customizing the Component Information Viewer diagnostics in 241-6001-301 *Preside MDM Customization Administrator Guide*. The Commands menu and its submenus are all detachable to make their commands easier and faster to use. To detach a menu, press the middle mouse button on the dotted white line at the top of the

menu and drag the menu off the window. Since the commands in a menu are sensitive to the type of component currently targeted by the Information panel, the availability of these commands will be re-evaluated when you change the value in the Information for field or when the field loses the focus.

The figure “Detachable Commands menu” (page 315) shows the available commands.

**Figure 37**  
**Detachable Commands menu**



### Information list

The information list displays information about selected components. The content of the information list depends on the type of information that you select from the Information Type box. You can display active alarms, status records (DPN only), recent alarms, model data, customer data, and diagnostics.

Each information type has its own pop-up menu. The figure “Component Information Viewer pop-up menus” (page 305) shows the pop-up menu for the diagnostic information type.

When active alarms and recent alarms display in the Information list, the following commands are available from the pop-up menu:

- **Copy** copies the text of the selected alarm in the information panel to the clipboard and a specified destination.
- **Copy All** copies all the alarms in the information panel to the clipboard and a specified destination.
- **Set Terse Format** lets you to display the selected alarms in terse format. For detailed information on terse format, see “Terse” (page 223).
- **Set Normal Format** lets you to display the selected alarms in normal format. For detailed information on normal format, see “Normal” (page 224).
- **Set Full Format** lets you to display the selected alarms in full format. For detailed information on full format, see “Full” (page 224).
- **Start Tool** lets you to start other tools and utilities. For details, see “Starting other MDM tools from Component Information Viewer” (page 358).
- **Acknowledge Alarms...** lets you to indicate to other network operators that you are currently investigating a fault causing an alarm. This is available for Active Alarms only. For more information, see “Acknowledging active alarms” (page 369).

- **Unacknowledge Alarms...** lets you take selected alarms out of the Acknowledged state and indicate to other network operators that the fault causing the alarm has been resolved or needs to be investigated. This is available for Acknowledged Active Alarms only. For more information, see “Unacknowledging active alarms” (page 370).
- **Local Clear** clears the selected alarms on the Preside Multiservice Data Manager (MDM) system only. This is available for Active Alarms only. For more information, see “Clearing active alarms for DPN” (page 361).
- **Global Clear** clears alarms from the appropriate DPN-100 OAs and from MDM. For more information, see “Clearing active alarms for DPN” (page 361).
- **Global Clear** clears alarms from the appropriate Passports and MDM servers. For more information, see “Clearing active alarms for Passport” (page 368).

When status records, model data, customer data, and diagnostic information display in the Information list, the following commands are available from the pop-up menu:

- **Copy** copies selected text to the clipboard.
- **Select All** selects all text in the Information list.
- **Deselect All** cancels the selection of any text.
- **Copy Component to Target Field** copies the current text selection, or the text surrounding the cursor position, to the Information for field for use as another command. In the absence of a selection, the command tries to identify a component ID in the text around the cursor position and then uses this text as the subcomponent portion in the Information for field. For example, using the output of a Passport list command, click somewhere on one of the output component names and select Copy Component to Target Field. The copied component becomes the subcomponent in the Information for field. Pressing the Shift key and double-clicking the middle mouse button on text in the information list performs the same function as the Copy Component to Target Field command.

## Preference boxes

The Component Information Viewer contains the following boxes:

- Auto-Context
- Auto-Refresh
- Refresh Display

### Auto-Context

The Auto-Context button controls whether or not the Component Information Viewer tools automatically retrieves components from context. For example, if you turn on automatic context and then select a component in any of the MDM tools that support context, that component information automatically displays in the Component Information Viewer window. You can also set Auto-Context in the Preference Settings Dialog box. For details on using this dialog, see “Setting Preferences” (page 350). For more information about component context, see “Context” (page 38).

### Auto-Refresh

The Auto-Refresh button controls whether or not the information in the Component Information Viewer window automatically refreshes. The refresh interval is set in the Preference Settings Dialog. You can also set Auto-Refresh in the Preference Settings Dialog. For details on using this dialog, see “Setting Preferences” (page 350).

## Refresh button

The Refresh Display button lets you immediately refresh the contents of the Component Information Viewer window.

## Customizing the Component Information Viewer display

You can customize the following items in the Component Information Viewer:

- “Alarm list” (page 319)
- “Related components list menu” (page 320)
- “Information for field pop-up menu” (page 320)
- “Component Information Viewer Diagnostic Command menu” (page 321)

- “Other resources” (page 321)

## Alarm list

For procedures on customizing the Start Tool menu for the Alarm List, see the section on customizing the toolsets and Start Tools menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

When you modify the Start Tool menu file, use one of the following substitution variables in the command line:

- `$SEVERITY`: the Common format severity of the alarm, which can be UNKNOWN, CRITICAL, MAJOR, MINOR, WARNING, or CLEARED
- `$DPNSEV`: the DPN format severity of the alarm which can be ncsUnknown, ncsDEGRADE, ncsOVERLOAD, ncsMINOR, ncsMAJOR, or ncsWILDCARD
- `$EVENT`: the type of the alarm which can be CLEAR, SET, or MESSAGE
- `$DPNMNEM`: the DPN alarm mnemonic, which can be TRAPDATA, ACTIVATE, INVALID, MISSING, DUPLICAT, MEMORY, CONJEST, FAILED, REFUSED, TIME\_OUT, CRITICAL, OOS, THRESHLD, ENABLED, DISABLED, PROBE, CALL\_BLK, or DISCARD. This variable has a value for DPN alarms only.
- `$DPNACTION`: the Network Control System (NCS) action value, which can be ncsServiceData, ncsHardware, ncsSoftware, ncsSecurity, ncsProtocol, ncsDebug, ncsNetwork, ncsEngineering, ncsOperations, ncsUnclassified, or ncs Wildcard. This substitution value is for DPN alarms only.
- `$FCODE`: the alarm fault code. This eight-digit fault code is used to specify the alarm. The first four digits are used to identify the source of the alarm, and the last four digits are used to identify the alarm.
- `$DATE`: the date of the alarm in the format:YY-MM-DD
- `$TIME`: the time of the alarm in the format:HH:MM:SS
- `$COMP`: the internal component name of the target
- `$DCOMP`: the display component name of the target

- **\$DTYPE**: the DPN device type. This variable has a value for DPN alarms only
- **\$FORMAT**: the present format of an alarm, which can be **TERSE**, **NORMAL**, or **FULL**
- **\$TYPE**: the alarm type, which can be communications, qualityOfService, processing, equipment, environment, security, operator, debug, or unknown. This value gives a general explanation of the cause of the alarm.
- **\$RAWSTATE**: the corresponding component's raw state
- **\$CMT**: the operator comment data text
- **\$OPER**: the operator data text

### Related components list menu

For procedures on customizing the Start Tool menu for the Related Components List, see the section on customizing the toolsets and Start Tools menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

When you modify the file, you one of the following substitution variables on the command line:

- **\$COMP**: the internal component name of the target
- **\$DCOMP**: the display component name of the target

### Information for field pop-up menu

You can customize the pop-up menu that opens when you right-click on the triangle at the right of the Information for field. This pop-up menu contains the Get Context command and a list of up to 10 of the last targeted components. If you frequently use the same components, you can customize the list so that it contains these frequently used component names or name patterns. To customize the list, create one of the following files:

- To customize the list for a single user (\$HOME), create the file `$HOME//MagellanNMS/CIVInfoTargets.cfg`.
- To customize the list for all users of the workstation, create the file `/opt/MagellanNMS/cfg/CIVInfoTargets.cfg`.

- For second-party integrators customizing the list for all users of the workstation, create the file  
`/opt/MagellanNMS/ext/lib/cfg/CIVInfoTargets.cfg`

The Component Information Viewer searches for custom files in the order they are listed in the preceding bulleted list. The first file found is used to populate the list.

The file format is as follows:

```
# comments are blank lines, or lines that
# start with #, !, or *
labelString: <label to appear in the menu>
value: <component name or patterns to be used
      as a target upon selection>
```

## Component Information Viewer Diagnostic Command menu

For details about customizing the Diagnostic Command menu, see the section on diagnostic menu management in 241-6001-301 *Preside MDM Customization Administrator Guide*.

## Other resources

You can customize the resources to control

- the colors associated with propagated states, problem states, and severity
- whether or not the problem states are shown in the related components list
- whether or not the bell rings upon error

The table “Resources for color control of propagated states” (page 322) lists the resources you use to control the colors associated with the propagated states displayed by Component Information Viewer components. This table also lists the resources you use to control the state color at the module level. If the value of this resource is true, then the unknown state color at the module level is different from the default unknown color.

**Table 44**  
**Resources for color control of propagated states**

Resource	Description	Legal values
*stateINVALID *stateUNKNOWN *stateINSV *stateSTB_1 *stateSTB_2 *stateSTB_3 *stateSTB_4 *stateSTB_5 *stateOOS_1 *stateOOS_2 *stateOOS_3 *stateOOS_4 *stateOOS_5 *stateMTCE *stateHIER_MTCE *stateACKED moduleStateUNKNOWN	Specifies the state-to-color mapping used to indicate the current state of the components in the Related Components List. (These are the same resources used for the NV.)	Any legal X windows color or specification. See 241-6001-301 <i>Preside MDM Customization Administrator Guide</i> .
<hr/>		

The table “Resources for color control of common alarms” (page 323) lists the resources you use to control the colors associated with the common alarm format severity displayed by the Component Information Viewer components.

**Table 45**  
**Resources for color control of common alarms**

Resource	Description	Legal values
*BackgroundColorUnknown *ForegroundColorUnknown *BackgroundColorCritical *ForegroundColorCritical *BackgroundColorMajor *ForegroundColorMajor *ForegroundColorMinor *BackgroundColorMinor *BackgroundColorWarning *ForegroundColorWarning *BackgroundColorCleared *ForegroundColorCleared *BackgroundColorDefault *ForegroundColorDefault	Specifies the background and foreground color-to-severity mappings for the common alarm formats.	Any legal X windows color or specification. See 241-6001-301 <i>Preside MDM Customization Administrator Guide</i> .

The table “Resources to control the ringErrorBell” (page 323) lists the resources you use to control the ringErrorBell.

**Table 46**  
**Resources to control the ringErrorBell**

Resource	Description	Legal values
CIV*ringErrorBell	If True, the Component Information Viewer rings the bell when it cannot find data for a target. If False, the Component Information Viewer does not ring the bell. The default is True.	True or False

The table “Resources for customizing the Acknowledgement/unacknowledgement Alarms Dialog” (page 324) lists the resources you use to customize the *Acknowledge Alarms Dialog* and the *Unacknowledge Alarms Dialog*.

**Table 47**  
**Resources for customizing the Acknowledgement/unacknowledgement Alarms Dialog**

Resource	Description	Legal values
*AckAlarmDlog*userIdFieldField.editable	If True, the <i>User</i> field in the dialog used for acknowledging or unacknowledging alarms, can be modified. The default is False.	True or False
*AckAlarmDlog*commentData.maxLength	The maximum length of <i>Reason</i> text that can be specified when acknowledging or unacknowledging alarms. The default length is 256.	Any legal <i>Motif</i> value associated with the <i>MaxLength</i> resource.
CIV*differentModuleUnknownColor	If <i>differentModuleUnknownColor</i> is true, then the unknown color for the node at the module level is different from the default unknown.	True or False

**Table 48**  
**Resources for Customer Database component ID alias**

Resource	Description	Legal values
CIV*cdbSupportAlias	Enables support for Customer Database component name aliasing.	True to enable alias support, False (default) to prevent alias support

## Diagnostic commands

The Component Information Viewer window supports the following diagnostics:

- “Select Command Route” (page 326)
- “Command Console” (page 326)
- “Query Historical Alarms” (page 326)
- “Passport Commands” (page 326)
- “Passport Tests” (page 328)
- “Passport Inventory” (page 330)
- “DPN Commands” (page 331)
- “DPN Inventory” (page 333)
- “NRS Commands” (page 334)
- “Passport Port Test Console” (page 335)

The availability of the commands varies according to the configuration at your installation. The following subset of diagnostic commands are always available:

- Select Command Route...
- Command Console...
- Query Historical Alarms...

- Help

## Select Command Route

The Select Command Route... command is always available from the Commands list. Selecting this command opens the Connection Console dialog box to connect to, or disconnect from, a destination. This dialog also lets you select the default destination for diagnostic commands.

## Command Console

The Command Console... command is always available from the Commands list. Selecting this command starts the Command Console tool with the component specified in the Component Information Viewer.

## Query Historical Alarms

The Query Historical Alarms... command is always available from the Commands list. This command opens the Real-Time Alarm Collection (RTAC) Access tool. This tool consists of a two-page dialog that lets you specify filters for retrieving RTAC spooled alarms. For details about this tool, see “Query Historical Alarms” (page 383). For procedures on using this tool from Component Information Viewer, see “Querying historical alarms from Component Information Viewer” (page 375).

## Help

The Help command is always available from the Commands list. Selecting this command opens the online documentation for Command diagnostics.

## Passport Commands

Except where indicated, commands in the table “Passport Command diagnostics” (page 327) apply to all Passport component types. The table lists all Passport diagnostic commands, however the list of available Passport Commands at your installation may differ.

**Table 49**  
**Passport Command diagnostics**

Passport Command	Description	Command line equivalent
Describe Component	Displays all attributes of the target component and any of its subcomponents. The subcomponents are listed by instance. For example, if multiple Dlcis are defined for a specified FrUni, all are listed.	
List Comps	Lists the first level subcomponents of the Passport.	<code>list -o -p</code>
Display LPs	Displays all attributes of all LPs.	<code>display -o -p lp/*</code>
Display LP	Opens the Passport Component Selector dialog box and lets you select a single LP for which the attributes will display.	<code>display -notab -o -p lp/&lt;selected&gt;</code>
Display Cards	Displays all attributes of all.	<code>display -notab -o -p shelf cards/* CARDS</code>
Display Trunks	Displays all attributes of all Passport Trunks.	<code>display -notab -o -p trk/*</code>
Display Software	Displays the current loaded software versions.	<code>display -p sw</code>
Display Provisioning	Displays all attributes of provisioned components.	<code>display -o prov</code>
List Files	Opens a dialog box that prompts for a file path and then lists the files in the specified path.	<code>list -file -path ("&lt;file path&gt;") fs</code>
List Subcomponents	Lists all subcomponents of a target component.	<code>list -o -p &lt;target&gt;</code> (for subcomponents only)
Display Attributes	Displays all attributes of the target component.	<code>display -notab -o -p &lt;target&gt;</code> (for subcomponents only)
(Sheet 1 of 2)		

**Table 49 (continued)**  
**Passport Command diagnostics**

Passport Command	Description	Command line equivalent
Display Subcomps	Displays all attributes of all subcomponents of the target component.	<code>display -notab -o -p &lt;target&gt; *</code> (for subcomponents only)
Display Stats Delta	Opens a dialog box that prompts for the time delta and optional repeat count and then starts the MDM Passport Delta script. The script displays changes in all the attribute values of the target between sampling intervals. Use for subcomponents only.	
Display Connections	Available for Frame Relay (FrUni, FrNNi, FrAtm), and AtmIf and their subcomponents. This command lists their connection components (Dlcis, Vccs, Vpcs, Vpts, and Vpt-Vccs) indicating their state and any correlation IDs.	
Display Troubled Conn	Similar to Display Connections, but only lists the disabled connections. This command requires that the target Passport node support be at least PCR 2.x software. Otherwise, it acts like the Display Connections command.	
Help	Opens the online documentation for Passport Commands.	
(Sheet 2 of 2)		

## Passport Tests

The table “Passport Test diagnostics” (page 329) lists all Passport test and trace commands, however the list of available commands at your installation may differ.

**Table 50**  
**Passport Test diagnostics**

Passport Test	Description	Command line equivalent
Ping IP Address	Prompts with an input dialog the IP address to ping and then pings that address through the corresponding Virtual Router.	<code>ping -ipAddr (&lt;IP address&gt;) -traceRoute &lt;target VR prefix&gt; ip icmp</code> (for virtual routers and their subcomponents only)
Trace AtmIf Circuit	Traces the Atm Virtual Circuit.	<code>trace &lt;target VCC prefix&gt;</code> (for ATM VCCs only)
Trace AtmIf Path	Traces the Atm Virtual Path.	<code>trace &lt;target VPC or VPT prefix&gt;</code> (for ATM VCCs and VPTs only)
Ping DPRS Node	Starts the DPRS Ping command and traces the path followed to reach the target RID, MID, or remote DLCI.	<code>ping -roundTripDelay -allPaths &lt;target RID prefix&gt;</code> (for RTG-RID components only)  <code>ping -roundTripDelay -allPaths &lt;target MID prefix&gt;</code> (for RTG-MID components only)  <code>ping -roundTripDelay &lt;target DLCI prefix&gt;</code> (for Frame Relay DLCI components only)
Trace PORS Connection	Traces a PORS connection across one or more routing regions (through the gateways), and reports the Logical Channels, Gateway Calls, and applications used (applicable to TRK, RGTY, TRK-LCH, RGTY-CALL, VS, HTDS, and BTDS components. For TRK and RGTY, connections on the Trunk or Routing Gateway are traced)	

(Sheet 1 of 2)

**Table 50 (continued)**  
**Passport Test diagnostics**

Passport Test	Description	Command line equivalent
Port-Interface Test	starts the Passport Port Test Console. Use for port-interface and service components only. For details, see “Passport Port Test Console” (page 335).	
Help	Opens the online documentation for Passport Tests.	
(Sheet 2 of 2)		

## Passport Inventory

For details on Passport Inventory reports, see the section on Passport Inventory reports in 241-6001-808 *Preside MDM Device Inventory Tools User Guide*. Passport Inventory commands are applicable to any Passport component type. Depending on availability, you may see the following set of Passport inventory reporting utilities

The table “Passport Inventory diagnostics” (page 330) lists all of the Passport Inventory reporting utilities, however the list of available utilities at your installation may differ.

**Table 51**  
**Passport Inventory diagnostics**

Passport Inventory	Description
Module Report	Opens the Passport Module Summary Inventory report for the target module.
Card Report	Opens the Passport Card Inventory report for the target module.
Trunk Report	Opens the Passport Trunk Inventory report for the target module.
Software Report	Opens the Passport Software Inventory report for the target module.
ATM Report	Opens the Passport ATM Services Inventory report for the target module.
(Sheet 1 of 2)	

**Table 51 (continued)**  
**Passport Inventory diagnostics**

Passport Inventory	Description
FrameRelay Report	Opens the Passport FrameRelay Services Inventory report for the target module.
Help	Opens the online documentation for Passport Inventory.
(Sheet 2 of 2)	

## DPN Commands

**Table 52**  
**DPN Command diagnostics**

DPN Command	Description	Command line equivalent
List Active DPNs	Lists the currently active DPNs below the current default OA destination.	This command maps to the existing dpnup macro. Use for DPN AN CA components
Display DPN Calls	Lists all active calls on the target port.	This command maps to the AllCall macro. Use for port components only.
OA Directory	Lists the OA hierarchy below the target OA.	<target OA name> DIR (for OA components only)
OA List	Lists the OZ hierarchy below the target OA.	<target OA name> OA LIST
Module Stats	Displays the module level statistics.	(D STATS)
Display MCFs	Displays the active MCF information.	(D MCF)
Display Spooling Sys.	Displays the current state of the spooling system (local or remote).	DSP D
Display File Sys.	Displays the current state of the file system.	FILE D
List PEs	Lists the available PEs on the target module.	D
List MCFs	Lists the available MCFs on the target module.	LIST MCF
(Sheet 1 of 3)		

**Table 52 (continued)**  
**DPN Command diagnostics**

DPN Command	Description	Command line equivalent
List File(s)...	Prompts for a file name pattern and then lists the matching files from the file system of the target module.	FILE DIR <name pattern>
Query Module	Displays the module level configuration information for the target module.	Q MOD
Query Switch	Displays the switch level configuration information for the target module	Q SWITCH
Query Network	Displays network level configuration for the target module.	Q NET
Query All on Module	Displays configuration for the target module.	Q *
PE Hardware	Displays hardware status information for the target PE.	<target PE> D HARD (for PEs and their subcomponents only)
PE Image	Displays the active software image for the target PE.	<target PE> D IMAGE (for PEs and their subcomponents only)
PE Stats	Displays statistics for the target PE.	<target PE> D STAT (for PEs and their subcomponents only)
Query PE	Displays configuration information for the target PE.	<target PE> Q for PEs and their subcomponents only
Display Ports	Displays the Ports below the target PI.	<target PI> D (for PIs and their subcomponents only)
Query PI	Displays configuration information for the target PI.	<target PI> Q (for PIs and their subcomponents only)
(Sheet 2 of 3)		

**Table 52 (continued)**  
**DPN Command diagnostics**

DPN Command	Description	Command line equivalent
Display Link	Displays link information for the target PO.	<target PO> D LINK (for Ports and their subcomponents only)
Display Service	Displays service information for the selected PO.	<target PO> D SERV (for Ports and their subcomponents only)
Display Stats	Displays statistics information for the target PI.	<target PO> D STATS (for Ports and their subcomponents only)
Query Link	Displays link level configuration for the target PO.	<target PO> Q LINK (for Ports and their subcomponents only)
Query Service	Displays service level configuration information for the target PO.	<target PO> Q SERV (for Ports and their subcomponents only)
Query DNA	Displays DNA/CUG level configuration information for the target PO.	<target PO> Q DNA (for Ports and their subcomponents only)
Help	Opens the online documentation for DPN commands.	
(Sheet 3 of 3)		

## DPN Inventory

For details on DPN Inventory reports, see the section on DPN Inventory reports in 241-6001-808 *Preside MDM Device Inventory Tools User Guide*.

The table “DPN Inventory diagnostics” (page 334) lists all of the DPN Inventory reporting utilities, however the list of available utilities at your installation may differ.

**Table 53**  
**DPN Inventory diagnostics**

DPN Inventory	Description
Full Module Report	Opens the DPN Full Module Inventory report for the target module
Module Summary Report	Opens the DPN Module Summary Inventory report for the target module.
PE Report	Opens the DPN PE Inventory report for the target module.
PI Report	Opens the DPN PI Inventory report for the target module.
SCR Report	Opens the DPN Source Call Router Inventory report for the target module.
NL/Trunk Report	Opens the DPN Network Link and Trunk Inventory report for the target module.
Help	Opens the online documentation for DPN inventory.

## NRS Commands

For details about the Network Reporting System (NRS), see 241-6001-022 *Preside MDM Network Reporting System User Guide*. Except where indicated, all commands apply to any DPN or Passport component types. The table “NRS Command diagnostics” (page 334) lists all of the NRS reporting utilities, however the list of available utilities at your installation may differ.:

**Table 54**  
**NRS Command diagnostics**

NRS Command	Description
Find DNA	opens a dialog and prompts for a DNA GREP pattern. The pattern is then passed to the nrsFinddna utility to identify the component(s) that support it.
Configuration Report	opens the xnrsdatah utility for multiple graphical display reports with the parameters Module, Report on fields, Filtered and Current set.
(Sheet 1 of 2)	

**Table 54 (continued)**  
**NRS Command diagnostics**

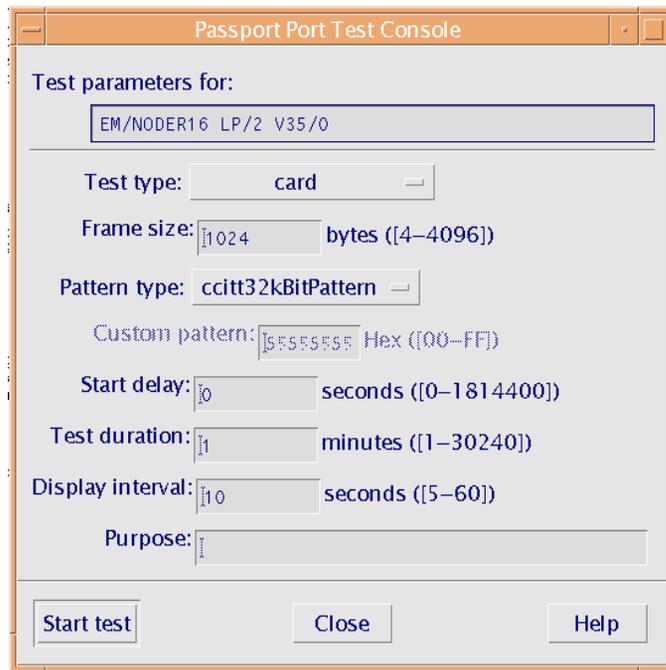
NRS Command	Description
Configuration Diff	opens the xnrsdiff utility for multiple graphical display reports with the Module parameter set to the target component, the Dated parameter set to the latest dated configuration (source) and the Current parameter (destination) set.
DPN Service Config	opens the nrdserv NRS utility and reports the target node's service configuration. Use for DPN components only.
Help	Opens online documentation for NRS Command.
(Sheet 2 of 2)	

## Passport Port Test Console

The Passport Port Test Console opens a dialog that prompts for the test parameters and target component ID. The component ID can be the name of the actual port-interface to test or a service component that uses the port.

The figure “The Passport Port Test Console dialog” (page 336) shows the Passport Test Dialog

**Figure 38**  
**The Passport Port Test Console dialog**



### Passport Port Test Console dialog

The dialog controls map to the standard Passport Port-Interface Test components, with the exception of display interval. The controls are as follows:

- **Test parameters for:** specifies the target component name. The component name can be either a port interface (for example, V35, X21, DS1, Sonet) or a service component (for example, FrUni, Trk, DpnGate). If you specify a service component, the tool automatically identifies the port-interface in use.
- **Test type:** supports a list of port tests. Port tests include card, manual, localLoop, remoteLoop, externalLoop, payloadLoop, remoteLoopThisTrib, v54RemoteLoop, and pn127RemoteLoop.
- **Frame size:** specifies the size of frames to send.

- **Pattern type:** supports a list of pattern types to send in those frames. Pattern types include ccitt32kBitPattern, ccitt8MBitPattern, and customizedPattern.
- **Custom pattern:** is available only if you use the pattern type customizedPattern and lets you specify a bit pattern for the test frames.
- **Start delay:** specifies (in seconds) the delay before the test starts.
- **Test duration:** specifies (in minutes) the duration of the test.
- **Display interval:** specifies (in seconds) the delay between the sampling of intermediate results. Note that this is not the same as the on-switch attribute. Passport only emits results in minute intervals. So, to provide intermediate results in less than one-minute intervals, this tool polls for results rather than waiting for Passport to send them.
- **Purpose:** lets you specify the reason for performing the test.

For more information about Passport port tests, see 241-1501-610 *Passport 15000 FP Configuration and Testing Guide* and 241-7401-610 *Passport 7400 FP Configuration and Testing Guide*

### **Port test console output**

The Port Test Console automatically locks the interface, starts the test, and regularly polls the port-interface for the test's intermediate results. The output goes to standard output (Component Information Viewer Diagnostics). When started from a UNIX Access window or macro, the output can be sent to an xmsg window or a file.

The figure “Passport Port Test Console output (xmsg window)” (page 338) shows a sample port test output.

**Figure 39**  
**Passport Port Test Console output (xmsg window)**

	Sent/Recv	Sent/Recv	Sent/Recv	Received	Rate	(min)
1	2359	2415616	19324928		0	0e+00
	2358	2414592	19316736			
2	4469	4576256	36610048		0	0e+00
	4468	4575232	36601856			
3	6589	6747136	53977088		0	0e+00
	6588	6746112	53968896			
4	8711	8920064	71360512		0	0e+00
	8710	8919040	71352320			
5	10831	11090944	88727552		0	0e+00
	10830	11089920	88719360			
6	12570	12871680	102973440		0	0e+00
	12570	12871680	102973440			

Test completed (testTimeExpired) after 60 seconds.

Frame Rate: 209 Frames/sec  
 Byte Rate: 214528 Bytes/sec  
 Bit Rate: 1716224 Bits/sec  
 Frame Error Rate: 0 %

Dismiss

The test output consists of a header, test parameters, a summary of the current configuration and operational parameters of the port, a table with the intermediate results, and a footer summarizing the test results, and the current operational state once again, in case it changed.

### Sample Passport Port Test Console output (full text)

The following example shows the a sample of the full text of the Passport Port Text output.

```
Port-interface card test
for EM/NODEYBC5 LP/4 V35/3 (EM/NODEYBC5 FRUNI/4300).
-----
Test Parameters:
  Test Frames: 1024 byte(s) frames with pattern
  Duration: 1 minute(s) with a 0 second(s) start delay
  polling for results every 10 seconds
```

Current port-interface configuration:

```

applicationFramerName = FrUni/4300 Framer
  clockingSource = local
  commentText =
  customerIdentifier = 0
dataTransferLineState = rfs dsr dcd rts
dteDataClockSource = fromDce
enableDynamicSpeed = no
  ifAdminStatus = up
  ifIndex = 59
  lineSpeed = 192000 bit/s
lineStatusTimeOut = 1000 msec
  linkMode = dte
  readyLineState = rfs dsr dcd rts
  vendor =

```

Current port-interface state:

```

actualLinkMode = dte
actualRxLineSpeed = 192000 bit/s
actualTxLineSpeed = 192000 bit/s
dataXferStateChanges = 4
  lineState = rfs dsr dcd ~rts

```

Sample	Frames Sent/Recv	Bytes Sent/Recv	Bits Sent/Recv	Err. Frms Received	Bit Err Rate	Remaining (min)
1	2359	2415616	19324928	0	0e+00	1
	2358	2414592	19316736			
2	4469	4576256	36610048	0	0e+00	1
	4468	4575232	36601856			
3	6589	6747136	53977088	0	0e+00	1
	6588	6746112	53968896			
4	8711	8920064	71360512	0	0e+00	1
	8710	8919040	71352320			
5	10831	11090944	88727552	0	0e+00	1
	10830	11089920	88719360			

```

6          12570      12871680    102973440          0      0e+00      0
          12570      12871680    102973440
-----

```

Test completed (testTimeExpired) after 60 seconds.

```

Frame Rate:      209 Frames/sec
Byte Rate:      214528 Bytes/sec
Bit Rate:      1716224 Bits/sec
Frame Error Rate: 0 %

```

Current port-interface state:

```

actualLinkMode = dte
actualRxLineSpeed = 192000 bit/s
actualTxLineSpeed = 192000 bit/s
dataXferStateChanges = 5
lineState = rfs dsr dcd rts

```

The tool expects that the appropriate Passport group is already connected. For this reason, the Component Information Viewer Diagnostics uses this tool as an argument to the `execWithDest` utility.

The tool's command line follows:

```

/opt/MagellanNMS/bin/ppPortTest
  [-ask|-noask]
  [-stay]
  [-o <output file> | -x]
  [-fsize <frame size>]
  [-type <test type>]
  [-pat <pattern type>]
  [-cust <custom pattern>]
  [-delay <start delay in seconds>]
  [-duration <test duration in minutes>]
  [-interval <display interval in seconds>]
  [-purpose <string>]
  <port-interface/service component ID>

```

where:

```

-ask|-noask  specifies whether the dialog is invoked. If you specify
-ask, the dialog always opens and prompts for the test parameters. If you

```

specify `-noask`, the dialog does not open and testing proceeds with the parameters provided on the command line.

`-stay` does not close the dialog after the test completes to allow you to start a test on a different component. This option is most useful with the `-x` option).

`-o <output file>|-x` specifies the destination of the test output. If you specify `-o` and an output file name, the test output is sent to that file. If you specify `-x`, the output is sent to an independent xmsg window. A new window opens for each test. By default, the output is sent to the standard output stream.

`-fsize <frame size>` specifies the size of frames to send.

`-type <test type>` specifies the port type test.

`-pat <pattern type>` specifies the pattern types to send in the frames.

`-cust <custom pattern>` specifies a bit pattern for the test frames.

`-delay <start delay>` specifies (in seconds) the delay before the test starts.

`-duration <test duration>` specifies (in minutes) the duration of the test.

`-interval <results polling interval>` specifies (in seconds) the delay between the sampling of intermediate results.

`-purpose <test purpose>` specifies the default values for the corresponding fields in the dialog.

`<port-interface/service component ID>` specifies the target component for the test in display or canonical format with the specified module specified (for example, `EM/NODEYBC5 LP/4 V35/4` or `EM/NODEYBC5 FRUNI/44`).

## Procedures

This section provides procedures for using the Component Information Viewer tool.

### Getting Started

- “Starting Component Information Viewer without context” (page 344)
- “Starting Component Information Viewer with context” (page 345)
- “Exiting Component Information Viewer” (page 346)
- “Displaying Component Information Viewer online help” (page 347)

### Using filters and preferences

- “Setting component filters” (page 348)
- “Setting Preferences” (page 350)
- “Using previously saved preference settings” (page 354)

### Working with related components

- “Setting a target in the related components panel” (page 355)
- “Setting the acknowledge state for a component” (page 356)
- “Setting the maintenance state for a component” (page 357)
- “Starting other MDM tools from Component Information Viewer” (page 358)

### Displaying additional information

- “Setting a target in the information panel” (page 359)
- “Displaying additional component information” (page 360)
- “Clearing active alarms for DPN” (page 361)
- “Clearing a Passport alarm using Local Clear” (page 362)
- “Clearing a Passport alarm using Global Clear” (page 363)
- “Clearing a Passport alarm using the Global Clear tool” (page 365)
- “Clearing active alarms for Passport” (page 368)

- “Acknowledging active alarms” (page 369)
- “Unacknowledging active alarms” (page 370)

**Displaying diagnostics**

- “Displaying diagnostic information” (page 371)
- “Selecting a new command route” (page 373)
- “Querying historical alarms from Component Information Viewer” (page 375)

## Starting Component Information Viewer without context

Use this procedure to start the Component Information Viewer tool without component context.

### Expected results

Starting the Component Information Viewer tool without context opens the tool without populating it with any component information. When the window opens, you need to specify the component for which you want information.

### Procedure steps

- 1 In the Preside Multiservice Data Manager window, select **Fault** and then **Component Information Viewer**.

The Component Information Viewer window opens.

## Starting Component Information Viewer with context

Use this procedure to start the Component Information Viewer tool with component context. Context lets you transfer component information among those Preside Multiservice Data Manager (MDM) tools that also support context:

You can start the Component Information Viewer tool with context from the following Preside Multiservice Data Manager (MDM) tools:

- Network Viewer
- Alarm Display
- Network Status Bar
- Component Status Display
- Circuit Viewer

### Expected results

When you start the Component Information Viewer tool from other MDM tools, the Component Information Viewer tool opens and automatically displays information about the component in context.

### Procedure steps

- 1 From any of the Preside Multiservice Data Manager (MDM) tools that support context, select a component.
- 2 Open the **Start Tools** pop-up menu, point to **Fault** and then select **Component Information Viewer**.

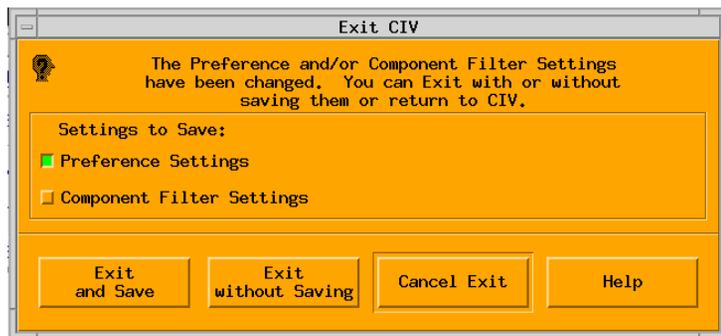
The Component Information Viewer opens and the **Related Components for** and **Information for** fields are populated with the component in context.

## Exiting Component Information Viewer

The Exit CIV dialog box opens when you modify any preference or component filter settings and do not save these changes before you try to exit the Component Information Viewer tool. Use the Exit CIV dialog box to specify how your changes are to be handled.

### Procedure steps

- 1 If you try to exit Component Information Viewer without saving changes to the preference or filter settings, the **Exit CIV** dialog opens.



- 2 From the **Exit CIV Dialog** box, select one of the following actions:
  - **Exit and Save** to exit Component Information Viewer and save the modified settings
  - **Exit without Saving** to exit Component Information Viewer without saving the changes
  - **Cancel Exit** to cancel the exit operation and return to the Component Information Viewer window
  - **Help** to display online help

## Displaying Component Information Viewer online help

Use this procedure to view online help for the Component Information Viewer tool. You can display various types of online help.

### Procedure steps

#### Help On Context

Help on Context displays online information about a specific area of the Component Information Viewer window.

- 1 From the Component Information Viewer **Help** menu, select **On Context**.  
The mouse pointer changes to a question mark (?).
- 2 Move the mouse pointer onto an area of the window for which you want help and click the mouse button.  
The online help window opens with information specific to the area you selected.

#### Help on Window

Help on Window provides a description of the elements of the Component Information Viewer window.

- 1 From the Component Information Viewer window **Help** menu, select **Help on Window**.  
The online help window opens with a description of the Component Information Viewer window.

## Setting component filters

Use the Component Filter Settings Dialog box to limit the number of related components that display in the related components panel. You can filter components based on raw or propagated states.

### Expected results

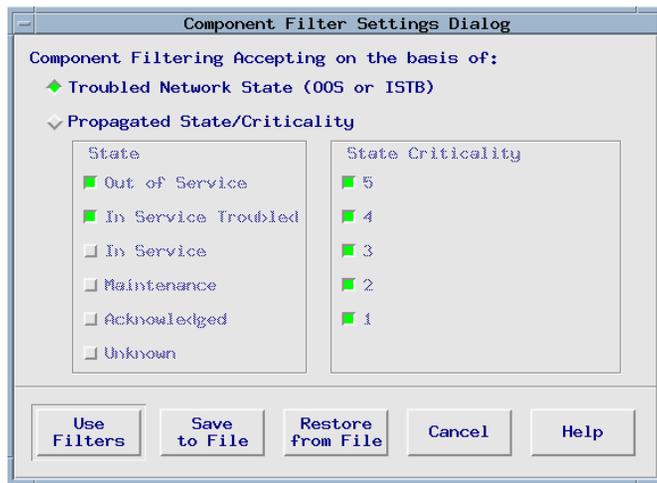
The Troubled Network State (OOS or ISTB) filter option displays only those components that have a raw state of Out-Of-Service (OOS) or In-Service-Troubled (ISTB). Components with a state of Acknowledged or Maintenance but are still OOS or ISTB are also included.

The Propagated State/Criticality filter option displays only those components that have the propagated states and state criticalities that you select. You need to select at least one propagated state and one state criticality. The criticality values range from 1 (lowest) to 5 (highest) and are only used for the OOS and ISTB states.

### Procedure steps

- 1 In the Component Information Viewer **Filter** list box, select **On**.
- 2 From the **Options** menu, select **Change Component Filter Settings....**

The **Component Filter Settings** Dialog box opens.



- 3 Select either the **Troubled Network State (OOS or ISTB)** or **Propagated State/Criticality** filter option. If you select **Propagated State/Criticality**, then you also need to specify at least one state value and one criticality value.
- 4 When you finish modifying filter settings, use one of the following buttons to specify how the settings are to be used:
  - To apply the new settings, click **Use Filters**.
  - To save the new settings to a file, click **Save to File**. The settings are saved to the file \$HOME/MagellanNMS/CIVfilt.cfg.
  - To restore filter settings from an existing \$HOME/MagellanNMS/CIVfilt.cfg file, click **Restore from File**.
  - To cancel any changes that you made to the **Component Filter Settings Dialog** box, click **Cancel**.

## Setting Preferences

Use the Preference Settings Dialog box to control the following set of Component Information Viewer operating parameters:

- **Auto-Context** controls whether or not the Component Information Viewer window automatically updates the related components and information panels whenever a new component is put in context.
- **Auto-Raise Window** controls whether or not the Component Information Viewer window automatically moves to the top of the window stack when a context operation occurs. If Auto-Raise window is turned off, the Component Information Viewer window will not move to the top of the window stack, however a bell will sound to indicate a context change. Auto-Raise Window is available only when Auto-Context is turned on.
- **Auto-Refresh** controls whether or not the Component Information Viewer window regularly refreshes the contents of the related components and information panels.
- **Refresh Interval (sec)** controls the number of seconds between refreshes. Refresh Interval (sec) is available only when Auto-Refresh is turned on. The interval represents the number of seconds the Component Information Viewer waits after a completed refresh before attempting another one. If one panel cannot refresh in time before a new cycle starts, it is ignored. The failure of one panel being refresh in time does not stop the other from being updated.
- **Alarm Format** controls the level of alarm information that displays in the information panel. Terse displays the least amount of alarm information, Full displays the most, and Normal displays a mid range.
- The **CDB database name** and **server host** fields identify the name and server to access for customer database (CDB) information. Customer information displays in the information panel when the Information Type box is set to Customer Data. Customer information also displays when you select Recent Alarms or Active Alarms using full format.
- The **Insert matching data from CDB server in alarms** checkbox controls whether or not the Component Information Viewer window automatically displays customer information that matches the component IDs in common full format alarms.

- **Display component ID alias from the CDB server in alarms** is available only if you have enabled alias substitution. Use this checkbox to specify whether or not to display aliases in alarms.

## Prerequisite

The Alarm Display provides an option to substitute an alias for a component name in the display of alarms. By default, this functionality is disabled. To use aliases, you first need to enable the functionality. Then, you can use the CDB Preferences Dialog to turn the display of aliases on or off.

To enable alias substitution, you need to modify the CIV\*cdbSupportAlias resource. For details, see the section on customizing resources used by MDM tools in 241-6001-301 *Preside MDM Customization Administrator Guide*.

After alias substitution has been enabled, an additional checkbox (Display component ID alias from the CDB server in alarms) displays in the CDB Preferences Dialog so that you can chose whether or not to display the aliases.

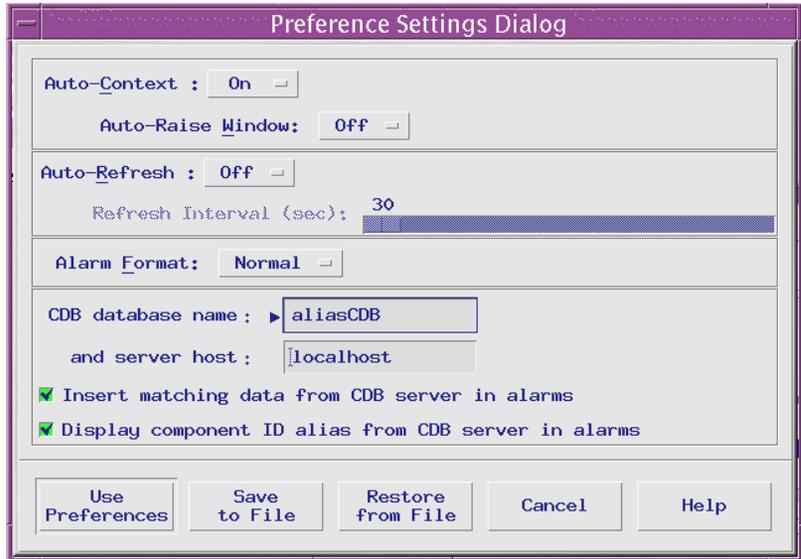
## Expected results

When alias substitution is enabled, the component name is replaced by the alias in the Customer Database's Related Component field. The alias displays in all alarm formats. However, a new second line displays in the normal and full formats to indicate the real component name.

## Procedure steps

- 1 From the **Options** menu, select **Change Preference Settings...**

The **Preference Settings Dialog** box opens.



- 2 To change the automatic context setting, in the **Auto-Context** list box, select **On** to enable automatic context, or **Off** to disable it.
- 3 To change the setting for raising the Component Information Viewer window to the top of multiple windows whenever the context changes, in the **Auto-Raise** list box, select **On** to enable raising the window, or **Off** to disable it.
- 4 To change the automatic refresh setting, in the **Auto-Refresh** list box, select **On** to enable automatic refreshing, or **Off** to disable it.
- 5 To set the refresh interval, move the **Refresh Interval (sec)** slider left to decrease the time interval or right to increase it.
- 6 To set the alarm format, from the Alarm Format list, select **Terse**, **Normal**, or **Full**.
- 7 To display customer database information in the window, specify the name of the customer database to use for data retrieval in the **CDB database name** field and the name of the server host in the **and server host** field.
- 8 To display customer data in the alarms, select the **Insert matching data from CDB server in alarms** checkbox.

- 9 If you have enabled alias substitution and the **Display component ID alias from the CDB server in alarms** checkbox is available, select the checkbox to turn on the display of aliases, or clear the checkbox to turn off the display.
- 10 When you finish modifying preferences, use one of the following buttons to specify how the preferences are to be used:
  - To apply the new settings, click **Use Preferences**.
  - To save the new settings to a file, click **Save to File**. The settings are saved to the file \$HOME/MagellanNMS/CIVPref.cfg.
  - To restore preference settings from an existing \$HOME/MagellanNMS/CIVPrefs.cfg file, click **Restore from File**.
  - To cancel any changes that you made to the **Preference Settings Dialog** box, click **Cancel**.

## Using previously saved preference settings

Use this procedure to retrieve and apply previously stored preference settings. The settings are restored from your *\$HOME/MagellanNMS/CIVPrefs.cfg* file.

### Procedure steps

- 1 From the **Options** menu, select **Change Preference Settings....**  
The **Preference Settings Dialog** window opens.
- 2 Click **Restore from File**.  
The restored settings display in the dialog box.
- 3 To apply the filter settings, click **Use Preferences**.  
The restored settings, with the exception of the sash position, are applied to the Component Information Viewer window.

## Setting a target in the related components panel

To display related information about a component in the Component Information Viewer window, you need to target, or specify, the name of a component or subcomponent for which you want related information.

### Expected results

The type of related component information that the Component Information Viewer displays is shown in the table “Related components” (page 355).

**Table 55**  
**Related components**

Target component	Related information
Organizational node	Next level links, nodes, and the parent node.
Link	Endpoint components, parent components, and links.
Module	All subcomponents of the module, all links terminating on the module and the parent component.
Subcomponent	All subcomponents of the subcomponent, all links terminating on the subcomponent and all parents up to the module.

### Procedure steps

- 1 To target a component in the related components panel, select one of the following methods:
  - Type the name of the component in the **Related Components for** text field and then press the Enter key.
  - Right-click the triangle at the end of the **Related Components for** field and from the resulting **Get Context** pop-up menu select a component.
  - If the related components list has entries, right-click on an entry and from the resulting pop-up menu select **Show Related**.
  - From the **Auto-Context** list box, select **On** and then select a component in another monitoring tool.

## Setting the acknowledge state for a component

Use this procedure to set the acknowledge state on or off. Setting the acknowledged state on temporarily hides the current troubled state of a component causing the acknowledged component to behave as if in-service.

The availability of the on or off command depends on the current acknowledge state of the component. If a component is not in acknowledge state, you can set the acknowledge state on. If a component is currently in acknowledge state, you can set the acknowledge state off.

### Expected results

If no related components are troubled, the acknowledged component displays a state of acknowledged (ACKED). When an acknowledged component changes state, the acknowledgment is automatically removed and the real state of the component is shown. For more information on Acknowledged state, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

A component is also put into acknowledged state by acknowledging all active alarms against the component.

### Procedure steps

- 1 To set the acknowledge state on or off, use one of the following actions:
  - To set the acknowledge state on, right-click on a component in the related components list and then from the resulting pop-up menu, select **Set Acknowledge State On**.
  - To set the acknowledge state off, right-click on an acknowledged component in the related components list and then from the resulting pop-up menu, select **Set Acknowledge State Off**.

## Setting the maintenance state for a component

Use this procedure to set the maintenance state on or off. Setting the maintenance state permanently hides the current troubled state of a component. Any children of the selected component are also put into maintenance state. For more information on maintenance state, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

The availability of the on or off command depends on the current maintenance state of the component. If a component is not in maintenance state, you will be able to set the maintenance state on. If a component is currently in maintenance state, you will be able to set the maintenance state off.

### Procedure steps

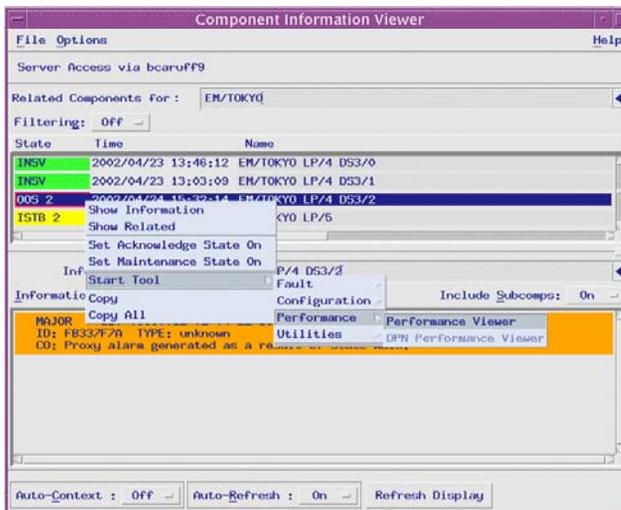
- 1 You can set the maintenance state on or off. Use one of the following actions.
  - To set the maintenance state on, right-click on a component in the related components list and then from the resulting pop-up menu, select **Set Maintenance State On**.
  - To set the maintenance state off, right-click on an acknowledged component in the related components list and then from the resulting pop-up menu, select **Set Maintenance State Off**.

## Starting other MDM tools from Component Information Viewer

Use this procedure to start other MDM tools to view additional fault management data without exiting from the Component Information Viewer. For more details about starting other MDM tools, see “Start Tool” (page 39).

### Procedure steps

- 1 Right-click on a component in the related components list.  
A pop-up menu opens
- 2 On the pop-up menu, point to **Start Tool**, then point to one of the Start Tool categories, and then select the appropriate MDM software tool.



## Setting a target in the information panel

To display additional component information in the Component Information Viewer window, you need to target, or specify, the name of a component or subcomponent for which you want additional information.

### Procedure steps

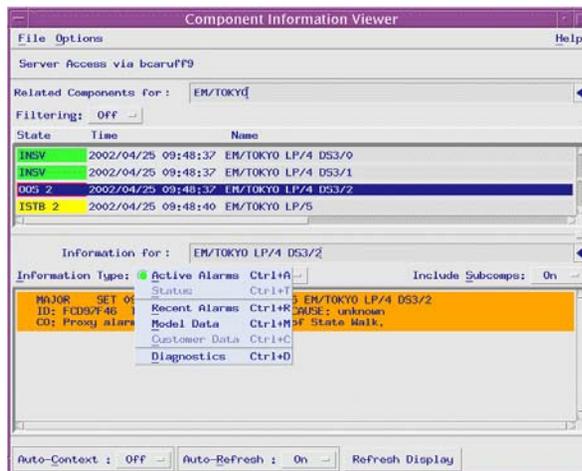
- 1 To target a component in the information panel, select one of the following methods:
  - Type the name of the component in the **Information for** text field and then press the Enter key.
  - Right-click the triangle at the end of the **Information for** field and from the resulting **Get Context** pop-up menu select a component.
  - Right-click on a component in the related components list and select **Show Information** from the resulting pop-up menu.
  - With **Auto-Context** turned off, double-click on a component in the related components list.
  - With **Auto-Context** turned on, select a component in the related components panel.
  - With **Auto-Context** turned on, select a component from another MDM tool that supports component context.

## Displaying additional component information

Use the information panel to further investigate information. You can display management or diagnostic information to help diagnose a fault and determine its impact.

### Procedure steps

- 1 Set a target in the **Information for** field. For details, see “Setting a target in the information panel” (page 359).
- 2 In the information panel, click the **Information Type**: list box to display a list of information types to apply to the target component.
  - To display the currently active alarms for the component, select **Active Alarms**. To display alarms for the component and all its subcomponents, in the **Include Subcomps**: list box, select **On**.
  - To display the most recent status record from a DPN component, select **Status**.
  - To display the alarm history, select **Recent Alarms**.
  - To display network model information, select **Model Data**.
  - To display data from the customer database, select **Customer Data**.
  - To display diagnostic commands, select **Diagnostics**.



## Clearing active alarms for DPN

If you need, you can clear active alarms from the information panel in the Component Information Viewer window.

### Procedure steps

- 1 If the information panel is not set to display alarms, display alarms using the following steps:
  - a. Specify a target for which you want alarms in the **Information for:** field.
  - b. From the Information Type: list box, select **Active Alarms**.
- 2 In the information list, select the alarm that you want to clear.
  - To select contiguous multiple alarms, click the first alarm in the range and then shift-click the last alarm in the range.
  - To select non-contiguous multiple alarms, click the first alarm and then ctrl-click additional alarms.
- 3 Right-click on a selected alarm in the information list to open a pop-up menu.
- 4 You can clear alarms from several different menu selections:
  - While holding down the right-mouse button, select **Local Clear** or **Global Clear** and then release the mouse button.
  - While hold down the right-mouse button, select **Start Tool ->Fault->Global Clear of Alarm**.
- 5 Click **Refresh**.

### Expected results

- If you clicked **Local Clear**, the alarm is cleared from the GMDR/DMDR/FMDR/SMDR/IMDR database.
- If you clicked **Local Clear** or **Global Clear**, your userID, hostname, and the “DISPLAY” environment variable value will be displayed in the comment data of the resulting **Clear Alarm**
- If you clicked **Global Clear**, the alarm is cleared from the GMDR/DMDR database and from the active alarm list stored on the OA in the network

## Clearing a Passport alarm using Local Clear

You can clear Passport alarms locally from the Component Information Viewer window to clear them from the MDM servers. This procedure is intended for any MDM operator and multiple alarms can be cleared at one time.

### Prerequisites

- The GMDR server must be up and running.

### Procedure steps

- 1 If the information panel is not set to display alarms, display alarms using the following steps:
  - a. Specify a target for which you want alarms in the **Information for:** field.
  - b. From the Information Type: list box, select **Active Alarms**.
- 2 In the information list, select the alarm that you want to clear.
  - To select contiguous multiple alarms, click the first alarm in the range and then shift-click the last alarm in the range.
  - To select non contiguous multiple alarms, click the first alarm and then ctrl-click additional alarms.
- 3 Right-click on a selected alarm in the information list to open a pop-up menu.
- 4 Select **Local Clear** and then release the mouse button.

A Confirmation dialog box is displayed asking “You are about to clear the selected alarm(s) locally from MDM. Are you sure you want to clear the alarm(s)?” Select Yes if you are sure you want to locally clear the alarms. Select No if you do not want to clear the alarms.
- 5 Click **Refresh** or wait for the next refresh period for alarms to disappear.

### Expected results

- The alarm is cleared from the GMDR/FMDR databases.
- Your userID, hostname, and the “DISPLAY” environment variable value will be displayed in the comment data of the resulting **Clear Alarm**.

## Clearing a Passport alarm using Global Clear

You can clear Passport alarms globally from the Component Information Viewer window to clear them out of the MDM servers and the on-switch databases. This procedure is intended for any MDM operator and multiple alarms can be cleared at one time.

### Prerequisites

- Passport Global alarm clearing must be configured on the DMA server.
- The GMDR servers must be up and running.
- The GMDR server must be able to access a DMA server through its configuration.

### Procedure steps

- 1 If the information panel is not set to display alarms, display alarms using the following steps:
  - a. Specify a target for which you want alarms in the **Information for:** field.
  - b. From the Information Type: list box, select **Active Alarms**.
- 2 In the information list, select the alarm that you want to clear.
  - To select contiguous multiple alarms, click the first alarm in the range and then shift-click the last alarm in the range.
  - To select non contiguous multiple alarms, click the first alarm and then ctrl-click additional alarms.
- 3 Right-click on a selected alarm in the information list to open a pop-up menu.
- 4 Select **Global Clear** and then release the mouse button.

A Confirmation dialog box is displayed asking “You are about to clear the selected alarm(s) globally from MDM. Are you sure you want to clear the alarm(s)?” Select Yes if you are sure you want to globally clear the alarms. Select No if you do not want to clear the alarms.
- 5 Click **Refresh** or wait for the next refresh period for alarms to disappear.

If one or more requests failed, a dialog box opens with the error messages.

### Expected results

- Your userID, hostname, and the “DISPLAY” environment variable value will be displayed in the comment data of the resulting **Clear Alarm**.
- The alarm is cleared from the GMDR/FMDR databases and from the active alarm list stored on the Passports in the network.

## Clearing a Passport alarm using the Global Clear tool

You can clear a Passport alarm globally from the Component Information Viewer window to clear it out of the MDM servers and the on-switch database. This procedure requires that the MDM operator set up connection authentication first. Only one alarm can be cleared at a time.

### Prerequisites

- The Host Group Directory Services (HGDS) server and the Passport Comms Mgr server (FDTM) must be up and running.

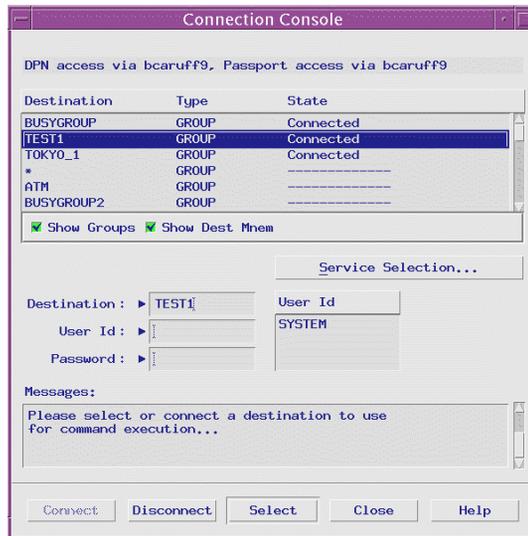
### Procedure steps

- 1 If the information panel is not set to display alarms, display alarms using the following steps:
  - a. Specify a target for which you want alarms in the **Information for:** field.
  - b. From the Information Type: list box, select **Active Alarms**.
- 2 In the information list, select the alarm that you want to clear.
- 3 Right-click on a selected alarm in the information list to open a pop-up menu.
- 4 Select **Start Tool -> Global Clear of Alarm** and then release the mouse button.

A Confirmation dialog box is displayed asking “You are about to clear the selected alarm(s) globally from MDM. Are you sure you want to clear the alarm(s)?” Select Yes if you are sure you want to globally clear the alarms. Select No if you do not want to clear the alarms.

The **Connection Console** dialog box opens and displays the first Passport group to which the node belongs. The **Connection Console**

dialog box does not display if you are already connected to a group that contains the Passport.



- 5 Connect to a destination. Use the default selected destination or select another destination.
- 6 Type a valid user ID in the **User Id** text box.
- 7 Type a valid password in the **Password** text box.  
You can repeat steps 5-7 as often as needed.
- 8 Click **Connect**.
- 9 Select a connected destination using one of the following steps:
  - Double-click on a connected network destination in the **Destination** list.
  - Select a connected network destination in the **Destination** list and then click **Select**.
  - Select the Passport wild-card route (\*). The wild card lets you direct commands to Passport nodes in any of the connected groups without having to know which group the node belongs to.

If the request failed, a dialog box opens with the error message.

### **Expected results**

- Your userID, hostname, and the “DISPLAY” environment variable value will be displayed in the comment data of the resulting Clear Alarm.
- The alarm is cleared from the GMDR/FMDR databases and from the active alarm list stored on the Passports in the network.

## Clearing active alarms for Passport

If you need, you can clear active alarms from the information panel in the Component Information Viewer window.

### Procedure steps

- 1 If the information panel is not set to display alarms, display alarms using the following steps:
  - a. Specify a target for which you want alarms in the **Information for:** field.
  - b. From the Information Type: list box, select **Active Alarms**.
- 2 In the information list, select the alarm that you want to clear.
  - To select contiguous multiple alarms, click the first alarm in the range and then shift-click the last alarm in the range.
  - To select non contiguous multiple alarms, click the first alarm and then ctrl-click additional alarms.
- 3 Right-click on a selected alarm in the information list to open a pop-up menu.
- 4 You can clear alarms from several different menu selections:
  - While holding down the right-mouse button, select **Local Clear** or **Global Clear** and then release the mouse button.
  - While hold down the right-mouse button, select **Start Tool ->Fault->Global Clear of Alarm**.
- 5 Click **Refresh**.

### Expected results

- If you clicked **Local Clear**, the alarm is cleared from the GMDR database.
- If you clicked **Global Clear**, the alarm is cleared from the GMDR/FMDR database and from the active alarm list stored on the Passport in the network.
- If you clicked **Local Clear** or **Global Clear**, your userID, hostname, and the “DISPLAY” environment variable value will be displayed in the comment data of the resulting **Clear Alarm**.

## Acknowledging active alarms

Use this procedure to acknowledge an active alarm. You acknowledge an alarm to let others know that the fault is under investigation. You can remove the acknowledgement with the unacknowledge command.

### Expected results

Acknowledged alarms display a check mark on the left of the alarm list, both in active mode and log mode, even though alarms can only be acknowledged from active mode. If you display the alarms in full format the date and time of the acknowledgement, the user ID, and the reason for the acknowledgement displays in the alarm list.

### Procedure steps

- 1 If the information panel is not set to display alarms, display alarms using the following steps:
  - a. Specify a target for which you want alarms in the **Information for:** field.
  - b. From the Information Type: list box, select **Active Alarms**.
- 2 In the information list, select the alarm that you want to acknowledge.
  - To select contiguous multiple alarms, click the first alarm in the range and then shift-click the last alarm in the range.
  - To select non contiguous multiple alarms, click the first alarm and then ctrl-click additional alarms.
- 3 Right-click on a selected alarm in the information list and select **Acknowledge Alarms on Component**  
The **Acknowledge Alarm(s) Dialog** box opens.
- 4 Type a reason for the action and a user ID (if the user ID field has been configured to be editable). The default is <UnixUserID>@<Hostname>.
- 5 Click **Ack Alarm(s)**.

## Unacknowledging active alarms

Use this procedure to remove the acknowledgement from active alarms.

### Expected results

Unacknowledged alarms display a crossed-out check mark icon on the left of the alarm list, both in active mode and log mode, even though alarms can only be unacknowledged from active mode. If you display the alarms in full format the date and time of the unacknowledgement, the user ID, and the reason for the unacknowledgement display in the alarm list.

### Procedure steps

- 1 If the information panel is not set to display alarms, display alarms using the following steps:
  - a. Specify a target for which you want alarms in the **Information for:** field.
  - b. From the Information Type: list box, select **Active Alarms**.
- 2 In the information list, select the alarm that you want to unacknowledge.
  - To select contiguous multiple alarms, click the first alarm in the range and then shift-click the last alarm in the range.
  - To select non-contiguous multiple alarms, click the first alarm and then ctrl-click additional alarms.
- 3 Right-click on a selected alarm in the information list and select **Unacknowledge Alarms on Component**  
The **Unacknowledge Alarm(s) Dialog** box opens.
- 4 Type a reason for the action and a user ID (if the user ID field has been configured to be editable). The default is <UnixUserID>@<Hostname>.
- 5 Click **Unack Alarm(s)**.

## Displaying diagnostic information

Use the diagnostic capability to diagnose network faults. The Component Information Viewer tool supports a range of diagnostics. For details about each diagnostic, see “Diagnostic commands” (page 325).

The availability of diagnostic commands depends on several factors including the type of device and whether or not the diagnostic menu has been customized at your installation. For information about customizing diagnostic menus, see the section on customizing Component Information Viewer diagnostics in 241-6001-301 *Preside MDM Customization Administrator Guide*.

### Expected results

Diagnostic information in the Component Information Viewer window does not support manual or automatic refresh commands. To update diagnostic information, you need to execute the diagnostic command again.

### Procedure steps

- 1 Set a target in the **Information for:** field to specify the component for which you want diagnostic information.
- 2 In the **Information Type:** list box, select **Diagnostics**.
- 3 In the **Commands:** list box, select one of the following commands:
  - **Select Command Route...** to open the Connection Console dialog box. For details, see “Selecting a new command route” (page 373).
  - **Command Console...** to start the Command Console tool. If no connection has been made the Connection Console dialog box opens first. For details, see “Selecting a new command route” (page 373).
  - **Query Historical Alarms...** to open the Real Time Alarm Collection (RTAC) tool to access RTAC spooled alarms. For details, see “Querying historical alarms from Component Information Viewer” (page 375).
  - **Passport Commands** to execute a selection of Passport diagnostic commands
  - **Passport Tests** to execute a selection of Passport tests.
  - **Passport Inventory** to execute a selection of Passport inventory reporting utilities

- **DPN Commands** to execute a selection of DPN diagnostic commands
- **DPN Inventory** to execute a selection of DPN inventory reporting utilities
- **NRS Commands** to execute a selection of Network Reporting System (NRS) utilities
- **Passport Port Test Console** to open a dialog box that prompts for the test parameters and target component ID.

## Selecting a new command route

The Component Information Viewer retains the last OA and Passport Group command routes. Use this procedure only if you need to establish a new connection or change the route of an OA or Passport Group.

You select a new route using the Connection Console dialog box. This dialog box lets you manage network connections by connecting to or disconnecting from a network destination and by setting a default destination.

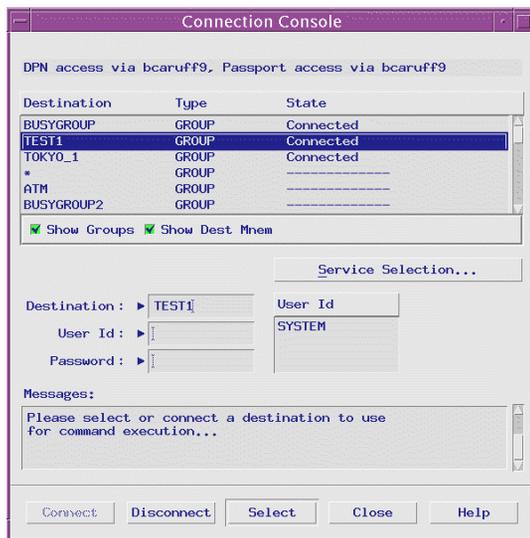
### Expected results

The Connection Console dialog box is similar to the Command Console Connection Management dialog box except for the addition of the Select button. For details, see the section on the Command Console Connection Management dialog in 241-6001-804 *Preside MDM Workstation Utilities User Guide*. The Connection Console dialog supports the Passport wild card route (\*) as a legal Passport group. Although you can select the Passport wild-card route, you cannot establish a connection with it.

### Procedure steps

- 1 In the **Information Type:** list box, select **Diagnostics**.
- 2 In the **Commands:** list box, select **Select Command Route....**

The **Connection Console** dialog box opens.



- 3 If needed, establish a connection to another network destination.
  - Click on an entry in the **Destination** list to populate the **Destination:** text box.
  - Type a valid user ID in the **User Id** text box.
  - Type a valid password in the **Password:** text box.
  - Click **Connect**.
- 4 Select a connected destination using one of the following steps:
  - Double-click on a connected network destination in the **Destination** list.
  - Select a connected network destination in the **Destination** list and then click **Select**.
  - For Passports only, select the Passport wild-card route (\*). The wild card lets you direct commands to Passport nodes in any of the connected groups without having to know which group the node belongs to.

## Querying historical alarms from Component Information Viewer

Use this procedure to start the Real-time Alarm Collection (RTAC) search tool to from Component Information Viewer. This tool accesses RTAC spooled alarms so that you can extract short-term historical alarms.

- “Prerequisite” (page 375)
- “Procedure steps” (page 375)
- “Procedure job aid” (page 378)

### Prerequisite

RTAC must be running on the same workstation as the Component Information Viewer host, or its database directory must be accessible by the Network File System (NFS).

### Procedure steps

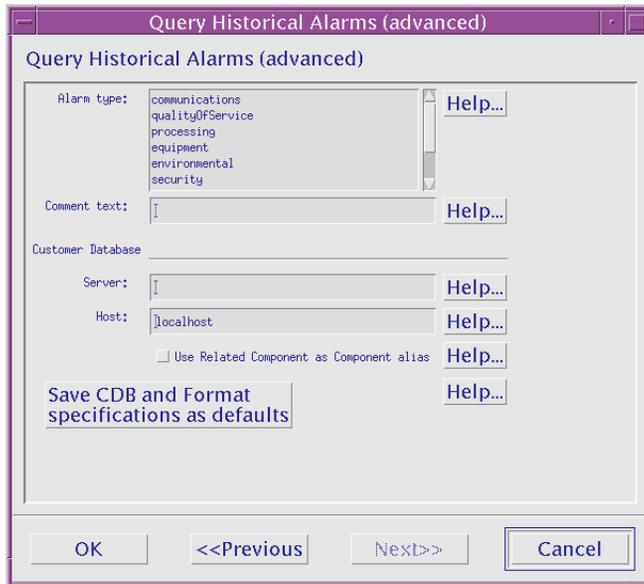
- 1 In the **Information Type:** list box, select **Diagnostics**.
- 2 In the **Commands:** list box, select **Query Historical Alarms...**

The Query Historical Alarms dialog opens and displays the first of the two-page dialog.



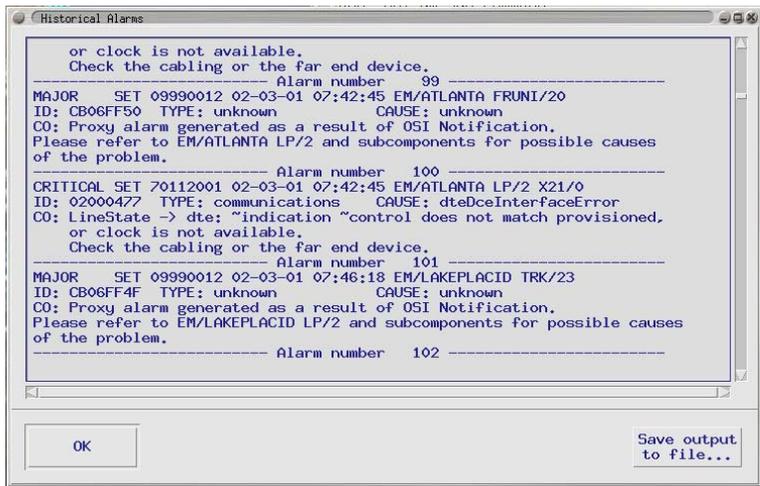
- 3 On the first page of the dialog, refine the alarm query by using the following filters. For a description of the filters, see the table “Query Historical Alarm filters” (page 378).

- 4 If you do not require any further filters, click **OK** to start the query, otherwise click **Advanced** to open the second page of the dialog.



- 5 Further refine the alarm query by using any of the following filters. For a description of the filters, see the table “Query Historical Alarm filters” (page 378).
- 6 Optionally, to save the Customer Database (CDB) options and alarm output format settings so that they are used the next time you start the Query Historical Alarms tool, click **Save CDB and Format specifications as defaults**.
- 7 To begin the historical alarm query, click **OK**.

Depending on the length of time to search for matching alarms, a tracking dialog may open. This dialog tracks the search progress. As matching alarms are identified, they display in the Historical Alarms output window.



- 8 To save the contents of the Historical Alarms dialog to a file, click **Save output to file...** or to close the dialog, click **OK**.

The Historical Alarms dialog closes.

## Procedure job aid

**Table 56**  
**Query Historical Alarm filters**

Filter	Description
<b>First page of dialog:</b>	
Component	specifies the component for which you want to retrieve alarms. By default, the Component field is populated with the component in context. If you specify a component filter, the alias filter is ignored.
(Sheet 1 of 3)	

**Table 56 (continued)**  
**Query Historical Alarm filters**

<b>Filter</b>	<b>Description</b>
or Alias	specifies the component alias. The alias replaces the component ID in the display with the matching Related Component ID value from the customer database. If you do not use a customer database, or if you specify a component filter, this alias filter is ignored.
From date/time	specifies the start of the time period for which you want alarms. The initial value for this field is the current date and time minus one day. If you override the initial value in this field or in the To date/time field and need to reestablish the initial values, click the Reset Date-Time button.
To date/time	specifies the end of the time period for which you want alarms. The initial value for this field is the current date and time. If you override the initial value in this field or in the From date/time field and need to reestablish initial values, click the Reset Date-Time button
Fault code	specifies the fault code to use for filtering alarms. You can use GREP style patterns to specify these fault codes.
Alarm event	specifies the alarm event to use for filtering alarms. If needed, you can specify multiple alarm events.
Alarm severity	specifies the alarm severity to use for filtering alarms. If needed, you can specify multiple severities.
Display format	specifies the level of alarm output to display, from the least output (terse) to the most output (full).
<b>Advanced page of dialog:</b>	
Alarm type	specifies the alarm type to use for filtering. If needed, you can select multiple types.
(Sheet 2 of 3)	

**Table 56 (continued)**  
**Query Historical Alarm filters**

<b>Filter</b>	<b>Description</b>
Comment text	text specifies the comment data pattern (GREGP) to use for filtering.
Customer Database Server	specifies the service name of the Customer Database (CDB) that has the customer data and alias information. The Query Historical Alarms tool supports the same CDB interaction as the Alarm Display and Component Information Viewer tools.
Customer Database Host	specifies the host name of the CDB that has the customer data and alias information.
(Sheet 3 of 3)	

## Errors and warnings

The Component Information Viewer provides the following error and warning messages to help you take corrective action:

- “Service Selection Warning Dialog” (page 381)
- “Save Settings Error Dialog” (page 381)
- “Restore Settings Error Dialog” (page 381)
- “Manual Alarm Clearing Error Dialog” (page 382)

### Service Selection Warning Dialog

The Service Selection Warning Dialog box indicates that the Component Information Viewer is using a new management data server due to a LAN selection change.

Update the contents of the Component Information Viewer window by clicking the Refresh Display button.

### Save Settings Error Dialog

The Save Settings Error Dialog box indicates that the preference file cannot be saved to the \$HOME/MagellanNMS/CIVPrefs.cfg file or the component filter settings file cannot be saved to the \$HOME/MagellanNMS/CIVCFilt.cfg file.

Ensure that there is write access to the home directory and the configuration file. Ensure there is sufficient disk space for the home directory.

### Restore Settings Error Dialog

The Restore Settings Error Dialog indicates that the preference file cannot be restored from the \$HOME/MagellanNMS/CIVPrefs.cfg file or the component filter settings cannot be restored from the \$HOME/MagellanNMS/CIVCFilt.cfg file.

Ensure that the configuration file exists and that there is read access to the home directory and the configuration file. If the file exists and has the appropriate permissions but the file contents are not recognized, recreate the appropriate settings using the Component Filter or Preference Settings Dialog boxes, and save them again.

## **Manual Alarm Clearing Error Dialog**

The Manual Alarm Clearing Error Dialog box opens when an alarm cannot be cleared. The dialog box displays a message indicating the cause and information used to clear the alarm.

---

## Chapter 10

# Query Historical Alarms

---

This section describes the Query Historical Alarms tool to search and display short-term historical alarms. This section contains the following topics:

- “Overview” (page 383)
- “Query Historical Alarms dialog” (page 384)
- “Procedures” (page 386)

### Overview

You can start the Query Historical Alarms tool from the Preside Multiservice Data Manager (MDM) tool set window, from within the Component Information Viewer tool, or through a command line interface.

The Query Historical Alarms tool lets you search and display short-term historical alarms. The collection and saving of these short-term alarms are done by the real-time alarm collection (RTACCOL) server. Each day, the RTACCOL creates a file for the collection of alarms (using the format “alarms.<yyyy>-<mm>-<dd>” for the file name) and stores this file in the directory defined in the RTAC.cfg configuration file. For further details about RTACCOL, see the section on the real time alarm collection tool in 241-6001-310 *Preside MDM Server Reference Guide*.

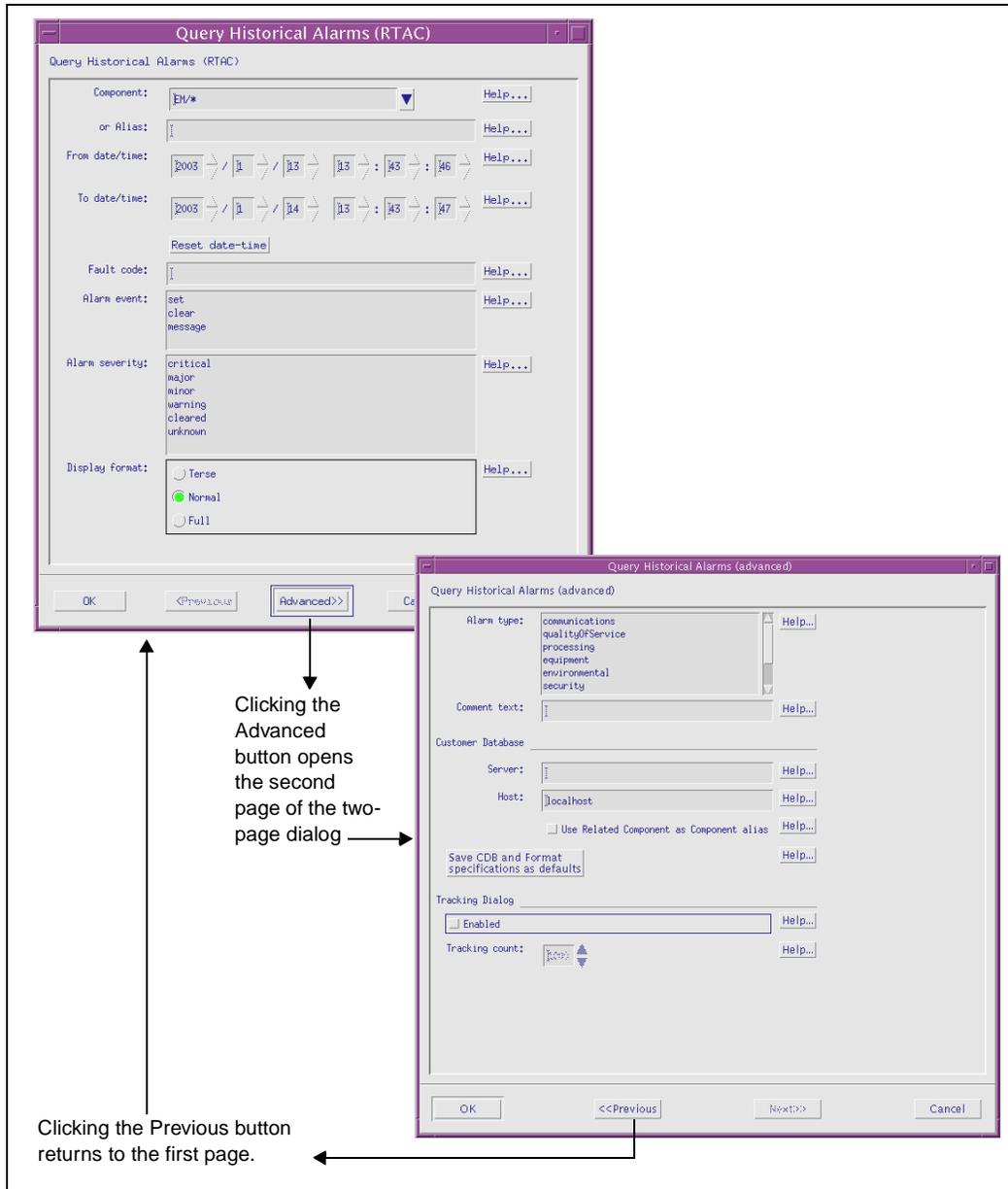
The Query Historical Alarms tool extracts information from the historical alarm files and displays its output in the Historical Alarms output dialog. When you close the output dialog, the Query Historical Alarms dialog reopens if you started the tool from the Preside MDM tool set window. If you started the Query Historical Alarms tool using Component Information

Viewer, the Query Historical Alarms dialog does not automatically reopen. In this case, you need to select the Query Historical Alarms command from Component Information Viewer once again.

## Query Historical Alarms dialog

The Query Historical Alarms dialog is a two-page dialog that contains a selection of fields to help refine the search criteria. Each field has a Help button that displays a brief explanation of the associated field. You can filter the alarm search on such parameters that include date and time ranges, fault codes, events, alarm severity, alarm types, alarm output level, and customer database services. The figure “Sample Query Historical Alarms dialog” (page 385) shows a sample dialog.

**Figure 40**  
**Sample Query Historical Alarms dialog**



## Procedures

This section contains the following procedures:

- “Querying historical alarms tool from the Preside MDM tool set window” (page 387)
- “Querying historical alarms from the command line interface” (page 392)

You can also query historical alarms from the Component Information Viewer. To do so, see the following procedures:

- “Starting Component Information Viewer without context” (page 344) or “Starting Component Information Viewer with context” (page 345)
- “Querying historical alarms from Component Information Viewer” (page 375)

## Querying historical alarms tool from the Preside MDM tool set window

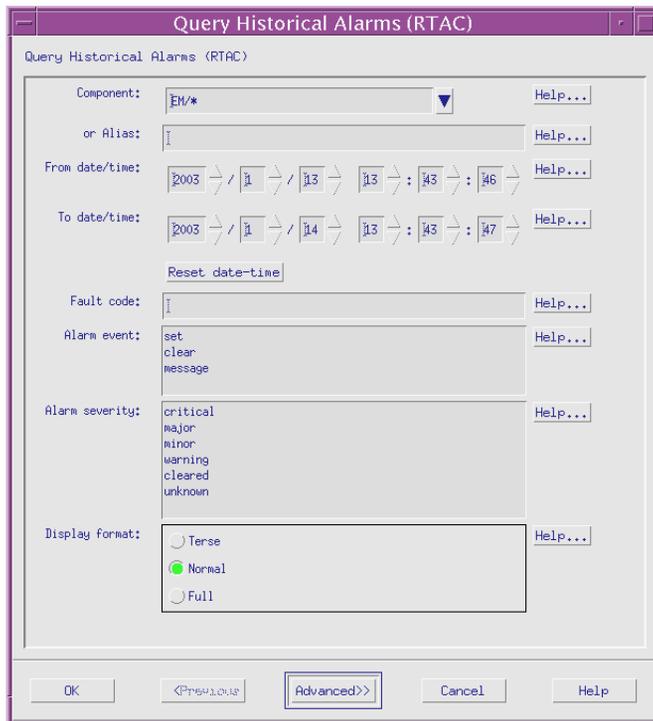
You can start the Query Historical Alarms tool using various methods. Use this procedure to start the tool from the Preside MDM tool set window.

- “Procedure steps” (page 387)
- “Procedure job aid” (page 390)

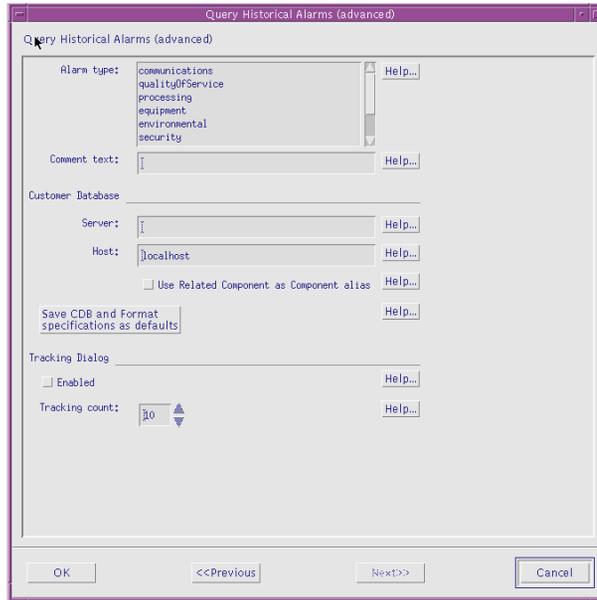
### Procedure steps

- 1 In the Preside Multiservice Data Manager window, select **Fault -> Query Historical Alarms**.

The Query Historical Alarms dialog opens and displays the first of the two-page dialog.



- 2 On the first page of the dialog, refine the alarm query by using the following filters. For a description of the filters, see the table “Query Historical Alarms filters” (page 390).
- 3 If you do not require any further filters, click **OK** to start the query, otherwise click **Advanced** to open the second page of the dialog.



- 4 Further refine the alarm query by using any of the following filters. For a description of the filters, see the table “Query Historical Alarms filters” (page 390).
- 5 Optionally, to save the Customer Database (CDB) options and alarm output format settings for the next time you start the Query Historical Alarms tool, click **Save CDB and Format specifications as defaults**.
- 6 Optionally, to display a tracking dialog that counts the alarms scanned during the search, click to select the **Enabled** check box.
  - To control the number of alarms scanned before the tracking dialog refreshes, change the value in the **Tracking count** box. Turning on tracking may slow the search.
- 7 To begin the historical alarm query, click **OK**.

The **Historical Alarms** dialog box opens.



If you enabled tracking, the tracking dialog also opens.



As matching alarms are identified they display in the **Historical Alarms** output window. When the scan is complete, the tracking dialog closes.

- 8 To save the contents of the Historical Alarms dialog box to a file, click **Save output to file...** or to close the dialog box, click **OK**.

The Historical Alarms dialog box closes and the Query Historical Alarms dialog box reopens so that you can make further alarm queries.

## Procedure job aid

**Table 57**  
**Query Historical Alarms filters**

Filter	Description
<b>First page of dialog:</b>	
Component	specifies the component for which you want to retrieve alarms. By default, the component is EM/*, which retrieves all Passport alarms. Alternatively, you can specify the component for which you want alarm information. If you specify a component filter, the alias filter is ignored.
or Alias	specifies the component alias. The alias replaces the component ID in the display with the matching Related Component ID value from the customer database. If you do not use a customer database, or if you specify a component filter, this alias filter is ignored.
From date/time	specifies the start of the time period for which you want alarms. The initial value for this field is the current date and time minus one day. If you override the initial value in this field or in the To date/time field and need to reestablish the initial values, click the Reset Date-Time button.
To date/time	specifies the end of the time period for which you want alarms. The initial value for this field is the current date and time. If you override the initial value in this field or in the From date/time field and need to reestablish initial values, click the Reset Date-Time button
Fault code	specifies the fault code to use for filtering alarms. You can use GREP style patterns to specify these fault codes.
Alarm event	specifies the alarm event to use for filtering alarms. If needed, you can specify multiple alarm events.
(Sheet 1 of 2)	

**Table 57 (continued)**  
**Query Historical Alarms filters**

<b>Filter</b>	<b>Description</b>
Alarm severity	specifies the alarm severity to use for filtering alarms. If needed, you can specify multiple severities.
Display format	specifies the level of alarm output to display, from the least output (terse) to the most output (full).
<b>Advanced page of dialog:</b>	
Alarm type	specifies the alarm type to use for filtering. If needed, you can select multiple types.
Comment text	text specifies the comment data pattern (GREG) to use for filtering.
Customer Database Server	specifies the service name of the Customer Database (CDB) that has the customer data and alias information. The Query Historical Alarms tool supports the same CDB interaction as the Alarm Display and Component Information Viewer tools.
Customer Database Host	specifies the host name of the CDB that has the customer data and alias information.
(Sheet 2 of 2)	

## Querying historical alarms from the command line interface

You can start the Query Historical Alarms tool using various methods. Use this procedure to start the tool from the command line.

- “Procedure steps” (page 392)
- “Variable definitions” (page 393)
- “Procedure job aids” (page 394)

### Procedure steps

- 1 Execute the real-time alarm search tool by typing the following command syntax as one continuous command:

```
/opt/MagellanNMS/bin/rtacsrch
[-format <TERSE|NORMAL|FULL|DUMP>]
[-output <WINDOW|MORE|STDOUT|FILE <output file>]
[-noseparator]
[-start <date> [<time>]]
[-end <date> [<time>]]
[-component <component id pattern>]
[-fault <fault code pattern>]
[-cid <customer id pattern>]
[-<any alarm field name> <pattern>]
[-h]
```

## Variable definitions

Variable	Definition
-format [<TERSE NORMAL FULL DUMP>]	<p>specifies the alarm output level. The output formats correspond to those of the Alarm Display tool. Output ranges from the least output (TERSE) to the complete alarm output (FULL). DUMP format is an output of the non-empty alarm fields in format:</p> <pre>&lt;field 1 name&gt; = &lt;file 1 value&gt; &lt;field 2 name&gt; = &lt;file 2 value&gt; 336 . &lt;field n name&gt; = &lt;file n value&gt;</pre> <p>The default format is TERSE.</p>
-output [<WINDOW MORE STDOUT FILE <output file>]	<p>specifies where the output displays. WINDOW displays alarms in a scrollable window. MORE sends output to standard output using the more program. STDOUT sends output to the standard output stream. FILE sends output to the named file. The default output is WINDOW.</p>
-noseparator	<p>omits separators between alarms</p>
-start <date> [<time>]	<p>specifies the start date for the query. &lt;date&gt; and &lt;time&gt; specify the start range of the alarm records. The default start date and time is 1900-01-01 00:00:00.</p> <p>&lt;date&gt; can be in the form yymmdd, yyymmdd, yy-mm-dd, or yyyy-mm-dd.</p> <p>&lt;time&gt; can be in the form hhmmss or hh:mm:ss.</p>
(Sheet 1 of 2)	

Variable	Definition
-end <date> [ <i>time</i> ]	<p>specifies the end date for the query. &lt;date&gt; and &lt;time&gt; specify the end range of the alarm records. The default start date and time is 9999-12-31 23:59:59.</p> <p>&lt;date&gt;</p> <p>can be in the form <i>yymmdd</i>, <i>yyyymmdd</i>, <i>yy-mm-dd</i>, or <i>yyyy-mm-dd</i>.</p> <p>&lt;time&gt; can be in the form <i>hhmmss</i> or <i>hh:mm:ss</i>.</p>
-component <component ID pattern>	<p>specifies the component identifier pattern.</p> <p>&lt;component ID pattern&gt; is considered anchored (^&lt;pattern&gt;\$).</p>
-fault <fault code pattern>	<p>specifies a fault code pattern.</p> <p>&lt;fault code pattern&gt; is considered anchored (^&lt;pattern&gt;\$).</p>
-cid <customer Id pattern>	<p>specifies a customer identifier pattern.</p> <p>&lt;customer Id pattern&gt; is considered anchored (^&lt;pattern&gt;\$).</p>
-<any alarm field name> <pattern>	<p>&lt;any alarm field name&gt; can be any field present in an alarm record. The list of available fields is available in the <i>ala.rdf</i> file.</p> <p>&lt;pattern&gt; is considered anchored (^&lt;pattern&gt;\$).</p>
-h	displays command line usage information.
(Sheet 2 of 2)	

### Procedure job aids

The table “Command line abbreviations” (page 395) details those command line options that support abbreviations:

**Table 58**  
**Command line abbreviations**

Option	Abbreviation
format	fo
output	o
noseparator	nos
start	s
end	e
component	co or compId
fault	fa or faultcode
cid	ci or customerId

The figure “Sample rtacsrch command lines” (page 396) provides sample rtacsrch command lines

**Figure 41**  
**Sample rtacsrch command lines**

<p>Examples:</p> <p>rtacsrch</p> <p>This command extracts every alarm and prints them in TERSE format. The alarms are displayed in a scrollable window.</p> <p>rtacsrch -s 00-01-12 -e 20000227 13:04:58 -fo normal -co "EM/NODEA FRUNI/7.*" -o file NODEA_7.alarms</p> <p>This command line extracts the alarms related to FRUNI 7 on Passport NODEA that were generated between January 12, 2000 at midnight and February 27, 2000 at 13:04:58. The alarms are printed in NORMAL format and saved in file NODEA_7.alarms</p>
--

The table "Exit codes for rtacsrch command" (page 396) details the exit codes from rtacsrch command.

**Table 59**  
 Exit codes for rtacsrch command

Exit code	Description
0	Normal success
1	Major errors were found
2	Terminated because of signal received

# Chapter 11

## Component Status Display

---

This section describes the Component Status Display and provides you with instructions on how to use this tool. The following information is included:

- “Component Status Display overview” (page 397)
- “Component status” (page 399)
- “Component Status Display main window” (page 401)
- “Keyboard shortcuts” (page 409)
- “Component Status Display dialogs” (page 409)
- “Component Status Display procedures” (page 417)
- “Setting Component Status Display preferences” (page 423)
- “Customizing the Component Status Display” (page 425)

### Component Status Display overview

The Component Status Display is a monitoring tool that provides a textual display of the current state or criticality of network model components. Component Status Display allows you to view status at the following levels:

- region
- site
- module
- components

The Component Status Display provides the same basic functionality as the Network Viewer tool, which monitors the network graphically, but provides the information in text form.

The Component Status Display is equipped with preference dialogs that let you

- set up filtering to display the status of one or more component types based on Troubled Raw state, or Propagated state and Criticality
- sort information displayed for components based on the component name, the Propagated state and Criticality, or the time of the last state change
- set the refresh interval for component states
- turn on or turn off automatic refreshing of component states

You can customize the Component Status Display. The Component Status Display features a Start Tool command from which you can launch other Preside Multiservice Data Manager (MDM) tools. You can customize the list of tools available from the Start Tool command. For details, see the section on customizing the toolsets and Start Tools menu in 241-6001-301 *Preside MDM Customization Administrator Guide*. You can also customize resources such as alarm colors. For details, see “Customizing the Component Status Display” (page 425).

The Component Status Display also allows you to react to a fault by putting the component into Acknowledged state or Maintenance state.

See also...

- “Component Status Display overview” (page 397)
- “Component status” (page 399)
- “Component Status Display main window” (page 401)
- “Component Status Display dialogs” (page 409)
- “Component Status Display procedures” (page 417)
- “Setting Component Status Display preferences” (page 423)
- “Setting Component Status Display preferences” (page 423)

- “Customizing the Component Status Display” (page 425)

## Component status

The status of a component is determined by its state. Each component in the network model contains a set of core attributes to model its state. There are two categories of states: raw and propagated. Raw states apply to a single component and are produced by the Surveillance Data Servers. Propagated states reflect the impact of raw states on related components and are computed by the Surveillance Network Updater (SURNUP) or, in the case of Acknowledgment and Maintenance, are originated by the operator.

For further information on component states and criticality, see *241-6001-015 Preside MDM Network Model Administrator Guide*.

### Raw state values

Raw state values are provided by the Surveillance Data Servers and only apply to a single component. Possible raw state values are shown in the table “Raw state values” (page 399).

**Table 60**  
**Raw state values**

Raw state value	Label	Meaning
Unknown	UNK	MDM has not heard from the component and does not know its state
In-Service	INSV	The component is known to be working properly.
Out-Of-Service	OOS	The component is not working.
In-Service–Troubled	ISTB	The component is known to be In-Service but experiencing some difficulties, for example, overloaded

### Propagated state values

Propagated states consist of two elements—a state value and a criticality value (N). Possible propagated state values are shown in the table “Propagated state values” (page 400).

**Table 61**  
**Propagated state values**

Propagated state value	Label	Meaning
Unknown	UNK	MDM has not heard from the component and does not know its state.
In-Service	INSV	The component, its parents, and all its children are working properly.
Out-Of-Service-N	OOS-N	The component is not working because of a fatal fault or because one of its parents is out-of-service. N is its criticality.
Hierarchical-Out-Of-Service-N	OOS-N	The component's parents or one of its grandparents is not working and N is the component's criticality.
In-Service-Troubled-N	INST-N	The component is working but has suffered a non-fatal fault, or one of its subcomponents is troubled or out-of-service. N is the criticality of the most important subcomponent affected, if not that of the component itself.
Acknowledged	ACKED	The component has been put in acknowledged state and no other faults are apparent.
Maintenance	MTCE	The component has been put into maintenance state
Hierarchical Maintenance	HIER_MTCE	One of the component's parents has been put in maintenance state.

Propagated values are computed by the Surveillance Network Updater (SURNUP). In addition, the operator can assign the following state values:

### **Acknowledged**

In the Acknowledged state, a component's true raw state is masked. The component behaves as though it is in-service (that is, if other related components are troubled, the component's Propagated state reflects this). If no troubled-related components exist, the Acknowledged component displays an ACKED propagated state instead of INSV. If at least one endpoint of a link is ACKED and the others are ACKED, INSV, or UNKNOWN, the link also displays an ACKED propagated state. As soon as another raw state change is received from the network for the component (through alarms or other network management data), the Acknowledged state is automatically removed; the new raw state is applied and propagated. The Acknowledged state therefore acts as a temporary Maintenance state. See "Putting a component into Acknowledged state" (page 420) for procedures.

### **Maintenance**

In the Maintenance state, a component's true raw state, and that of its subcomponents, are masked. The component displays a propagated state of MTCE (its children display HIER MTCE). In contrast to the Acknowledged state, components in the Maintenance state ignore any additional raw state change from the network. The component can only be removed from the Maintenance state manually or when the model is reloaded. See "Putting a component into Maintenance state" (page 420) for procedures.

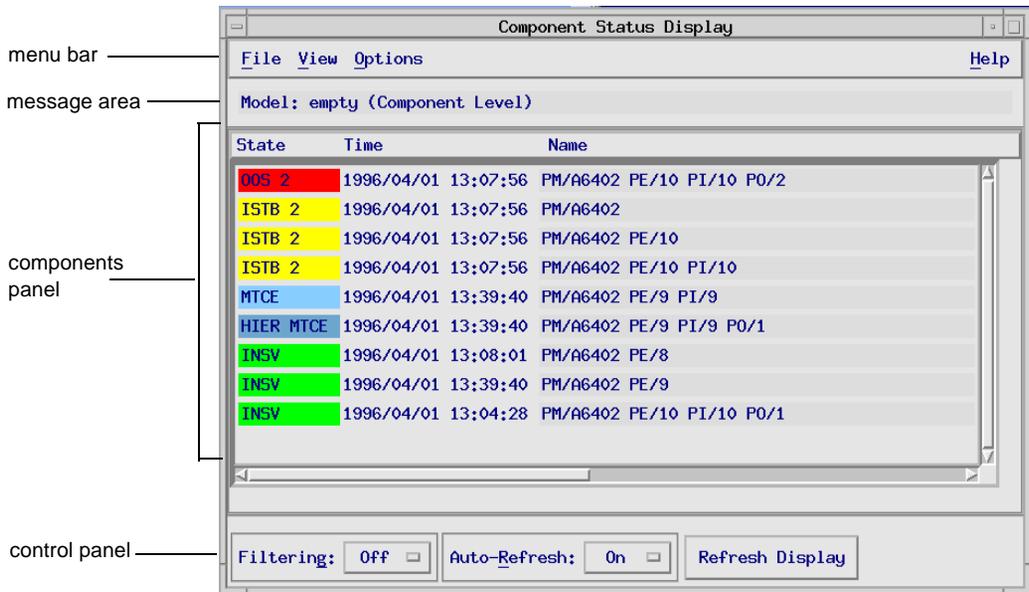
## **Component Status Display main window**

The Component Status Display main window is divided into the following areas:

- "Menu Bar" (page 402)
- "Message area" (page 404)
- "Components Panel" (page 404)
- "Control panel" (page 409)

The figure "Component Status Display main window" (page 402) shows a sample Component Status Display main window.

**Figure 42**  
**Component Status Display main window**



## Menu Bar

The menu bar contains the following command menus:

- “File menu” (page 402)
- “View menu” (page 403)
- “Options menu” (page 403)
- “Help menu” (page 404)

## File menu

The File menu contains the following command:

- **Exit** closes the Component Status Display and its dialogs. If any Preference or Component Filter settings are modified, a dialog opens and prompts you to save either, both, or none of these settings before exiting. You can also close the dialog without exiting.

### View menu

The View menu contains the following commands:

- **Select Organization** displays the available organizations and lets you choose a new organization from the current network model. Select the desired organization, then choose the *Open Organization* menu item on the display, or simply double-click on the organization. All region nodes in the selected organization are displayed.
- **Show Region Level** displays all region nodes in the current organization.
- **Show Site Level** displays all site nodes in the current organization.

*Note:* If you expand downwards (that is, the current display shows regions), you see only sites that are under the selected region(s). If no selected regions are in the list, all sites in the selected organization are shown.

- **Show Module Level** displays all module nodes in the current organization.

*Note:* If you expand downwards (that is, the current display shows sites) you see only modules that are under the selected site(s). If no selected sites are in the list, then all modules in the selected organization are shown.

- **Show Component Level** displays all component nodes in the current organization.

*Note:* If you expand downwards (that is, the current display shows modules), you see only components that are under the selected module(s). If no selected modules are in the list, then all components in the selected organization are shown.

### Options menu

The Options menu contains the following commands:

- **Change Component Filter Settings...** opens the Component Filter Settings Dialog to allow you to modify, save, and restore these settings.
- **Change Preference Settings...** opens the Preference Settings Dialog to allow you to modify, save, and restore these settings.

### Help menu

The Help menu contains the following commands:

- **On Context** displays information about a selected area of the Component Status Display window.
- **On Window** displays descriptive information about the Component Status Display window components.

### Message area

The Message Area displays the name of the network model, the level that is currently being displayed (that is, the Region, Site, Module, or Component) and the number of components in the current list. The number of components may be a subset of the total at the given level, if filtering is turned on. This area is also used for displaying a user prompt that indicates you need to select a new organization. This prompt could be the result of your request to choose a new organization, or the result of a new network model being loaded while Component Status Display is running.

### Components Panel

The Components Panel lets you monitor components at a particular level. This panel takes its information from the Network Model Coordinator and displays it in a format similar to that of the Related Components Panel of the Component Information Viewer.

The Components Panel lists components at a particular level within the organization (region, site, module, and component). For example, you can monitor only the components that meet a selected state criteria (if filtering is turned on) based on a specified sort criteria. Even with filtering turned off, you can view a subset of components at a particular level by selecting a subset of components at one level and requesting to view a lower level. For example, you can select a set of *Site* components and then ask to view the *Module* level. In this case, only the modules that are found under the selected sites are displayed at the Module Level. Then filtering can be used to further reduce the displayed list.

### Component fields

The following fields are provided for each component listed in the Components Panel:

- *State* displays the component Propagated state by name and color. The colors and names are the same as those used by the Network Viewer. See “Propagated state values” (page 400) for more information about the displayed states.
- *Time* displays the date and time of the last Propagated state change that the component has undergone. If no state change has yet occurred, this field displays the string *Never Changed*.
- *Component* displays the actual component display name.

### Component filtering

You can filter the contents of the Component Panel based on the components’ Raw or Propagated states, and component types. Component filter settings are modified through the *Component Filter Settings Dialog*, which can be opened from the *Options* menu; filtering is turned *On* or *Off* by means of the *Filtering* option button. Filtering is disabled at the Region Level and Site Level, and when organizations are displayed.

### Context

When a component is selected in the Components Panel, its name is automatically put into hot context. Any tools that are running and are set up to respond to a change in hot context automatically home to the selected component.

### Pop-up menu

The Components Panel contains a pop-up menu that displays the following commands:

- *Open Organization* opens (loads) the selected organization, clears the contents of the Components Panel, and displays the Region components for the selected organization.

**Note:** The Components Panel displays components at a particular level within the current organization. It also displays a list of the available organizations within the network model. Therefore, this menu item is only enabled when the Components Panel contains a list of organizations.

- *Show Region Level* clears the current contents of the Components Panel and populates it with the regions in the current network model. This is subject to filtering and the current selection.
- *Show Site Level* clears the current contents of the Components Panel and populates it with the sites in the current network model. This is subject to filtering and the current selection.
- *Show Module Level* clears the current contents of the Components Panel and populates it with the modules in the current network model. This is subject to filtering and the current selection.
- *Show Component Level* clears the current contents of the Components Panel and populates it with the components found in the current network model. This is subject to filtering and the current selection.
- *Set Acknowledge State On/Off* puts a component in the Acknowledged state or removes it from the Acknowledged state.

If the component is a module or subcomponent, holds a Troubled Raw state (OOS or ISTB) and is not already in the Acknowledged or Maintenance state, the Components Panel pop-up menu shows the *Set Acknowledge State On* command. Selecting the command puts the component in the Acknowledged state and triggers a refresh of the Components Panel. Since this refresh may be done automatically before the operation is complete, the resulting display might only reflect a transitional state. If in doubt, refresh the panel again within a few seconds.

If the component is already in the Acknowledged state, the pop-up menu shows the *Set Acknowledge State Off* command which, when selected, removes the component from the Acknowledged state and refreshes the Components Panel.

If none of the outlined conditions exists, the pop-up menu shows the *Set Acknowledge State On* command in a disabled state.

- *Set Maintenance State On/Off* puts a component in the Maintenance state or removes it from the Maintenance state.

If the component is not already in the Maintenance state (MTCE or HIER MTCE), the pop-up menu shows the *Set Maintenance State On* command. Selecting the command puts the component and its subcomponents into the Maintenance state and triggers a refresh of the Components Panel. Since this refresh may be done automatically before the operation is complete, the resulting display might only reflect a transitional state. If in doubt, refresh the panel again within a few seconds.

If the component is already in the Maintenance state (MTCE only), the pop-up menu shows the *Set Maintenance State Off* command which, when selected, removes the component and its subcomponents from the Maintenance state and refreshes the Components Panel.

If none of the outlined conditions exists, the pop-up menu shows the *Set Maintenance State On* command in a disabled state.

- *Start Tool* opens a menu that lists various categories of tools and utilities that you can start from Component Status Display. For details on the Start Tool menu, see “Start Tool” (page 39).
- *Copy* copies the text of an item selected in the Components Panel to the Primary Selection (accessed with the middle mouse button in a text field) and the Clipboard (accessed with the Paste Edit menu items).
- *Copy All* copies the text of all items in the Components Panel to the Primary Selection (accessed with the middle mouse button in a text field) and the Clipboard (accessed with the Paste Edit menu items).

### **Filtering option button**

The *Filtering* option button lets you activate or deactivate the Components Panel component filtering. This button provides the following options:

- *On* enables component filtering. Only the components that match the current filter settings are displayed in the Components Panel.
- *Off* disables component filtering.

**Note:** The value of this option button is part of the Component Status Display Preference Settings, and is saved and restored with the other settings. The Filtering state is, therefore, persistent across Component Status Display invocations. See “Changing the Component Filter Settings” (page 421) for procedures. See “Using previously saved filter settings” (page 422) to reverse the procedures.

Component Status Display supports these forms of component state filtering:

- filtering on Troubled Raw states
- filtering on Propagated states and Criticalities

If filtering on Troubled Raw states is selected, only components that currently hold a Troubled Raw state (OOS or ISTB) are displayed (the components for which the network sends MDM information indicating a fault). If Propagated State Filtering is selected, you can specify the specific (Propagated) states and state criticalities to be displayed. You need to select at least one state and one state criticality.

Each type of state filtering is subject to the component types that are currently selected. You need to select at least one component type.

To change the current component filter settings, open the *Component Filter Settings Dialog* from the *Options* menu.

### **Auto Refresh option button**

The *Auto-Refresh* option button turns on or turns off automatic refreshing of the Component Panel at a scheduled interval. This interval is set in the *Preference Settings Dialog*.

The options for the Auto-Refresh option button are

- *On* enables Auto-Refresh.
- *Off* disables Auto-Refresh.

**Note:** When the network model changes, the network model Coordinator notifies the Component Status Display of the change. The Component Status Display automatically refreshes its Components Panel. Auto-Refresh does not apply to the Components Panel when organization components are displayed.

### Refresh Display Button

The *Refresh Display* button forces an immediate refresh of the Components Panel. If the *Auto-Refresh* button is currently set to *On*, and the refresh triggered by the *Refresh Display* button is complete, the refresh timer is reactivated.

### Control panel

The Control Panel provides controls that apply to it, namely the *Filtering* and *Auto-Refresh* controls, and the *Refresh Display* command button. The values of controls contained within the Panel can be saved across Component Status Display invocations as part of the Preference Settings.

### Keyboard shortcuts

The Component Status Display provides the following keyboard shortcuts:

- *Ctrl + E* closes the Component Status Display tool and its dialogs.
- *Ctrl + O* executes the *Select Organization* command.
- *Ctrl + G* executes the *Show Regional Level* command.
- *Ctrl + I* executes the *Show Site Level* command.
- *Ctrl + M* executes the *Show Module Level* command.
- *Ctrl + C* executes the *Show Component Level* command.

For details on the commands run by the *Ctrl + O*, *G*, *I*, *M*, and *C* options, see “View menu” (page 403).

### Component Status Display dialogs

The Component Status Display provides the following dialogs:

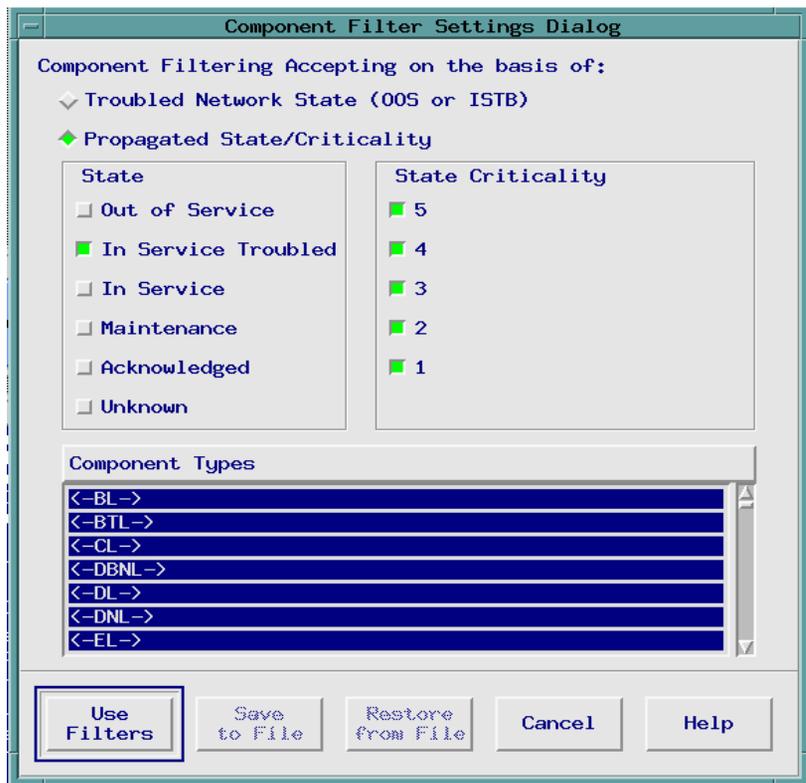
- “Component Filter Settings Dialog” (page 410)
- “Preference Settings Dialog” (page 411)
- “Exit CSD Dialog” (page 414)
- “Warning and error dialogs” (page 415)

## Component Filter Settings Dialog

The *Component Filter Settings Dialog*, sets up the Component Status Display so that it displays the component status for one or more component types. The component status is based on the raw state Troubled, or on the propagated state and criticality.

The figure “Component Filter Settings Dialog” (page 410), shows a sample Component Filter Settings Dialog.

**Figure 43**  
**Component Filter Settings Dialog**



If you select *Troubled Network State (OOS or ISTB)*, only components that currently hold an out-of-service (OOS) Troubled Raw state or an in-service Troubled Raw state (ISTB) are displayed. These are components for which the network sent the Preside Multiservice Data Manager (MDM) information indicating a fault.

If you select *Propagated State/Criticality*, you can select the specific (propagated) states and state criticalities to be displayed. You need to select at least one state and one state criticality.

Each type of state filtering is subject to the component types that are currently selected. You need to select at least one component type.

The Component Filters Setting Dialog buttons provide the following functions:

- *Use Filters* applies the new settings to the main Component Status Display main window and closes the dialog. If *Filtering* is already *On*, the Components Panel immediately refreshes to display the new settings. Applied settings are not automatically saved to file (see *Save to File* button).
- *Save to File* saves the current settings to file *\$HOME/MagellanNMS/CSDCompFilt.cfg*. The settings are not automatically applied to the main Component Status Display window (see *Use Filters* button). If the settings cannot be saved, an error dialog is displayed.
- *Restore from File* restores the settings from file *\$HOME/MagellanNMS/CSDCompFilt.cfg*. Restored settings are applied to the dialog but not to the main Component Status Display window (see *Use Filters* button). If the settings cannot be restored, an error dialog is displayed.
- *Cancel* closes the dialog. Closing the dialog neither applies nor saves the settings (click *Use Filters* or *Save to File* first).

## Preference Settings Dialog

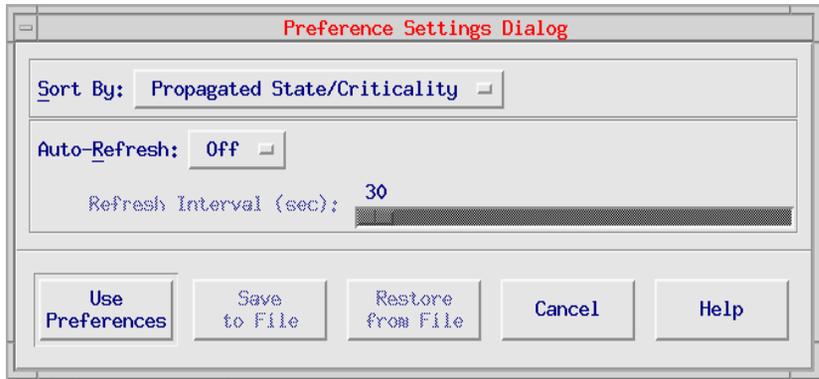
The *Preference Settings Dialog* lets you

- sort information displayed for components based on the Propagated state and Criticality, or the time of the last state change
- turn on or turn off the *Auto-Refresh*

- set the refresh interval for the component status displayed with the tool

See the figure “Preference Settings Dialog” (page 412) for an overview of the dialog.

**Figure 44**  
**Preference Settings Dialog**



The *Preference Settings Dialog* buttons provide the following functions:

- *Sort By* controls the sort key used by the Component Status Display for displaying the components in the Components Panel. This button provides the following options:
  - *Component Name* sorts the Components Panel in ascending order by component name.
  - *Propagated State/Criticality* sorts the Components Panel based on the predefined State/Criticality order listed in the table “State/Criticality label definition” (page 412).

**Table 62**  
**State/Criticality label definition**

State/Criticality	Label
1. OOS (5-1)	Out of Service
2. ISTB (5-1)	In Service Troubled
(Sheet 1 of 2)	

**Table 62 (continued)**  
**State/Criticality label definition**

State/Criticality	Label
3. ACKED	Acknowledged
4. MTCE	Maintenance
5. HIER MTCE	Hierarchical Maintenance
6. INVS	In Service
7. UNKNOWN	Unknown
8. INVALID	Invalid
(Sheet 2 of 2)	

*Time of Last State Change* sorts the Components Panel in descending order by the date/time that the component is last changed. The last component to have changed state appears at the top of the panel. Components that never changed state (that is, the time value is *Never Changed*) always appear at the end of the list.

See “Setting the sort key for the components list” (page 423) for procedures.

- *Auto-Refresh* turns on or turns off automatic refreshing of the Components Panel. This button provides the following options:
  - *On* enables *Auto-Refresh* and the *Refresh Interval* scale.
  - *Off* disables *Auto-Refresh* and the *Refresh Interval* scale.

**Note:** Turning on and turning off *Auto-Refresh* is also controlled from the Control Panel in the main window.

- *Refresh Interval* controls the number of seconds between refreshes when *Auto-Refresh* is enabled. The scale allows you to set the interval between refreshes to a value from 30 to 600 seconds (1/2 to 10 minutes).

To set the interval with the scale, see the procedures in “Setting the Auto-Refresh interval” (page 424).

- *Use Preferences* applies the new settings to the main Component Status Display window and closes the dialog. If any of the settings change, the Components Panel refreshes. Applied settings are not automatically saved to file; you need to save them using the *Save to File* button.
- *Save to File* saves the current dialog's Preference Settings to file *\$HOME/MagellanNMS/CSDPrefs.cfg*. This file is automatically restored when the Component Status Display starts up and maintains your saved settings across Component Status Display invocations.

The settings are not automatically applied to the Components Panel; you need to apply them using the *Use Preferences* button.

**Note:** When you sort by *Propagated State/Criticality*, you cannot rearrange the predetermined order of states.

- *Restore from File* retrieves the preferences that are stored in *\$HOME/MagellanNMS/CSDPrefs.cfg*. This button does not automatically apply the preferences that have been retrieved. You need to apply them using the *Use Preferences* button.

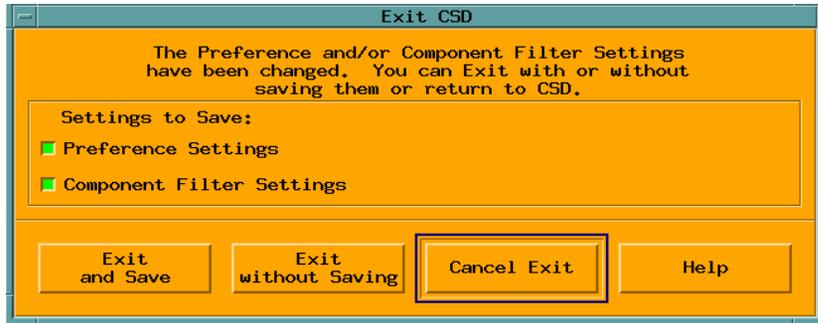
## Exit CSD Dialog

If you close the Component Status Display and do not save modified preference or component filter settings to their respective user-files, the Exit Component Status Display dialog opens. This dialog provides the following buttons and choices:

- *Exit and Save* saves the preferences or settings to a file and closes the Component Status Display Tool and its dialogs.
- *Exit without Saving* closes the Component Status Display Tool and its dialogs without saving the preferences or settings to a file.
- *Cancel Exit* aborts the exit.

See the figure “Exit CSD dialog window” (page 415) for an overview of the Exit dialog.

**Figure 45**  
**Exit CSD dialog window**



## Warning and error dialogs

The Components Status Display provides a number of warning and error dialogs. If a warning or an error dialog opens, take the action indicated.

### Save Settings Error Dialog

The *Save Settings Error Dialog* indicates that the preference or component filter settings (or both) could not be saved to their use-specific files (CSDPrefs.cfg and CSDCompFilt.cfg respectively in the user's home account under the directory *MagellanNMS*). Possible reasons for this failure are

- the home directory or the configuration files are protected (no write permission)
- there is insufficient disk space in the home directory

Ensure that the files and home directory have write permission and that enough disk space is left; then retry the operation.

### Restore Settings Error Dialog

The *Restore Settings Error Dialog* indicates that the preference or Component Filter Settings (or both) could not be restored from their user-specific files (CSDPrefs.cfg and CSDCompFilt.cfg respectively in the user's home account under the directory *MagellanNMS*). Possible reasons for this failure are

- the home directory or the configuration files are protected (no read permission)
- the files do not exist

- the files exist but their contents are not recognized

If files exist in the home directory and in *MagellanNMS* directory ensure that they have read permission. If the files do not exist, or if they exist but their contents are not recognized, recreate the appropriate settings using the Component Filter and Preference Settings dialogs; then save them again.

### **Maximum Components Warning Dialog**

This *Maximum Components Warning Dialog* warns you that the Component Status Display may take a few minutes to display the list of components that you requested.

### **No Network Model Coordinator Error Dialog**

The *Network Model Coordinator Error Dialog* indicates that the Component Status Display cannot establish a connection to the Network Model Coordinator. After the Component Status Display closes, verify whether or not the Network Model Coordinator is running. If it is not running, start with the Server Manager Administration Tool (if you have access to it), or contact your system administrator for assistance.

### **Network Model Access Error Dialog**

The *Network Model Access Error Dialog* indicates that the Component Status Display cannot access the network model. Most likely, the Network Model Coordinator is running, but a network model is not loaded in shared memory. Verify whether or not a network model is loaded. If it is not loaded, load one, or contact your system administrator for assistance.

### **Service Selection Warning Dialog**

The *Service Selection Warning Dialog* indicates that your workstation has been rehomed to a new network model host. This affects only tools such as the CIV that use the Network Model Server to access the LAN-selected host. However, the Component Status Display is unaffected since it uses only the local network model that runs on your workstation.

### **No Model Error Dialog**

The *No Model Error Dialog* indicates that the network model is either empty or corrupted. Verify that a network model is loaded in shared memory. If it is not loaded, load one. However, if a network model is already loaded, reload the model, or contact your system administrator for assistance.

**Lost Connection Error Dialog**

The *Lost Connection Error Dialog* indicates that the Component Status Display has lost its connection to the Network Model Coordinator. The most likely cause is that the Network Model Coordinator has terminated. Verify whether or not the Network Model Coordinator is running. Either restart or contact your system administrator for assistance.

**Model Locked Error Dialog**

The *Model Locked Error Dialog* indicates that the Component Status Display is attempting to access the network model while it is locked by another network model application. The network model is probably being updated; therefore, retry the command that you were attempting. If this dialog appears after successive attempts, you may want to contact your system administrator for assistance.

**Organization Not Found Error Dialog**

The *Organization Not Found Error Dialog* indicates that the Component Status Display cannot locate the selected organization in the network model that is currently loaded in shared memory. The organization may have been deleted by another network model application while you were running the Component Status Display. Choose *Select Organization* from the *View* menu to get an updated list of the available organizations in the network model. Select and open one of the organizations on the list.

## Component Status Display procedures

You can perform the following tasks with the Component Status Display:

- “Starting the Component Status Display” (page 418)
- “Refreshing the Components Panel” (page 418)
- “Choosing a new organization” (page 419)
- “Putting a component into Acknowledged state” (page 420)
- “Putting a component into Maintenance state” (page 420)
- “Changing the Component Filter Settings” (page 421)
- “Exiting the Component Status Display” (page 422)

## Starting the Component Status Display

Your system administrator may have the Component Status Display configured to open automatically. If not, you can open the Component Status Display tool from the fault management toolset.

**Note:** The Component Status Display does not use the network model server referred to by the current service selection. The Component Status Display needs to run on the same workstation as the network model shared memory.

### Starting the Component Status Display tool

- 1 In the Preside MDM Toolsets window, select Fault -> Component Status Display

The Component Status Display window opens. Any preferences that were saved to a file during a previous session are automatically used.

## Refreshing the Components Panel

You can refresh the Components Panel

- manually by using the *Refresh Display* button in the Main Window at any time
- automatically by using the Auto-Refresh feature. Auto-Refresh updates the contents of the Components Panel based on the interval that you set in the *Preferences Settings Dialog*. After you set the interval, you can activate it from the *Preference Settings Dialog* or from the main window.

When the network model changes, the Network Model Coordinator notifies the Component Status Display of the change. The Component Status Display then automatically refreshes the Components Panel.

**Note:** You cannot apply the Auto-Refresh feature to the Components Panel while organization components are displayed.

### Activating and deactivating Auto-Refresh from the Main Window

Use this procedure to activate or deactivate *Auto-Refresh* from the Component Status Display window. For instructions to set the Auto-Refresh interval and activate it from the *Preferences Setting Dialog*, see “Setting the Auto-Refresh interval” (page 424).

- 1 Select *On* from the *Auto-Refresh* option button to turn the function on, or select *Off* to turn the function off.

*On* appears next to the button to indicate that the function is activated or *Off* to indicate that the function is deactivated.

## Choosing a new organization

The network model can contain one or more organizations. Depending on the number of organizations present, the following actions can occur:

- **One organization** The Component Status Display automatically opens the organization and displays all regions within the organization.
- **Two organizations** If the first organization is *DEFAULT ALL*, the Component Status Display automatically opens the other organization; otherwise, it opens *DEFAULT ALL*.
- **More than two organizations** Component Status Display displays a list of all available organizations found in the network model and then prompts you to select and open one. Select the desired organization and choose *Open Organization* from the Components Panel pop-up menu. All the regions within the selected organization are displayed. If more than one organization is displayed, you can switch to a different organization by following the procedure “Choosing and opening a new organization” (page 419).

**Note:** You can also specify an organization value as a parameter in the startup command for the tool, by using the *-O* option. For example, the command `/opt/MagellanNMS/bin/csd -O "DPN R3_ORG"` & starts the Component Status Display and tells it to open the organization *DPN R3\_ORG*. The region records for this organization are automatically shown when the Component Status Display starts.

## Choosing and opening a new organization

- 1 From the *View* menu select *Select Organization*

The organizations appear in the Components Panel.

- 2 From the pop-up menu in the Component Panel, select *Open Organization*.

The organizations are automatically replaced by the region records for the selected organization.

## Putting a component into Acknowledged state

The Acknowledged state temporarily hides the current troubled state of a component (as indicated by the network). When a component is acknowledged, it acts as though it is in an In-Service state. If no other related components are troubled, the acknowledged component displays a state of ACKED instead of In-Service. When the component changes state, the acknowledgment is automatically removed and the real state of the component is shown. Only troubled modules and subcomponents (from the network) can be put into the Acknowledged state. For more information on the Acknowledged state, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

**Note:** You can put a component into the Acknowledged state by acknowledging all active alarms against the component.

### Putting a component into and taking it out of the Acknowledged state

- 1 In the Components Panel, click on the component you want to put into the Acknowledged state.

The component is highlighted.

- 2 From the pop-up menu in the Components Panel, select *Set Acknowledged State On*.

The next time the menu appears, the command changes to *Set Acknowledged State Off*.

**Note:** You can also put a component into the Acknowledged state by acknowledging all active alarms against the component using the *Start Tool* menu.

- 3 From the pop-up menu, select *Set Acknowledged State Off* to remove the component from the Acknowledged state.

## Putting a component into Maintenance state

Maintenance state permanently hides the current troubled state of a component. When a module or component is put into maintenance, its state is propagated downwards. For more information on the Maintenance state, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

### Putting a component into Maintenance state

- 1 In the Components Panel, click on the component you want to put into the Maintenance state.

The component is highlighted.

- 2 From the Components Panel pop-up menu, select *Set Maintenance State On*.

**Note:** The next time the menu is displayed, the command changes to *Set Maintenance State Off*. Select this new command to remove the components from the Maintenance state.

## Changing the Component Filter Settings

You can modify the Component Status Display to reduce the amount of information displayed in the Components Panel using the *Component Filter Settings Dialog*. For information about the items in this dialog, see “Component Filter Settings Dialog” (page 410).

You can use the component filter settings in these ways:

- You can set the components filter parameters and use them immediately. or, you can also save the settings to a file for reuse.
- You can retrieve previously stored filter settings from a file and use them.

### Setting component filtering from the Component Filter Settings Dialog

Use this procedure to set the component filter parameters from the Component Filter Settings Dialog and to save the settings to the *CSDCompFilt.cfg* file in your *\$HOME/MagellanNMS* directory.

- 1 Ensure that *Filtering* is turned to *On* in the Component Status Display main window.
- 2 From the *Options* menu, select *Change Component Filter Settings*  
The Component Filter Settings Dialog opens.
- 3 Click on *Troubled Network State* or *Propagated State/Criticality*.
- 4 If you click *Propagated State/Criticality*, select one or more *States* and one or more *Criticality* values.

**Note:** The criticality values, which range from 1 (lowest) to 5 (highest), are used only for the In-Service Troubled and Out of Service states.

- 5 Select one or more components that you want to filter from the component types list. All component types are automatically selected by default.

To add a component to your existing selection, press Control and click on the component you wish to add.

To add a contiguous group of components, click on one component, then drag the mouse to select the other components. Alternatively, click on the first component and on the last component; all components between them are selected automatically.

- 6 Select *Save to File* to permanently save the filter settings to the *CSDCompFilt.cfg* file in your *\$HOME/MagellanNMS* directory.
- 7 Select *Use Filters* to apply the new filter settings.

If filtering is turned to *On* in the Component Status Display main window, the newly filtered components are displayed in the Components List.

**Note:** Any changes made to the filter settings are lost if you do not apply them before closing. The last set of applied filters are displayed the next time the dialog is opened.

- 8 Click *Cancel* to close the dialog.

### Using previously saved filter settings

Use this procedure to retrieve and apply previously stored filter settings. The settings are restored from the *CSDCompFilt.cfg* file in your *\$HOME/MagellanNMS* directory.

- 1 From the *Options* menu, select *Change Component Filter Settings...*

The Component Filter Settings Dialog window opens.

- 2 Click *Restore from File*.

The restored settings are displayed in the dialog.

- 3 Click *Use Filters* to apply the filter settings to the Component Status Display main window.

The restored settings are applied to the Component Status Display main window.

## Exiting the Component Status Display

To close the Component Status Display and all its dialogs, select *Exit* from the *File* menu.

If you have made modifications in the Component Filter Settings Dialog or the Preferences Setting Dialog but did not save them, the Exit CSD dialog opens. For details about this dialog and the choices it provides, see “Exit CSD Dialog” (page 414).

## Setting Component Status Display preferences

The *Preference Setting Dialog*, described in “Preference Settings Dialog” (page 411), lets you tailor the Component Status Display main window and perform the following functions:

- set the Sort key
- turn Auto-Refresh on or off
- set the Auto-Refresh interval
- save the preferences to a file or restore them from a file
- apply the settings to the main window

### Setting the sort key for the components list

Use this procedure to set up the sort key to sort components according to Troubled Network state, Propagated State/Criticality, the component name, and the time that the component is last modified.

- 1 From the *Options* menu, select *Change Preference Settings*

The Preference Settings Dialog opens.

- 2 From *Sort-By*, select one of the sort keys.

**Note:** When you sort by *Propagated State/Criticality*, you cannot rearrange the order of states. Also, *out-of-service* (OOS) and *in-service troubled* (ISTB) states are sorted in descending order from most critical (5) to least critical (1).

- 3 Click *Use Preferences* to apply the sort key to the Components Panel in the Component Status Display main window.

The Components Panel refreshes to show the components according to the specified sort order.

- 4 Select *Cancel* to close the dialog.

The Preference Settings Dialog closes.

### Setting the Auto-Refresh interval

Use this procedure to set the interval at which information in the Main Window is refreshed.

You can set the interval to a value from 30 to 600 seconds. To set the value, click to the left or right of the slider to decrease or increase the setting by five-second increments; or, drag the slider to the left or right to decrease or increase the setting by one-second increments.

- 1 From the *Options* menu, select *Change Preference Settings*  
The Preference Settings Dialog opens.
- 2 Select *On* from the *Auto Refresh* option button.
- 3 Set the *Refresh Interval* to the desired number of seconds.
- 4 Select *Save to File* if you want to save the settings to the *CSDPrefs.cfg* file in your *\$HOME/MagellanNMS* directory.

The settings made in the dialog and preference settings that are exclusive to the Component Status Display main window, such as Filtering, are saved. The changes are not applied and the dialog remains open.

- 5 Click *Use Preferences* to apply these settings to the Component Status Display main window.
- 6 Click *Cancel* to close the dialog.  
The Preference Settings Dialog closes.

**Note:** This preference setting is dependant on the *Auto-Refresh* preference being enabled. If *Auto-Refresh* is deactivated, the *Refresh Interval* is disabled.

### Using previously saved preference settings

Use this procedure to retrieve and apply previously stored preference settings. The settings are restored from the *CSDPrefs.cfg* file in your *\$HOME/MagellanNMS* directory.

- 1 From the *Options* menu, select *Change Preference Settings*  
The Preference Settings Dialog opens.
- 2 Click *Restore from File*.  
The restored settings are displayed in the dialog.

- 3 Click *Use Preferences* to apply these settings to the Component Status Display Main Window.

The restored settings are applied to the Component Status Display main window.

## Customizing the Component Status Display

The Component Status Display lets you customize the following items:

- the Component List Start Tool menu
- other resources including
  - colors associated with propagated states and problem states
  - whether or not the problem states are shown in the Components Panel
  - whether or not a bell rings upon error

### Customizing the Components List Start Tool menu

For procedures on customizing the Start Tool menu for the Components Panel List, see the section on customizing the toolsets and Start Tools menus in 241-6001-301 *Preside MDM Customization Administrator Guide*.

To customize the Components Panel List Start Tool menu, copy the file `/opt/MagellanNMS/lib/tsets/$LANG/tools/surv/` and save it in either `$HOME/MagellanNMS/tools/` for a single user customization or `/opt/MagellanNMS/cfg/tsets/$LANG/tools/` for all users of a workstation

When you modify the file, use one of the following substitution variables in the command line:

- `$COMP`: the internal component name of the target
- `$DCOMP`: the display component name of the target

### Customizing other resources

The table “Resources for color control of propagated states by Component Status Display” (page 426) lists the resources you use to control the colors associated with propagated states displayed by Component Status Display.

**Table 63**  
**Resources for color control of propagated states by Component Status Display**

Resource	Description	Legal values
*stateOOS_1 *stateOOS_2 *stateOOS_3 *stateOOS_4 *stateOOS_5 *stateISTB_1 *stateISTB_2 *stateISTB_3 *stateISTB_4 *stateISTB_5 *stateACKED *stateMTCE *stateHIER_MTCE *stateINVS *stateUNKNOWN *stateINVALID moduleStateUNKNOWN	Specifies the state-to-color mapping used to indicate the current state of the components in the Components Panel (These are the same resources used for the NV.)	Any legal X windows color or specification. See 241-6001-301 <i>Preside MDM Customization Administrator Guide</i> .

**Table 64**  
**Resources for customizing the Acknowledgement/unacknowledgement Alarms Dialog**

Resource	Description	Legal values
*AckAlarmDlog*userIdFieldField.editable	If True, the <i>User</i> field in the dialog used for acknowledging or unacknowledging alarms, can be modified. The default is False.	True or False
*AckAlarmDlog*commentData.maxLength	The maximum length of <i>Reason</i> text that can be specified when acknowledging or unacknowledging alarms. The default length is 256.	Any legal <i>Motif</i> value associated with the <i>MaxLength</i> resource.
CIV*differentModuleUnknownColor	If <i>differentModuleUnknownColor</i> is true, then the unknown color for the node at the module level is different from the default unknown.	True or False

The table “Resources for color control of problem states by Component Status Display” (page 428) lists the resources you use to control the colors associated with the problem states displayed by Component Status Display components.

**Table 65**  
**Resources for color control of problem states by Component Status Display**

Resource	Description	Legal value
*stateNameOOS_1 *stateNameOOS_2 *stateNameOOS_3 *stateNameOOS_4 *stateNameOOS_5 *stateNameISTB_1 *stateNameISTB_2 *stateNameISTB_3 *stateNameISTB_4 *stateNameISTB_5 *stateNameACKED *stateNameMTCE *stateNameHIER_MTCE *stateNameINVS *stateNameUNKNOWN *stateNameINVALID	Specifies the state-to-name mappings used to indicate the current state of the components in the Components Panel. (These are the same resources used for the NV.)	Any legal character string. Caution must be exercised when modifying state names to ensure that the new name correctly and clearly identifies the state; otherwise, problem states could be shown for components which are in service and conversely.

---

## Chapter 12

# IP Discovery

---

This section describes how to use the Internet Protocol (IP) Discovery application to discover Simple Management Network Protocol (SNMP) devices.

*Note:* This document does not include software rollback procedures. See *Preside MDM Release Supplement*.

This section contains the following procedures:

- “Starting IP Discovery” (page 431)
- “Setting a password for IP Discovery” (page 432)
- “Starting IP Discovery with password protection” (page 433)
- “Changing a password for IP Discovery” (page 434)
- “Disabling password protection for IP Discovery” (page 435)
- “Discovering devices using direct discovery” (page 436)
- “Discovering devices using route-based discovery” (page 437)
- “Deleting devices” (page 438)
- “Updating devices” (page 440)
- “Finding devices” (page 441)
- “Adding an address” (page 442)
- “Creating a network setting” (page 443)
- “Changing network settings” (page 444)

- “Deleting network settings” (page 445)
- “Moving rows in network settings” (page 446)

For information on IP Discovery windows and log and errors messages, see the following:

- “IP Device Discovery window” (page 447)
- “Discovery window” (page 456)
- “Logging” (page 461)
- “Error messages” (page 462)
- “Warning messages” (page 465)

## Starting IP Discovery

Use this procedure to start IP Discovery without password protection.

To set a password, see “Setting a password for IP Discovery” (page 432).

### Prerequisites

- To use IP Discovery, you must install the Magellan Contrib (MagTcl), and Java Runtime Environment for Solaris (MagJ<release>) software packages. For more information, see the procedures for loading Preside MDM in 241-6001-100 *Preside MDM Installer Guide*.
- The IP Discovery server must be running.

### Procedure

- 1 From the **Preside MDM** window, select **Fault -> IP Discovery**.

A warning dialog box opens informing the user that IP Discovery is in non-secure mode.

- 2 Click **OK**.

The **IP Device Discovery** window is displayed.

## Setting a password for IP Discovery

Setting a password for the IP Discovery tool increases the security of your network by adding a layer of protection to your network settings. The network settings control access to the devices. Accessing or changing network settings can disrupt network surveillance of these devices and cause potential security problems. By adding a password to IP Discovery, you are decreasing the chances that an unauthorized user could get access to your network settings.

### Prerequisites

- You must be logged in as root to set the password for IP Discovery.

### Procedure steps

- 1 From the **Fault** menu, click **IP Discovery**.  
The **IP Device Discovery** window opens.
- 2 From the **Security** menu, click **Set/Change Password**.  
The **Set Password** dialog box opens.
- 3 Type a new password in the **New Password** field.
- 4 Type the same password again in the **Confirm Password** text field.
- 5 Click **OK**.

## Starting IP Discovery with password protection

When you start IP Discovery any time after you have set a password, you will be starting with password protection.

To find out how to set a password, see “Setting a password for IP Discovery” (page 432).

### Prerequisites

- To use IP Discovery, you must install the Magellan Contrib (MagTcl), and Java Runtime Environment for Solaris (MagJ<release>) software packages. For more information, see the procedures for loading Preside MDM in 241-6001-100 *Preside MDM Installer Guide*.

### Procedure steps

- 1 From the **Preside MDM** window, select **Fault -> IP Discovery**.

The **User Logon** dialog box opens.

- 2 Enter the password and click **OK**

If you do not enter the correct password after three attempts, the IP Discovery GUI shuts down.

## Changing a password for IP Discovery

Changing passwords on a regular basis ensures that your network settings remain secure from unauthorized users. You should also change your passwords when you feel that your network security might be compromised by events such as changes in your network or organization.

### Attention!

If another user is running an IP Discovery session when you change the password, that user will be prompted to relogin and enter the new password.

### Prerequisites

- You must be logged in as root to reset the password for IP Discovery.

### Procedure steps

- 1 From the **Preside MDM** window, select **Fault -> IP Discovery**.  
The **IP Device Discovery** window opens.
- 2 From the **Security** menu, click **Set/Change Password**.  
The **Change Password** dialog box opens.
- 3 Type the current password in the **Old Password** field.
- 4 Type a new password in the **New Password** field.
- 5 Type the new password again in the **Confirm Password** field.
- 6 Click **OK**.

## Disabling password protection for IP Discovery

Disabling password protection for IP Discovery may be necessary in situations where customers require non-secure access. This procedure removes the password protection file.

### Prerequisites

- You must be logged in as root to reset the password for IP Discovery.

### Procedure steps

- 1 From the command console, type the following command

```
rm /opt/MagellanNMS/cfg/private/IPM.passwd
```

Once this file is removed, the password for IP Discovery is disabled and it can be accessed in non-secure mode.

## Discovering devices using direct discovery

Use direct discovery to discover a device by its hostname or by its IP address. You can use both hostnames and IP addresses in one discovery session. See “Discovery window” (page 456) for more information.

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Device -> Discover**.  
The **Discovery** window opens.
- 2 In the **Method** field, select **Direct**
- 3 Enter the device you wish to discover by one of the following methods:
  - a. Type the IP address or hostname in the **IP Address** field. If you are discovering more than one device, separate the IP addresses and hostnames with a comma.
  - b. Click **Load from** to open a seed file which contains IP addresses and hostnames of devices to be discovered.
- 4 When you have finished choosing the parameters, click **Start** to begin discovery.

During the discovery process, the **Status** area shows the progress of the discovery as well as any errors.

**Note:** Several options are available during direct discovery. You can specify the device type with which you want the device discovered by using the **Discover As** option. You can also specify the option to **Register to Receive Traps**. For more information on these options, see “Discovery window” (page 456).

## Discovering devices using route-based discovery

Discover devices using route-based discovery in order to discover a network or part of it using an initial address or set of addresses as a starting point. See “Discovery window” (page 456) for more information.

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Device -> Discover**.  
The **Discovery** window opens.
- 2 In the **Method** field, select **Route based**.
- 3 Enter the device you wish to be used as a starting point for route-based discovery by one of the following methods:
  - a. Type the IP address or hostname in the **IP Address** field. If you are using more than one starting point, separate the IP addresses and hostnames with a comma.
  - b. Click **Load from** to open a seed file which contains IP addresses and hostnames of devices to be used as starting points.
- 4 When you have finished choosing the parameters, click **Start** to begin discovery.

During the discovery process, the status area shows the progress of the discovery.

**Note:** Several options are available during route-based discovery. In the **Exclude** field in the **Options** area, select the device types that you wish to exclude from the discovery. In the **IP Address Range** field in the **Options** area, enter the range of IP addresses to be discovered. Addresses outside of this range are ignored. For more information on these options, see “Discovery window” (page 456).

## Deleting devices

The delete command deletes selected devices in the **Devices** tab. The delete command is only available when you select the **Devices** tab and there is at least one selected entry in the table.

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Devices** tab.
- 2 Highlight one or more devices in the table. To select more than one device, do one of the following:
  - Press the **Shift** key and the left mouse.
  - Press the **Ctrl** key and the left mouse.
- 3 Right click on the item.
- 4 From the pop-up menu, select **Delete**.

A dialog opens to confirm the delete request with the following options:

- **Attempt device deletion from Network Model**
- **Attempt trap deregistration with device**

**Note 1:** The option **Attempt device deletion from Network Model** will delete a device from the Network Model, if possible, even if the option for automatic deletion of obsolete components in the surveillance update server SURNUP is disabled. This option may fail if the network model is not available for an update. This may occur if another user is in Edit mode in the Network Viewer when you attempt to delete the device. For more information, see the Surveillance Network Model Updater (SURNUP) section in the 241-6001-310 *Preside MDM Server Reference Guide*.

**Note 2:** The option **Attempt trap deregistration with device** may significantly slow down the deletion process.

- 5 Click **OK** to delete the device.

The selected device disappears from the table. If the deletion is unsuccessful, an error message is displayed.

A log containing the result of the delete operation is created by default in `/opt/MagellanNMS/data/log/ipm/ipDiscovery.out`. For more information, see "Logging" (page 461).

**Note 1:** The device may be deleted from the Network Model automatically if the fault servers support automatic deletion of obsolete components and the option for automatic deletion of obsolete

components is enabled in the surveillance updater server SURNUP. This is true even if **Attempt device deletion from Network Model** is not selected.

**Note 2:** A delete command may fail if the device cannot be found in the General Management Data Router (GMDR).

## Updating devices

You can update a device when it changes its configuration and/or MIB information.

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Devices** tab.  
The currently managed devices list is displayed in the table.
- 2 Highlight one or more devices in the table. To select more than one device, press the **Shift** key.
- 3 Right click on the item.
- 4 From the pop-up menu, select **Update**.

The updated devices are refreshed from the table. If the update is unsuccessful, an error message is displayed.

**Note:** An update command may fail if the device cannot be found in the General Management Data Router (GMDR).

## Finding devices

You can locate a device in the device table using a device name or IP address.

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Devices** tab.  
The currently managed devices list is displayed in the table.
- 2 Select the **Device -> Find Device**.
- 3 Input a device name or IP Address in the name field of the **Find Device** dialog.
- 4 Press the **Find** button or press Enter to locate the row with the matching device.
- 5 To continue searching for another match in the table, press **Find** again.
- 6 Press **Close** to close the **Find Device** dialog.

**Note:** The Find functionality searches the table from the first row to the very end of the table; however, if a row is selected before **Find** is used, the searching begins from the selected row to the end of the table and wraps around.

## Adding an address

You can add a polling or trap address (depending on the device cartridge's capabilities) to the address list for a specified device.

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Devices** tab.  
The currently managed devices list is displayed in the table.
- 2 Highlight one device from the table.
- 3 From the **Device** menu, select **AddAddress**. You can also right-click the device and select **AddAddress** from the pop-up menu.

The **AddAddress** dialog opens.

**Note:** If multiple address capability is not supported, a dialog opens indicating that multiple addressing is not supported by the device cartridge. In this case, you will not see the **AddAddress** dialog.

- 4 In the **IP Address** field, type in the IP Address of the device you wish to add.
- 5 In the **Community** field, type in the Read community string of the device you wish to add (for example, public).
- 6 In the **Type** field, select **Trap** or **Poll**.

**Note:** The options in the **Type** field depend on the device cartridge's capability. You may see Trap or Poll, or both Trap and Poll.

- 7 Click **Add**.

A message at the bottom of the **IP Device Discovery** window informs you when the address is added.

## Creating a network setting

Create network settings to add a new network device and its attributes.

### Prerequisites

- To perform network settings procedures, you must be in edit mode. Only one person at a time can perform these procedures. For more information, see “Network Settings” (page 452)

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Network Settings**.  
The current network settings list is displayed.
- 2 From the **Edit** menu, select **Add Row**.  
A new row is added into the table.
- 3 Enter the network setting attributes:
  - **IP Address** or address range
  - **Read Community String**
  - **Read Write Community String** (optional)
  - **Port**
  - **Device Type** (optional)
  - **SNMP Version** (optional)
- 4 Select **File -> Save** to save the new settings into the network settings configuration file.

## Changing network settings

Change network settings to restore communication with devices that are unreachable and are in an “unknown” state in MDM.

### Prerequisites

- To perform network settings procedures, you must be in edit mode. Only one person at a time can perform these procedures. For more information, see “Network Settings” (page 452)

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Network Settings**.  
The current network settings list is displayed.
- 2 Select and highlight the row you want to modify.
- 3 Enter the network setting attributes:
  - **IP Address** or address range
  - **Read Community String**
  - **Read Write Community String** (optional)
  - **Port**
  - **Device type** (optional)
  - **SNMP Version** (optional)
- 4 Select **File -> Save** to save the new settings into the network settings configuration file and apply them.

## Deleting network settings

Deleting network settings removes an entry from the list of network settings.

### Prerequisites

- To perform network settings procedures, you must be in edit mode. Only one person at a time can perform these procedures. For more information, see “Network Settings” (page 452)

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Network Settings**.

The current network settings list is displayed.

- 2 Highlight the entry or row you want to delete.

- 3 Select **Edit -> Delete Row(s)**.

**Note:** You can also right-click the item, and select **Delete Row(s)** from the pop-up menu.

- 4 Select **File -> Save** to save the new settings into the network settings configuration file.

## Moving rows in network settings

You may need to change the order of network settings because the ordering is important in IP Discovery. See “Network settings during discovery” (page 454) for more information.

### Prerequisites

- To perform network settings procedures, you must be in edit mode. Only one person at a time can perform these procedures. For more information, see “Network Settings” (page 452)

### Procedure steps

- 1 From the **IP Device Discovery** window, select **Network Settings**.  
The current network settings list is displayed.
- 2 Highlight the row you wish to move.
- 3 Perform one of the following:
  - a. To move a row up, select **Edit -> Move Row Up**.
  - b. To move a row down, select **Edit -> Move Row Down**.
- 4 The highlighted row has moved up or down in the table.
- 5 Save the settings by selecting **File -> Save**.

## IP Device Discovery window

The **IP Device Discovery** window contains the following areas:

- “Menu bar” (page 447)
- “Devices” (page 450)
- “Network Settings” (page 452)

### Menu bar

The **IP Device Discovery** menu bar consists of the following menus:

- “File” (page 447)
- “Edit” (page 447)
- “Device” (page 448)
- “Security” (page 449)
- “Help” (page 449)

### File

The **File** menu contains the following commands:

- **Save** saves the current network settings. The **Save** option is greyed out when the **Devices** tab is selected.
- **Save As** displays a file browser to let you specify where to save the IP addresses from the device list. The **Save As** command is greyed out when the **Network Settings** tab is selected.
- **Exit** closes the IP Discovery application. If there are unsaved changes, you are prompted to save the changes before exiting the application.

### Edit

The **Edit** menu contains the following commands:

- **Add Row** either adds a new row to the top of the list of settings profiles if no row has been selected, or adds a new row below an already selected row. The new entry does not have an IP address, but consists of default values for the other parameters. The **Add Row** command is only available when.
  - the network settings tab is selected

- you are in edit mode
- **Move Row Up** moves the selected row up one entry in the table. The **Move Row Up** command is only available when
  - the network settings tab is selected
  - you are in edit mode
  - there is an entry in the table
- **Move Row Down** moves the selected rows down one entry in the table. The **Move Row Down** command is only available when
  - the network settings tab is selected
  - you are in edit mode
  - there is an entry in the table
- **Delete Row(s)** deletes selected row(s). The **Delete Row(s)** command is only available when
  - the network settings tab is selected
  - you are in edit mode
  - there is an entry in the table
- **Select All** selects all devices or settings profiles, depending on which tab is visible.
- **Deselect All** deselects all devices or settings profiles, depending on which tab is visible.

### Device

The **Device** menu contains the following commands:

- **Discover** opens the Discovery window. You can discover devices using direct discovery or route-based discovery. For more information, see “Discovery window” (page 456).
- **Refresh List** rereads the list of SNMP-managed devices. The **Refresh List** command is only available when you select the Devices tab.
- **Update** rediscovers the selected devices. The **Update** command is only available when you select the **Devices** tab, and there is a selected entry in the table.

- **Delete** deletes any selected devices in the **Devices** tab.
- **Add Address** adds a polling or trap address to the address list for a specified device. The **Add Address** command is only available when you select the **Devices** tab, and there is a selected entry in the table. The **Add Address** may fail if one of the following occurs:
  - the device profile does not allow this action (not supported in the device cartridge)
  - the address has been assigned to another device, and this device is currently using the address for polling.

The following attributes must be specified in the request:

- IP address
  - community string
  - address type (poll or trap)
- **Find Device** locates a device in the device table using the device name or IP address. When Find Device is selected, a dialog box is displayed. You can enter a device name or IP address to search the Devices table. When the device is located, the row associated with the device is highlighted.

### Security

The **Security** menu contains the **Set/Change Password** command. This command is only available when you are logged in as root. The **Set/Change Password** command functions as follows:

- **Set/Change Password** displays the **Set Password** dialog box if you have never set a password for IP Discovery. If you have previously set a password for IP Discovery, this command displays the **Change Password** dialog box.

### Help

Invoking a help command launches online documentation. The **Help** menu contains the following commands:

- **Discovery Help** displays information on how to discover devices. This command is also available by clicking **Help** on the **Discovery** window.

- **Network Settings Help** displays information on how to use network settings.
- **Devices Help** displays information on how to use Device menu options. You must have installed the MDMHelp packages for these commands to work.

## Devices

The **Devices** tab is displayed by default when you launch the IP Discovery application. This window tab lists discovered devices that have an IP address and name. The fields are as follows:

- **Name** contains the Preside Multiservice Data Manager (MDM) assigned component ID for the device.
- **IP Address** contains the management address used by Preside MDM to communicate with the device.
- **Read Community String** contains the community string used to query and poll the device.
- **SNMP Version** contains the Simple Network Management Network Protocol (SNMP) version number that is used to query and communicate with the device. The SNMP version number is specified as SNMPv1 or SNMPv2c.

*Note:* The listing described is the default format by which the device information is displayed. You can display the information in any order by holding down the left mouse button on the heading, and moving it to the left or the right.

You can right click on a device to display a pop-up menu. From the pop-up menu, you can open the **Discovery** window, refresh the device list, update the device list or delete devices.

*Note:* The pop-up menu does not display if you do not select an entry.

*Note:* Updates to the device properties may take a few minutes to propagate to the IP Discovery device list. Give the changes time to propagate, and then refresh the list to see these updates.

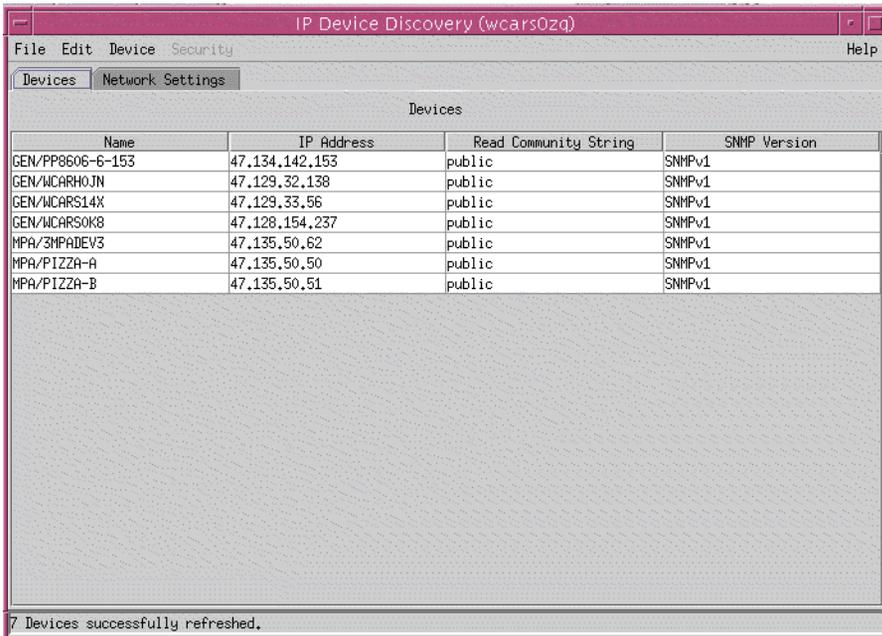
## Sorting devices

You can sort the listed devices by clicking one of the following headings:

- **Name** sorts the devices alphabetically from top to bottom.
- **IP Address** sorts the devices by IP address, with the smallest numerical IP address at the top.
- **Community string**  
Click on the **Read Community String** heading to sort the devices alphabetically from top to bottom.
- **SNMP Version** sorts the devices by Simple Network Management Protocol (SNMP) version.

The figure “Devices tab” (page 451) shows the device fields

**Figure 46**  
**Devices tab**



The screenshot shows a window titled "IP Device Discovery (wcars0zq)" with a menu bar (File, Edit, Device, Security, Help) and two tabs: "Devices" (selected) and "Network Settings". The main area displays a table of discovered devices with the following columns: Name, IP Address, Read Community String, and SNMP Version. The table contains seven rows of data. A status bar at the bottom indicates "7 Devices successfully refreshed."

Name	IP Address	Read Community String	SNMP Version
GEN/PP8606-6-153	47.134.142.153	public	SNMPv1
GEN/WCARHOJN	47.129.32.138	public	SNMPv1
GEN/WCARS14X	47.129.33.56	public	SNMPv1
GEN/WCARS0K8	47.128.154.237	public	SNMPv1
MPA/3MPADEV3	47.135.50.62	public	SNMPv1
MPA/PIZZA-A	47.135.50.50	public	SNMPv1
MPA/PIZZA-B	47.135.50.51	public	SNMPv1

## Network Settings

Network settings lets you add, delete, modify and rearrange SNMP read and read/write community strings and other attributes that control access to network devices.

Network settings can be edited by one user at a time. When the network settings tab is selected, you are put in edit mode, or in read-only mode if you are not the only person accessing this tab. One of the following messages is displayed in the status bar to indicate which mode you are in:

- **Viewing as read-only. Network settings currently locked by either another editing session or a discovery process.** This message indicates that another user is in edit mode, and that you can only view the network settings. You cannot modify the network settings in this mode.
- **Edit Network Settings.** This message indicates that you are in edit mode, and can modify the network settings.

When you exit the edit mode after making changes, a dialog prompts you to save the changes. If there is an error in an IP address field, a message is displayed, and you cannot proceed.

The network settings fields are as follows:

- **IP Address** (includes wildcards) contains an IP address range specification used to match management addresses of devices as they are discovered, in order to determine its network settings. Examples of the valid pattern specifications are as follows:
  - 134.177.125.31: matches the specified IP address
  - 134.177.125.1-31: matches all addresses in the range 134.177.125.1 to 134.177.125.31
  - 134.177.125.\*: matches all addresses in the range 134.177.125.1 to 134.177.125.255
  - 134.177.125-128.\*: matches all addresses in the range 134.177.125.\* to 134.177.128.\*
  - \*.\*.\*.\*: matches all addresses.
- **Read Community String** contains the read community string used to query and poll the device.

- **Read Write Community String** contains the write community string used to perform SNMP writes to the device. You can write to a device when the Register to Receive Traps option is enabled during the discovery of a device that supports the SNMP Target MIB, and the SNMP view based ACM MIB.
- **Port** contains the port number to be used by SNMP for device discovery.
- **Device Type** contains the type of devices supported by IP Discovery. If the device type is blank, this field matches against any device type.
- **SNMP Version** contains the Simple Network Management Protocol (SNMP) version number. This number is a configurable option in the network settings. When you configure the SNMP version number, the default number is overridden with the new version. The SNMP version is specified as SNMPv1, SNMPv2c, or a blank entry (“ ”):
  - **SNMPv1** indicates that SNMP1 will be used to discover and manage the device.
  - **SNMPv2c** indicates that SNMP2c will be used to discover and manage the device.
  - a blank entry (“ ”) indicates that the SNMP version in the DCD will be used to manage the device.

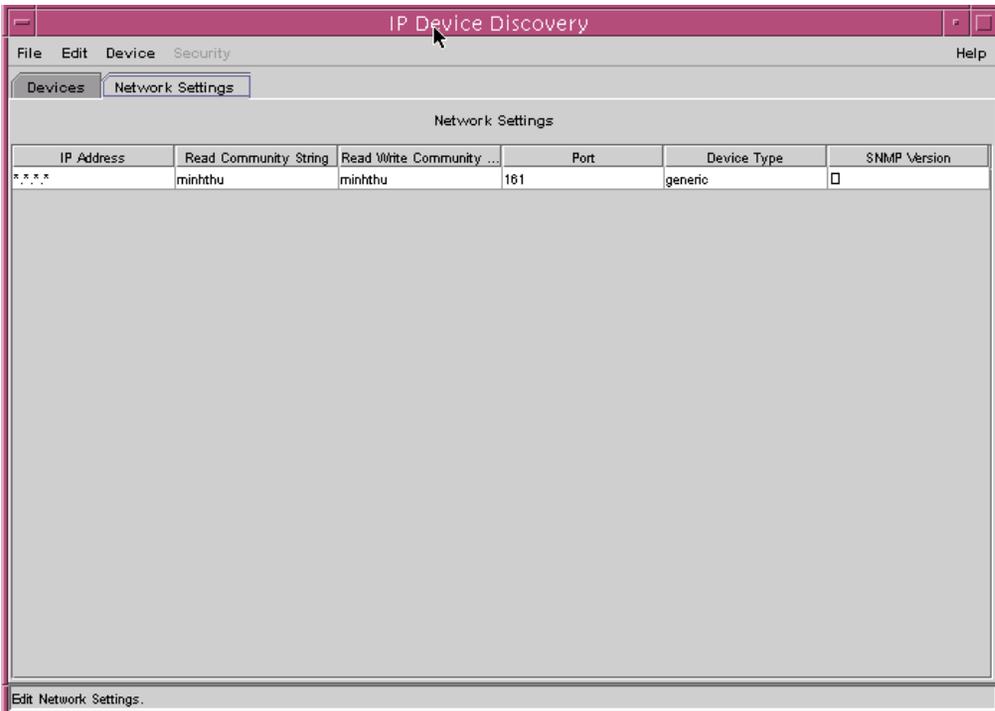
In edit mode, you can right click on a network setting to display a pop-up menu that displays the following:

- **Add Row**
- **Move Row Up**
- **Move Row Down**
- **Delete Row(s)**

*Note:* The pop-up menu does not display if you do not select an entry.

The figure “Network Settings tab” (page 454) shows the network settings fields.

**Figure 47**  
**Network Settings tab**



### Network settings during discovery

Network settings are applied during the discovery process as follows:

- The discovery process searches for a matching network setting entry starting at the top of the network settings list. Therefore, it is important to order the rows in the network settings properly.
- The matching, which includes wild carding, is performed on the IP address, device type (if specified). A blank (empty) value for a device type matches any device type in the network settings list. Then matching is done on port, community string and SNMP version.
- The discovery process attempts to apply the first match that it finds in the network settings that fits its criteria. If all constraints (such as valid IP range, device type exclusion, and absence of a similar device) are satisfied, then it tries to add the device with these settings.

- If the first match fails because constraints are not satisfied, the searching process continues down the network settings list for another best match.

This process continues until the discovery attempt is successful, or the end of the network settings list is reached.

For procedural information, see

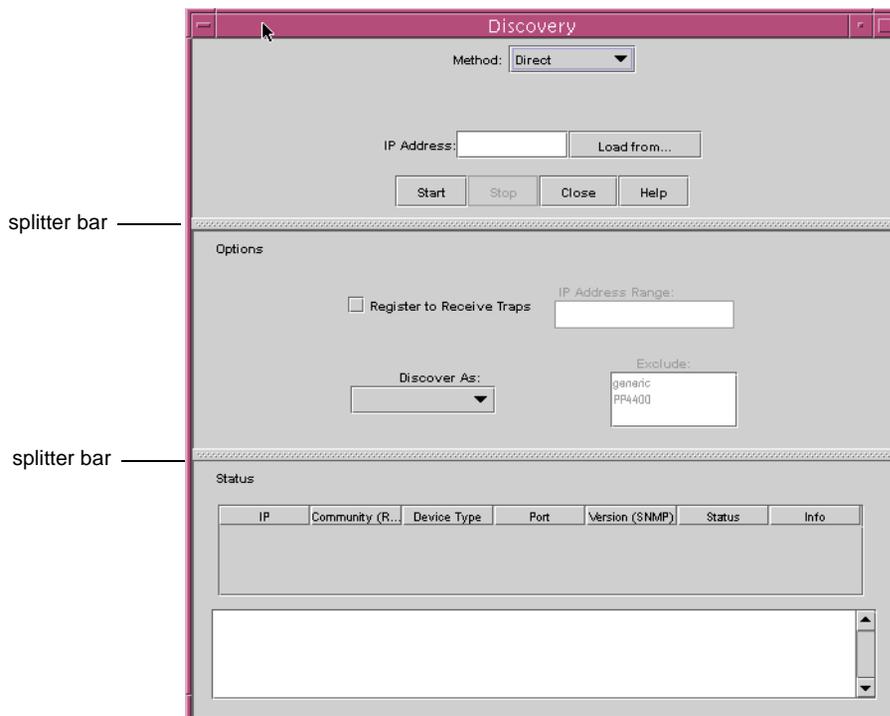
- “Creating a network setting” (page 443)
- “Changing network settings” (page 444)
- “Deleting network settings” (page 445)
- “Moving rows in network settings” (page 446)

## Discovery window

The Discovery window opens when you select **Device** -> **Discover** from the **IP Device Discovery** window. The window is split in to three sections. The **Options** area is hidden by default. View the **Options** area by clicking on the splitter bar and dragging the bar to the desired location.

See the figure “Discovery window” (page 456), which shows the **Options** area.

**Figure 48**  
**Discovery window**



The Discovery window contains the following items:

- **Method** contains a pull-down menu to choose the device discovery type. The options are **Direct**, and **Route based** discovery.

- **IP Address** lists the IP addresses or hostnames separated by a comma. When you select direct discovery, it lists the IP addresses or hostnames to be discovered. When you select **route-based discovery**, this field holds IP addresses or hostnames of seed devices. The **IP Address** field also contains the following pop-up menu items:
  - **Cut** lets you cut IP addresses or hostnames.
  - **Copy** lets you copy IP addresses or hostnames.
  - **Paste** lets you paste IP addresses or hostnames.
  - **Delete** lets you delete IP addresses or hostnames.
  - **Select All** lets you select all of the IP addresses or hostnames.
- **Load from** displays a file browser to let you select a file from which to read the IP addresses. The format of the file can be one of the following:
  - a comma separated list of hostnames and/or IP address
  - a host name or IP address entry per line without any punctuation (commas are allowed at the end of the line).

An example of the file format is as follows:

- 12.2.2.3
  - 12.2.4.5
  - xyz123
- **Register to Receive Traps** When you check this box, the discovery process attempts to register with the device to receive traps using the SNMP Target MIB specification in RFC 2573, and the SNMP view based ACM MIB specification in RFC 2575. If the process is successful, then Preside Multiservice Data Manager (MDM) receives traps from these devices without having to log in to the devices and configure them manually for sending traps to the management workstation.

- **IP Address Range** is available for route-based discovery and provides a range to discover IP addresses. If the device is not contained within the range, they will not be discovered. This field is greyed out if direct discovery is selected. The **IP Address Range** field also contains the following pop-up menu items:

**Cut** lets you cut an IP address range.

**Copy** lets you copy an IP address range.

**Paste** lets you paste an IP address range.

**Delete** lets you delete an IP address range.

**Select All** lets you select IP address ranges.

Examples of the valid pattern specifications are as follows:

- 134.177.125.1-31: matches all addresses in the range 134.177.125.1 to 134.177.125.31
  - 134.177.125.\*: matches all addresses in the range 134.177.125.1 to 134.177.125.255
  - 134.177.125-128.\*: matches all addresses in the range 134.177.125.\* to 134.177.128.\*
  - \*.\*.\*: matches all addresses
- **Discover As** contains a pull-down menu for direct discovery that lists all supported device types. When no device type is selected, the device is discovered as the type of device indicated by querying its sysObjectId. When a specific device type is selected, the device is discovered explicitly as the device type, without any queries being performed to verify the settings. To select more than one device type, press the shift key or the control button while selecting devices. To deselect an item, press the **Ctrl** key and left-click the mouse. The **Discover As** field is disabled automatically.

*Note:* “Discover As” does not guarantee that a device will be added to the device lists immediately, later, or not at all. It depends on the driver, the state of the device, and the network settings under the network settings tab.

*Note:* Specifying a device type is an optional step. For most device discoveries, it is typical to leave the **Discover As** option blank (default value)

- **Exclude** disables the discovery of selected device types for route-based discovery.
- **Start** starts the discovery process.
- **Stop** stops the discovery process.
- **Close** closes the Discovery window.
- **Help** displays help on how to use the Discovery window.
- **Status** shows the status of the discovery process.

The data collection daemon (DCD) attempts to discover the device for up to three days after the discovery request is made. A discovery request is shown as **Pending** in **Status** column in the **Discovery** window. When the device is successfully discovered, the status changes to **Succeeded**.

For procedural information, see

- “Discovering devices using direct discovery” (page 436)
- “Discovering devices using route-based discovery” (page 437)

## Route-based discovery

Route-based discovery reads the addresses of neighbouring devices from `ipRouteNextHop` in the routing table of the seed device found in the IP Address field of the Discovery window. The discovery process is then able to obtain a list of devices to reseed the algorithm with. The address resolution protocol (ARP) cache is also examined for potential devices. When a device type is included in the exclude list, that device cannot be discovered. It does not, however, prevent the devices in its routing table from being discovered.

## Direct discovery

Direct discovery accepts a list of devices, and attempts to discover each device as a SNMP-managed device.

### **Why a discovery may fail**

A discovery request may fail for the following reasons:

- The IP address or IP Address Range entered are not properly formatted.
- The device cannot be communicated with using the current settings.
- The device has already been discovered.
- A device with the same IP address and community string is already being managed by Preside Multiservice Data Manager (MDM).

## Logging

When a user performs any IP Discovery functions, the output messages and errors are displayed in the status area of the IP Device Discovery window. These messages and additional debugging information are also logged in log files. The log files are located in the directory `/opt/MagellanNMS/data/log/ipm` by default. Error log files have an extension of `.err` by default. The standard output log file has an `.out` extension by default.

Two variables determine the location where the output messages and errors are logged. They are contained in the file `/opt/MagellanNMS/bin/ipDiscovery`. These variables and their defaults are:

- `MDM_IPM_OUT_FILE=/opt/MagellanNMS/data/log/ipm/ipDiscovery.out`
- `MDM_IPM_ERROR_FILE=/opt/MagellanNMS/data/log/ipm/ipDiscovery.err`

Setting these variables to an appropriate file name causes output/errors from all scripts in the IP Discovery tool to be logged to the specified files.

To change the location of these files, see “Changing the IP Discovery log location” (page 461).

### Changing the IP Discovery log location

- 1 Close all instances of the IP Discovery application.
- 2 With root privileges, edit the file `/opt/MagellanNMS/bin/ipDiscovery` and set the values for `MDM_IPM_OUT_FILE` and `MDM_IPM_ERROR_FILE` to direct output to the desired log location.
- 3 Launch IP Discovery again.

## Error messages

The table “IP Discovery error messages” (page 462) contains information on error messages, their cause and action required.

**Table 66**  
**IP Discovery error messages**

Message	Details	Remedial action
Error: cannot resolve IP Address for host <host>		Verify that the IP address is correct.
Error: cannot find hostname <host>		Verify that the hostname is correct.
Error: cannot setup SNMP session to <IP address>		Verify MagTcl installation.
Error: unable to walk routing table	During route-based discovery, an attempt to read the routing table of a device was unsuccessful. No new devices were learned from the routing table of this device.	
Error: unable to walk ARP table	During route-based discovery, an attempt to read the ARP table of a device was unsuccessful. No new devices were learned from the ARP table of this device.	
Error: no valid agent profile found	DCD cartridge is not installed.	Install the required device integration cartridge.
Error: unable to register to receive traps	The trap registration option was used during discovery. The discovery was successful, but the trap registration was not.	Manually register for traps with the device.
(Sheet 1 of 3)		

**Table 66 (continued)**  
**IP Discovery error messages**

Message	Details	Remedial action
Error: device doesn't support trap registration	Trap registration was selected during discovery, but the device does not support the required MIBs, as outlined in RFC 2573 and RFC 2575.	Manually register for traps with the device.
Error: unable to open <file>. Defaulting to port 162.	Trap registration attempted to read Preside MDM's trap port from the appropriate file, but it was unable to. It proceeded to register to receive traps on the default SNMP trap port 162.	
Error: calculated SnmpTargetAddrParams too long. Try a shorter community string.	The read community string for this device is too long.	Shorten the read community string.
Error: cannot get sysObjectId from <IP address>.	Discovery was unable to perform an SNMP query to retrieve the device's sysObjectId.	Verify the SNMP community.
(Sheet 2 of 3)		

**Table 66 (continued)**  
**IP Discovery error messages**

<b>Message</b>	<b>Details</b>	<b>Remedial action</b>
Error: Application unable to read device list.	IP Discovery encountered an application error while trying to retrieve the current list of devices. This is most likely caused by system resource issues. This error is usually seen when there are other Java applications running on the workstation, and there are multiple launches of IP Discovery.	Exit unnecessary Java applications. Verify swap space is configured as recommended in 241-6001-101 <i>Preside MDM Engineering Guide</i> .
The help server is not running, please launch nmstool.	For IP Discovery's help to work, the help server must be running. This server is started when you launch nmstool.	Launch nmstool and retry the IP Discovery help.
(Sheet 3 of 3)		

## Warning messages

The table “IP Discovery warning messages” (page 465) contains information on warning messages, their cause and action required.

**Table 67**  
**IP Discovery warning messages**

Message	Details	Remedial action
Warning: entry not found in Vacm Security Table. Unable to Delete.	The feature to remove trap registration with the specified device is being used during device deletion, but trap registration from IP Discovery was never successfully performed against the device.	Manually unregister for traps with the device.
Warning: no entry in SNMP target address table.	The feature to remove trap registration with the specified device is being used during device deletion, but trap registration from IP Discovery was never successfully performed against the device	Manually unregister for traps with the device
Warning: no entry in SNMP target params table.	The feature to remove trap registration with the specified device is being used during device deletion, but trap registration from IP Discovery was never successfully performed against the device	Manually unregister for traps with the device
Network Model is in edit mode: device deletion from Network Model failed.	The network model is currently being edited, so the device is only partially deleted. It is deleted from the DCD, but remains in the network model.	Manually delete the device from the network model.
(Sheet 1 of 2)		

**Table 67 (continued)**  
**IP Discovery warning messages**

<b>Message</b>	<b>Details</b>	<b>Remedial action</b>
Warning: network settings currently locked by either an editing session or another discovery process. Discovery results may be less predictable.	The network settings are in edit mode. The network settings tab has been selected by a user either on the same instance or another instance of IP Discovery.	Stop the discovery process. Verify that no instance of the IP Discovery window has the network setting tab selected. Select the Devices tab and restart.
xx.xx.xx.xx could not be added. APPLICATION_ERROR No process to query.	IP Discovery attempts to add the device but cannot find the DCD process to communicate with.	Ensure that SMDR is connected with the DCD process and the DCD is running.
(Sheet 2 of 2)		

## Chapter 13

# Circuit Viewer

---

This section describes the Circuit Viewer interface and contains the following topics:

- “Circuit Viewer overview” (page 467)
- “Circuit management log files” (page 469)
- “Circuit Viewer window” (page 470)
- “Online help” (page 487)
- “Procedures” (page 488)

### Circuit Viewer overview

The Circuit Viewer tool is one component of the Preside Multiservice Data Manager (MDM) circuit management suite. This tool works in conjunction with the MDM Database Administration tool, service provisioning tools, and the Administration Database to support the management of circuits in the network. For details about the MDM Database Administration tool and the Administration Database, see 241-6001-400 *Preside MDM Administration Database User Guide*. For details about the supported service provisioning tools, see 241-6001-600 *Preside MDM Service Provisioning for ATM User Guide* and 241-6001-603 *Preside MDM Service Provisioning for Frame Relay User Guide*.

Circuit Viewer retrieves circuit information from the Administration Database. You can specify criteria for searching the database. The Circuit Viewer tool displays a list of circuits that meet the specified criteria. Then, from this list of circuits, you can select a circuit for which you want detailed

information. You can view data that includes the circuit information such as the circuit ID and type, customer information, circuit components, and connection states of those components.

The Circuit Viewer tool service diagnostic information helps you manage faults in the network. These diagnostics include state information about the circuit, circuit components, and connection components. As well, you can view a selection of statistics for the connection, interface, and port components across a circuit.

The Circuit Viewer supports the following circuits types:

- ATM
  - PVC
  - SPVC
  - PVP
  - SPVP
  - FR/ATM Access NPVC
  - FR/ATM Access SPVC
  - Trunk over ATM PVC
- Frame Relay
  - FRNNI
  - FRUNI
- Frame Relay IP VPN Access
  - Backhaul Access (2764)
  - Direct Access (2764)
  - IP Optimized Direct (2764 and 2547)
  - IP Optimized Backhaul (2764 and 2547)

## Circuit Viewer server configuration

To use the Circuit Viewer application, you need to configure the Passport command access server. For details, see the section on the Passport command access server (PPAccessServer) in 241-6001-310 *Preside MDM Server Reference Guide*.

If the Passport command access server is on a different machine than Circuit Viewer, then you should specify the appropriate host via Options->Server Configuration in Circuit Viewer. Otherwise, Circuit Viewer will be unable to connect to the server. For more information, refer to “Setting the server configuration options” (page 493).

## Circuit management log files

The Circuit Viewer tool stores log messages in the `/opt/MagellanNMS/data/log/CircuitManagement.log` file. These log files have a maximum size of 10 megabytes (MB). When this limit is reached, the content of `CircuitManagement.log` is moved and stored in `CircuitManagement.log.1`. New log messages accumulate in `CircuitManagement.log` once again. When `CircuitManagement.log` reaches its maximum size again, the following changes occur:

- the content of `CircuitManagement.log.1` moves to `CircuitManagement.log.2`
- the content of `CircuitManagement.log` moves to `CircuitManagement.log.1`
- new log messages accumulate in `CircuitManagement.log`

Current log messages are always stored in `CircuitManagement.log`. When this file reaches its size limit, the content is moved to another file in sequence. This roll-over process continues to create additional log files up to `CircuitManagement.log.9`. This method allows for a maximum of ten log files—one actively accumulating new log messages and nine others containing progressively older messages. When the maximum number of log files is reached, the roll-over process continues but the content of the oldest file, `CircuitManagement.log.9`, is lost.

*Note:* If a log file does not roll over as expected, another application may have a process that has the log file open. A rollover will occur when no process has the log file open and the log file nears its maximum size.

Since each log file can occupy up to 10 MB of disk space, and there are up to 10 log files, storage for log files can reach 100 MB. Therefore, it is recommended that you have a file management strategy that includes archiving and deleting older log files.

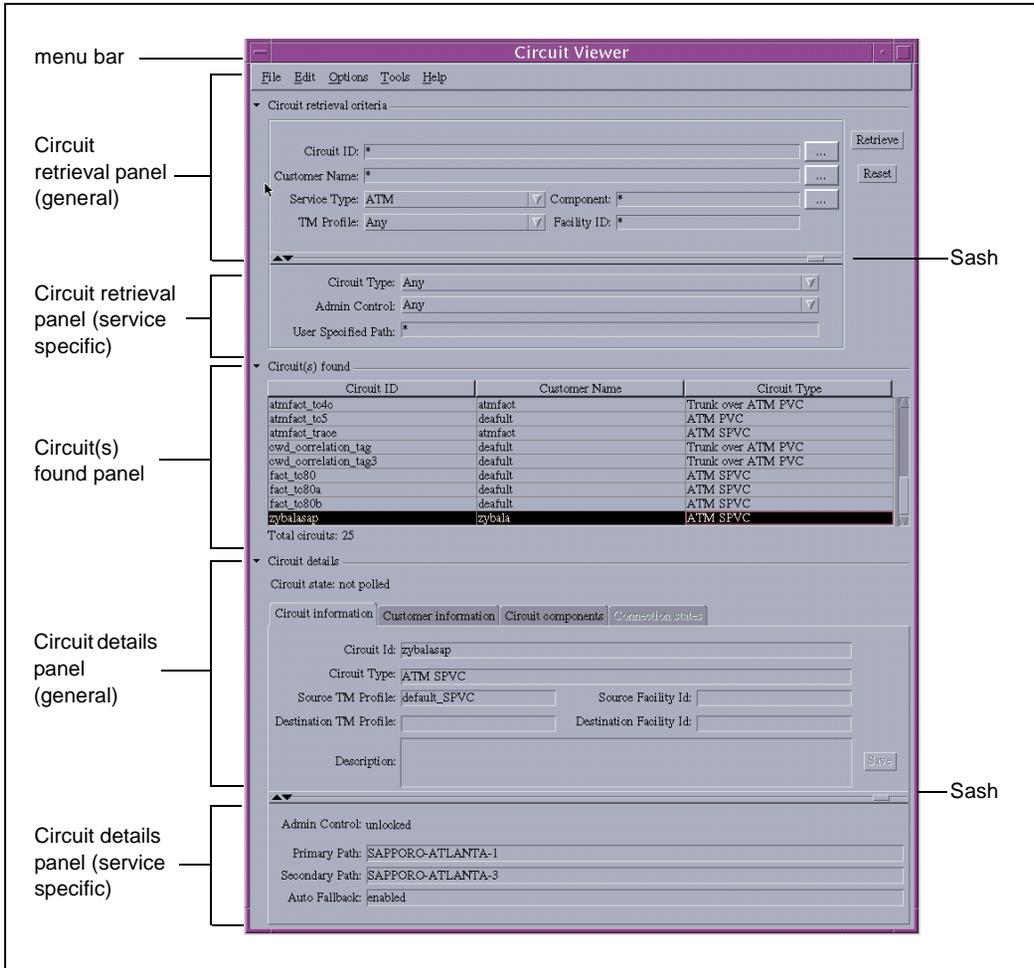
The MDM Database Administration tool also writes to the circuit management log file. As well, the ATM service provisioning tool writes to the circuit management log file if the provisioning causes errors in the Administration Database. Therefore, if you want to delete a current log file, first ensure that the log file is not being used by another application.

The Frame Relay Service Provisioning tool can be launched from a Frame Relay IP VPN Access circuit as long as the circuit is complete (status Normal) and it has been assigned to an IP Access Point.

## **Circuit Viewer window**

The figure “Circuit Viewer window” (page 471) shows a sample Circuit Viewer window.

**Figure 49**  
**Circuit Viewer window**



The Circuit Viewer window consists of the following elements:

- “Menu bar” (page 472)
- “Circuit retrieval criteria panel” (page 474)
- “Circuit(s) found panel” (page 477)
- “Circuit details panel” (page 478)

- “Sashes” (page 487)

For tasks that you can perform using Circuit Viewer, see “Procedures” (page 488).

## Menu bar

The menu bar contains the following menus:

- “File menu” (page 472)
- “Edit menu” (page 472)
- “Options menu” (page 472)
- “Tools menu” (page 473)
- “Help menu” (page 474)

### File menu

The File menu contains the following command:

- **Exit** closes the Circuit Viewer main window and exits the application.

### Edit menu

The Edit menu contains the following commands:

- **Copy** copies the current entry from the system clipboard.
- **Cut** deletes any selected text.
- **Paste** copies the current contents of the system clipboard to the current cursor position.
- **Select All** selects all entries in any editable text area.
- **Deselect All** cancels the selection of the Select All command.

### Options menu

The Options menu contains the following commands:

- **Server Configuration...** opens the Configuration dialog. Using this dialog, you can specify an MDM server host and port for accessing on-switch component information. To set the configuration options, see the procedure “Setting the server configuration options” (page 493).

- **Polling Configuration...** opens the Polling Configuration dialog for setting the circuit state and circuit component state polling. To set the polling configuration options, see the procedure “Setting the polling configuration options” (page 506).
- **Authentication...** opens the Authentication dialog where you specify default and node specific user names and passwords. To authenticate, see the procedure “Setting authentication information” (page 495).
- **Logging...** opens the Logging Options dialog where you select the type of information to log. To set the level of log information, see the procedure “Setting log file information levels” (page 494). Log messages are saved in the /opt/MagellanNMS/data/log/CircuitManagement.log file. For details about managing the size of log files, refer to “Circuit management log files” (page 469) and the section on circuit management log files in 241-6001-400 *Preside MDM Administration Database User Guide*.

## Tools menu

The Tools menu contains the following commands:

- **ATM Service Provisioning** starts the ATM service provisioning tool. To start the ATM service provisioning tool, see the procedure “Starting a service provisioning tool without context” (page 515). For information about ATM service provisioning, see 241-6001-600 *Preside MDM Service Provisioning for ATM User Guide*.
- **FR Service Provisioning** starts the Frame Relay service provisioning tool. To start the Frame Relay service provisioning tool, see the procedure “Starting a service provisioning tool without context” (page 515). For information about Frame Relay service provisioning, see 241-6001-603 *Preside MDM Service Provisioning for Frame Relay User Guide*.
- **MDM Database Administration** starts the MDM Database Administration tool. To start the MDM Database Administration tool, see the procedure “Starting the MDM Database Administration tool from Circuit Viewer” (page 517).

You can customize the contents of the Tools menu. For details, see the section on customizing menus that start other tools in 241-6001-301 *Preside MDM Customization Administrator Guide*.

## Help menu

The Help menu contains the following commands:

- **On Window** displays descriptive information about the Circuit Viewer window components.
- **On Context** displays information about a selected area of the Circuit Viewer window.

## Circuit retrieval criteria panel

Use the circuit retrieval panel to specify the criteria for searching the Administration Database. For some fields in this panel you can type an entry or a search pattern. For other fields you can use the drop down menu to select an entry.

This circuit retrieval panel has two sections: a general retrieval criteria area and a service retrieval criteria area. The general area lets you specify retrieval criteria that are applicable to all circuit service types. The service retrieval criteria area lets you specify retrieval criteria that are specific to a service type. The service criteria area is hidden until you select a service type.

### General retrieval criteria

The general retrieval criteria area lets you retrieve circuit information from the Administration Database based on the following criteria:

- **Circuit ID** retrieves circuits matching the identifier from the database. An asterisk (\*) in this field acts as a wildcard. This field supports a browse button [...] that provides a list of available circuit IDs.
- **Customer Name** retrieves circuits associated with customer names. An asterisk (\*) in this field acts as a wildcard. This field supports a browse button [...] that provides a list of available customers.
- **Service Type** retrieves circuits based on the specified service type. When you select a specific service type, its associated panel opens below the general panel to provide additional search criteria.
- **TM Profile** retrieves circuits based on types of service offerings.
- **Component** retrieves circuits based on the name of a component. An asterisk (\*) in this field acts as a wildcard. This field supports a browse button [...] that provides a list of available components.

- **Facility ID** retrieves circuits based on the facility identifier at either end of the circuit. An asterisk (\*) in this field acts as a wildcard.

The Circuit Viewer tool matches the TM Profile and Facility IDs against the values associated with circuit endpoints only, not intermediate components as in the case of a nailed up PVC.

### ATM retrieval criteria

The ATM service retrieval panel opens when you specify a service type of ATM.

- **Circuit Type** identifies the type of ATM circuit to retrieve from the database. The following types are available: PVC, SPVC, PVP, SPVP, FR/ATM Access NPVC, FR/ATM Access SPVC and Trunk over ATM PVC.
- **Admin Control** identifies the initial state of the connection following initial provisioning and after FP restarts and software reloads. The following values are available: permLocked and unlocked. If you select permLocked, the VPI and VCI numbers are reserved on the source node of the call but no bandwidth is used.
- **User Specified Path** specifies either the primary or secondary manual designated transit line (MDTL) route. If you do not want the MDTL path to be considered in the search, leave this field blank.

### Frame Relay retrieval criteria

The Frame Relay service retrieval panel opens when you select a service type of Frame Relay.

- **Data Network Address** identifies the data network address of the FrUni or FrNni at either the local or remote end.

### IP VPN Access criteria

The IP VPN Access retrieval panel opens when you select a service type of IP VPN Access.

- **Circuit Type** identifies the specific type of IP VPN Access circuit. The only type currently supported is FR IP VPN Access.

- **Site** identifies the name of the site containing the IP Access Points on which the desired circuits terminate. An asterisk (\*) in this field acts as a wildcard. This field supports a browser button [...] that provides a list of available sites based on the selected customer.
- **Access Point** identifies the name of the IP Access Point on which the desired circuits terminate. An asterisk (\*) in this field acts as a wildcard. This field supports a browse button [...] that provides a list of available access points based on the selected site. If the selected site is set to "Unassigned", the list will only show the access points that have not been assigned to any site. If a user chooses "Unassigned" from the list of the available access points, only the circuits that have not been assigned to any access point will be retrieved.
- **Interface** identifies the name of the Logical Interface component on which the desired circuits terminate.

**Note:** The **Site** and **Access Point** fields are enabled if the radio button to the left of the fields is selected. The **Interface** field is enabled if the radio button to the left of the field is selected.

For more information on setting up Sites and Access Points, refer to 241-6001-603 *Preside MDM Service Provisioning for Frame Relay User Guide* and 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*.

## Context support

Context refers to variables that are shared among the Preside Multiservice Data Manager (MDM) tools using the MDM Context Server. The Circuit ID and Component fields in the retrieval panel support context. You can retrieve a circuit or component if it is in context by right-clicking on the field and selecting the Get Context command from the popup menu. For information about using context, see “Putting a component or circuit into context” (page 513) and “Getting a component or circuit from context” (page 514).

## Command buttons

This panel contains the following command buttons:

- Retrieve  
The button initiates a retrieval from the Administration Database

- **Reset**  
This button resets the values in the Circuit retrieval criteria panel back to their default settings.

## Circuit(s) found panel

The Circuit(s) found panel displays a table containing all circuits in the database that meet the search criteria specified in the Circuit retrieval panel. The table includes the circuit identifier (ID), customer name, and the circuit type.

A Frame Relay circuit appears as a single circuit in the Circuit(s) found panel although it is actually several circuits. A Frame Relay circuit consists of a primary circuit and up to seven backup circuits, of which any can be active at a given time.

The name stored in the database for all IP VPN Access circuits is "IpCos". When an IP VPN Access circuit is displayed in the Circuit Viewer, it is further distinguished by its Site and Access Point, if they are known, and its IP CoS index. The name has the format Site/<site\_name> AccessPoint/<access\_point\_name> IPCoS/<IP CoS index>. For example:

Site/Ottawa Access Pt/Lab5 IpCos/1

If the Access Point or Site are not known, the string "none" appears as the name. For example:

Site/(none) Access Pt/(none) IpCos/0

Site/(none) Access Pt/Lab5 IpCos/1

Under certain conditions, icons display in the Circuit(s) found panel. For the circuit types SPVC and SPVP, a lock icon may display in the Circuit ID column. This icon indicates the connection is provisioned as locked. Absence of the lock icon can indicate that the circuit is unlocked or that the component is at a release prior to the introduction of the adminControl attribute (PCR 3.0).

You can reorder the display of columns in the Circuit(s) found list by dragging and dropping columns. See “Sorting a list in the Circuit(s) found panel” (page 499). You can also change the width of a column by dragging the

boundary line on the right side of the column heading until the column is the appropriate width. This panel also provides the total number of circuits based on the retrieval criteria.

When you select an entry from the circuit(s) found list, the circuit ID and serial number of that circuit are placed in context. Context lets you share information among other Preside Multiservice Data Manager (MDM) tools.

Right-clicking on a circuit in this panel opens a popup menu that lets you perform the following tasks:

- Launch Service Provisioning, see “Starting a service provisioning tool with context” (page 516)
- “Starting state polling” (page 508) or “Stopping state polling” (page 509)
- “Viewing circuit component statistics” (page 510)

## Circuit details panel

The Circuit details panel displays detailed circuit information including the following

- “Circuit state” (page 478)
- “Circuit information” (page 478)
- “Customer information” (page 480)
- “Circuit components” (page 481)
- “Connection states” (page 485)

### Circuit state

If you turn on state polling, the circuit state displays at the top of the Circuit details panel. The overall circuit state is computed based on the states of the circuit components. The state of a circuit component is based on its state attributes retrieved from the switch. To view more information about states of circuit components, select the Circuit components and Connection state tabs.

### Circuit information

The Circuit information pane displays general and service-specific information about the circuit selected in the Circuit(s) found list.

**General pane**

You can view the following information about circuits in the general circuit information pane:

- circuit identifier
- circuit type
- source traffic management profile
- destination traffic management profile
- source facility identifier
- destination facility identifier
- description

You can edit the circuit Description field from the Circuit information pane. To edit the other fields, you need to use the MDM Database Administration tool. The Save button saves any changes that you make to the circuit description in the Administration Database.

The figure “Circuit Viewer window” (page 471) shows a sample Circuit Viewer window with the Circuit Information tab selected.

**Service-specific pane**

You can view the following ATM information in the service-specific details pane:

- admin control
- primary path
- secondary path
- automatic fallback

Depending on the Admin Control values, icons may display in the Circuit information pane. A lock icon in the Admin Control field denotes a circuit that has been provisioned as locked.

No service-specific information is available for Frame Relay circuits.

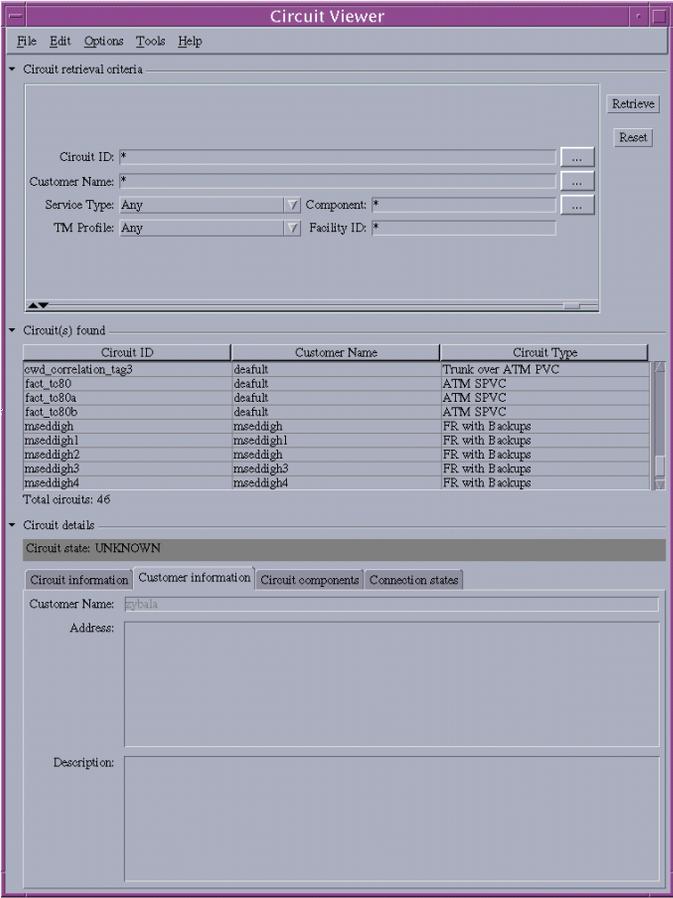
For IP VPN Access circuits, you can view the component ID of the IP Logical Interface if it is known.

### **Customer information**

The Customer information pane displays information about the customer assigned to the circuit selected in the Circuit(s) found list. This pane displays the customer name and address and any additional comments associated with the customer.

The figure “Sample Circuit Viewer window with Customer Information tab selected” (page 481) shows the Customer Information tab in the Circuit Viewer window.

**Figure 50**  
**Sample Circuit Viewer window with Customer Information tab selected**



### Circuit components

The Circuit components pane displays a table containing the provisioned components for the circuit selected in the Circuit(s) found list. As well, the pane contains command buttons for performing operations on the circuit components.

The circuit component information table includes the node, interface, connection, state, and traffic management (TM) profile data for all circuit types. If there are component attributes that are circuit dependent, then these attributes appear as additional columns in the table. For ATM circuits, the additional column displays the setting of the `aisGeneration` attribute for ATM SPVC and SPVP source connection components. For Frame Relay there is one column that indicates the DlcI type, either master or slave, and another column that displays the `dataNetworkAddress` attribute of the FrUni/FrNni Dna component. For FR IP VPN Access composite circuits, all components under the Frame Relay composite and the FrDte composite are displayed together in a single table.

The state of a circuit component shown in the table is derived from its own `operationalState` and `adminState` and that of its interface as well as additional state attributes, depending on the type of component. These states are shown in the Connection states tabbed pane.

When displaying SPVC and SPVP components, Circuit Viewer tries to find the destination `AtmIf` or `FrATM` interface from the called address. For `AtmIf`, if no address is provisioned, then a default address is computed by the loader and stored in the Administration Database when the component is loaded. It is this computed address that is used for the matching process. If Circuit Viewer finds an exact match to a single interface, then the interface and the connection type display in the component list. If no match is found, or if multiple matches are found, then the called address and the connection component without the connection type display in the component list. For the latter case, the connection type could be either a `FrAtm DlcI` or an `AtmIf Vcc`. Circuit Viewer performs these matches for the following SPVCs and SPVPs:

- `FrAtm` to `FrAtm`
- `AtmIf` to `AtmIf`
- `FrAtm` to `AtmIf`

This type of address matching cannot be used for `AtmIf` to `FrAtm` since the provisioned `FrAtm` address is not in NSAP format.

The Circuit components pane supports a popup menu that lets you start other Preside Multiservice Data Manager (MDM) tools or retrieve provisioned or operational attributes for a single component. If there is no connection to the command manager server, or if the component is a node, then the component popup menu is not available.

For procedures on displaying component information, see “Displaying circuit component information” (page 500).

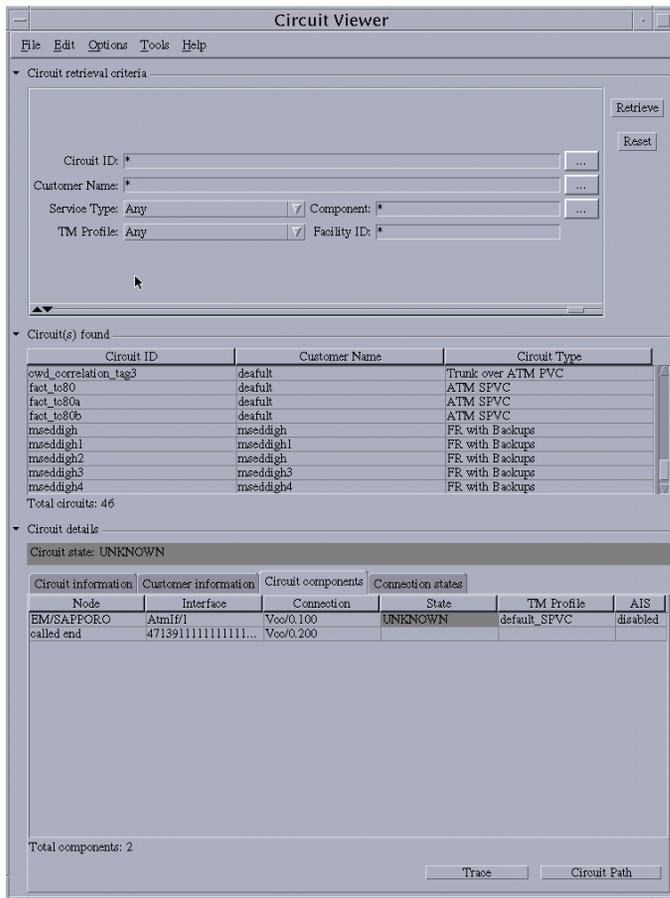
### **Command buttons**

The following command buttons are available in the Circuit components pane:

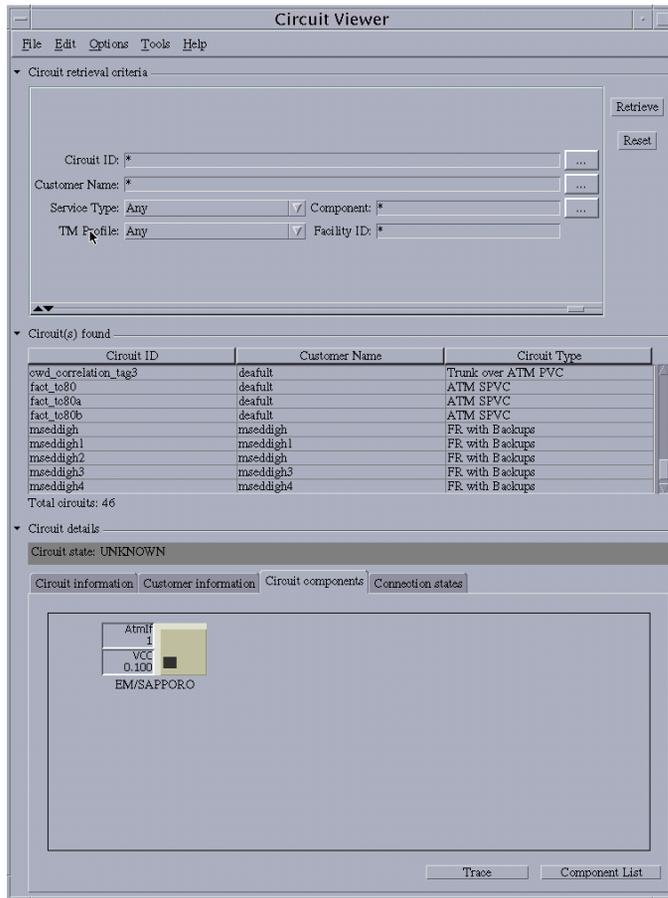
- **Trace** is available for ATM SPVC and SPVP circuits only. This button performs a PNNI connection trace on the source component. This trace provides the details for the intermediate circuit components in the path.
- **Circuit Path** is available for ATM circuits only. This button displays the circuit components graphically. When the display changes from tabular to graphical format, the label on the button changes to **List Components** to revert to the tabular format.

The figures “Sample Circuit Viewer window with Circuit Components tab (List view) selected” (page 484) and “Sample Circuit Viewer window with Circuit Component tab (Path view) selected” (page 485) show the two views of the Circuit components tab in the Circuit Viewer window.

**Figure 51**  
**Sample Circuit Viewer window with Circuit Components tab (List view)**  
**selected**



**Figure 52**  
**Sample Circuit Viewer window with Circuit Component tab (Path view)**  
**selected**



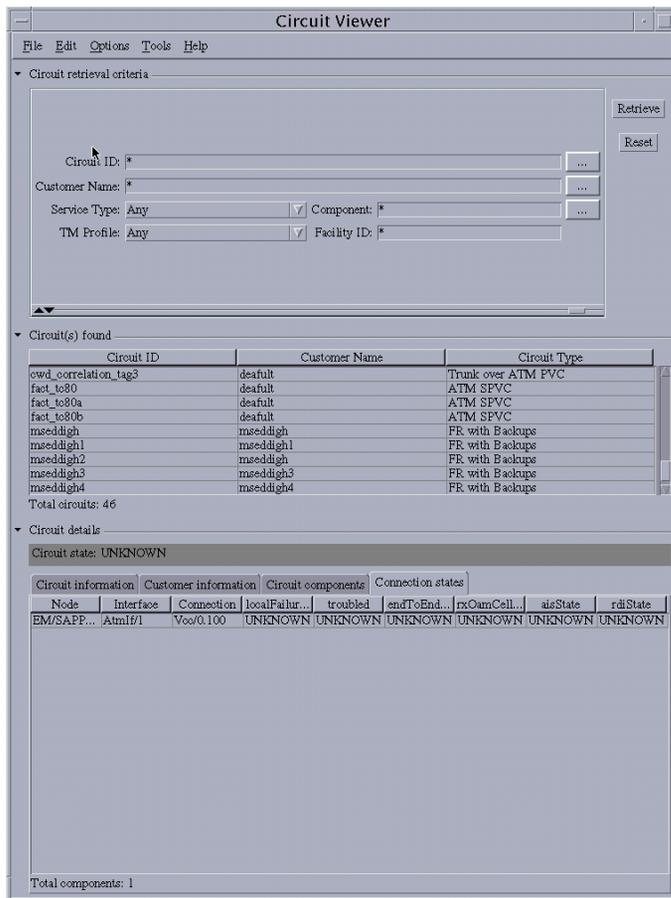
## Connection states

The Connection states tabbed pane is available only when state polling is turned on. This pane displays state attributes for each connection component that is polled. If a path trace has been done, the intermediate components will be displayed, otherwise just the endpoint state will be shown.

The node, interface and connection columns identify the connection components that make up the circuit. The remaining columns display the state attributes for each component.

The figure “Sample Circuit Viewer window with Connection states tab selected” (page 486) shows the Connection states tab in the Circuit Viewer window.

**Figure 53**  
**Sample Circuit Viewer window with Connection states tab selected**



## Sashes

There are a series of vertical sash bars in the window that let you change the amount of space a panel occupies. When you move a sash to increase the amount of space in one panel, the space for the other panels decrease correspondingly. To move a sash, drag the box in sash up and down.

## Online help

Help is available in most Preside Multiservice Data Manager (MDM) tools from either a Help menu or a Help button.

The Help menu provides general descriptive information for the Circuit Viewer tool. You can view a brief overview of the tool using the On Window command. Help on key areas of the window is available from the On Context command. For details, see “Displaying Circuit Viewer online help” (page 492).

General descriptive help is available for dialogs that contain a Help button. You can view the help information for a dialog by clicking the Help button in the dialog.

## Procedures

This section contains the following Circuit Viewer procedures:

### Getting Started

- “Starting the Circuit Viewer tool without component context” (page 490)
- “Starting the Circuit Viewer tool with component context” (page 491)
- “Displaying Circuit Viewer online help” (page 492)
- “Setting the server configuration options” (page 493)
- “Setting log file information levels” (page 494)
- “Setting authentication information” (page 495)

### Working with circuit information

- “Retrieving a list of circuits from the Administration Database” (page 496)
- “Using the Component Selection Dialog” (page 498)
- “Sorting a list in the Circuit(s) found panel” (page 499)
- “Displaying circuit component information” (page 500)
- “Displaying provisioned or operational attributes of a component” (page 502)

### Diagnosing circuits

- “Displaying a connection trace” (page 505)
- “Setting the polling configuration options” (page 506)
- “Starting state polling” (page 508)
- “Stopping state polling” (page 509)
- “Viewing circuit component statistics” (page 510)

### Using component context

- “Putting a component or circuit into context” (page 513)
- “Getting a component or circuit from context” (page 514)

**Starting other tools from Circuit Viewer**

- “Starting a service provisioning tool without context” (page 515)
- “Starting a service provisioning tool with context” (page 516)
- “Starting the MDM Database Administration tool from Circuit Viewer” (page 517)

For an overview of the Circuit Viewer tool and a description of the window, see “Circuit Viewer” (page 467).

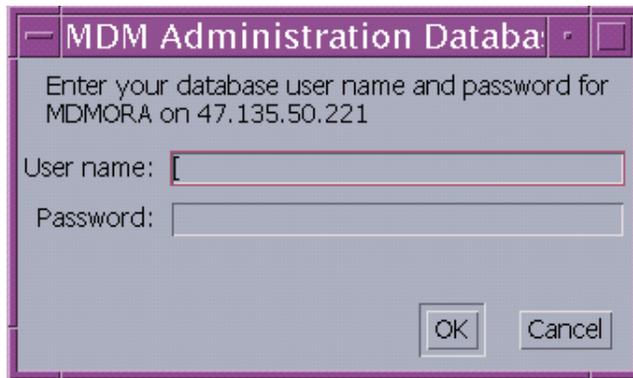
## Starting the Circuit Viewer tool without component context

Use this procedure to start the Circuit Viewer tool without component context.

### Procedure

- 1 In the Preside Multiservice Data Manager window, select **Fault** and then **Circuit Viewer**.

The MDM Administration Database authentication dialog opens.



- 2 In the MDM Administration Database authentication dialog, type a valid user name and password and click **OK**.

The Circuit Viewer tool opens.

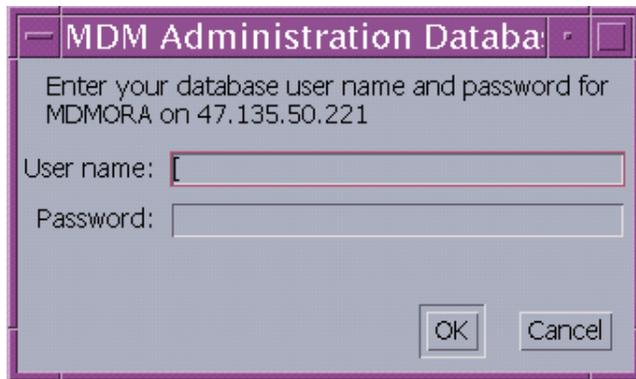
## Starting the Circuit Viewer tool with component context

Context lets you transfer component information among other Preside Multiservice Data Manager (MDM) tools that also support context. Starting Circuit Viewer with context populates the Component field in the Circuit retrieval panel with the component in context. Use this procedure to start the Circuit Viewer tool with component context.

### Procedure

- 1 From any of the Preside Multiservice Data Manager (MDM) tools that support context, select a component.
- 2 Open the **Start Tools** menu and select **Fault ->Circuit Viewer**.

The MDM Administration Database dialog opens.



- 3 In the MDM Administration Database dialog, type a valid user name and password and click **OK**.

The Circuit Viewer window opens with a circuit list that displays all circuits containing the selected component.

**Note:** The Network Viewer tool lets you select multiple nodes. If you select more than one node in Network Viewer and then start Circuit Viewer, Circuit Viewer opens with the first node that you selected.

## Displaying Circuit Viewer online help

Help is available in most Preside Multiservice Data Manager (MDM) tools from either a Help menu or a Help button. Use this procedure to view online help for the Circuit Viewer tool. You can view general descriptive information for the tool or context-specific help information.

### Procedure

- 1 For an overview description, from the Circuit Viewer window **Help** menu, select **On Window**.

The online help window opens with a general description of the Circuit Viewer tool.

- 2 For help on a specific area of the main window, from the Circuit Viewer **Help** menu, select **On Context**.

The mouse changes to a question mark (?).

- a. Move the mouse pointer onto an area of the Circuit Viewer window for which you want help and click the mouse button.

The online help window opens with information specific to the area you selected.

## Setting the server configuration options

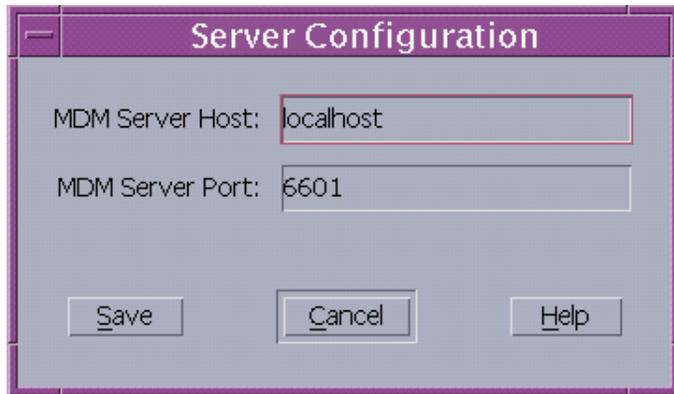
Use the Server Configuration dialog to change the settings for the MDM server host and port for accessing on-switch data. You need to change the server configuration information for the following reasons:

- If the Circuit Viewer tool resides on a client, then you need to specify the appropriate IP address of the MDM server host.
- If you are not using the default server port of 6601 for the Passport Command Access server, then you need to specify the server port number in the startup command for the server in the Server Administration tool. For details about configuring the Passport command access server, see the section on the Passport command access server (PPAccessServer) in 241-6001-310 *Preside MDM Server Reference Guide*

### Procedure

- 1 From the **Options** menu, select **Server Configuration**.

The Server Configuration dialog opens.



- 2 In the **MDM Server Host** field, type a valid host name.
- 3 In the **MDM Server Port** field, type a valid port number.
- 4 To save the settings and close the dialog, click **Save**.

## Setting log file information levels

Use the Logging Options dialog to set the appropriate information level to save in the Circuit Viewer log file. Circuit Viewer stores the specified log information in the /opt/MagellanNMS/data/log/CircuitManagement.log file.

### Related information

For more information about log files and their file size restrictions, see the section on circuit management log files in 241-6001-400 *Preside MDM Administration Database User Guide*

### Procedure

- 1 From the **Options** menu, select **Logging**.

The Logging Options dialog opens.



- 2 From the dialog, select the level of messages you want to log.
- 3 Click **Apply**.

## Setting authentication information

Use this procedure to specify authentication information to be used to log into a Passport node to retrieve polling and statistical information.

### Procedure

- 1 From the **Options** menu, select **Authentication....**

The Authentication dialog opens.



- 2 In the **Default User ID** field, specify the default user ID for authentication to Passport devices.
- 3 In the **Default Password** field, specify the default password to authenticate to Passport devices.
- 4 If there are nodes where user IDs and passwords differ from the default, then complete the following steps:
  - In the **Node** field, type the node name to which you want to connect. Or, click the browse button [...] to the right of the **Node** field to display a list of nodes from which you can select.
  - In the **User ID** field, type the user ID for the specified node.
  - In the **Password** field, type the password for the specified node.
- 5 To save the authentication information and close the dialog, click **Apply**.

## Retrieving a list of circuits from the Administration Database

Use this procedure to retrieve one or more circuits from the Administration Database.

### How to specify retrieval criteria

To retrieve circuits from the Administration Database, you need to specify the criteria for searching the database. The Circuit Viewer window contains a circuit retrieval panel where you specify the required criteria. The more fields you complete, the more specific the search. The following list details the various methods for specifying retrieval criteria.

- **Accept the default value**

When Circuit Viewer opens, some fields in the window have values in them. These values are default values. For example, the Circuit ID field has an asterisk (\*) as a default value. The asterisk matches all values for the field in the database. You can accept the default value or specify a different value. A default value of "Any" matches any possible value for the field.
- **Type a value**

Some fields let you type a value in the field. You can type a specific value or a search pattern. For example, a specific value such as west\_spvc2 in the Circuit ID field causes the Circuit Viewer tool to search the database for the single circuit named west\_spvc2. If you use a search pattern, then the Circuit Viewer tool searches the database for all circuit identifiers that satisfy the search pattern. For example, a search pattern such as west\* causes the Circuit Viewer tool to search the database for all circuit identifiers that begin with the string "west".
- **Use the browse button**

Some fields have a browse button [...] on the right side of the field. Clicking the browse button opens a selector dialog that lists all possible values. You can then select a value from this list. The browse buttons for Circuit ID and Customer Name open their corresponding Selection Dialogs. The browse button for Component opens the Component Selection Dialog.
- **Use the drop-down list**

Some fields have a drop-down list from which you can make a selection. The Circuit Type field is an example of a field with a drop-down list.

- **Get Context**

Some fields, such as Circuit ID support context. To retrieve a value name from context, position the cursor over the field and right-click to open a pop-up menu. From the pop-up menu, select the Get Context command.

### Related information

For a description of the fields in the **Circuit retrieval criteria** panel, see “Circuit retrieval criteria panel” (page 474).

### Procedure

- 1 In the **Circuit retrieval criteria** panel, specify a circuit identifier in the **Circuit ID** field.

**Note:** The name of an IP VPN Access circuit is stored in the database as 'IPCoS'. The display name described in the Circuit(s) Found section is constructed. Therefore, when you search for an IP VPN Access circuit, you must specify the Customer, Site and IP Access Point information separately (do not enter the display name in the Name field).

- 2 To refine your search, complete any remaining fields in the general retrieval criteria panel. If you use the **Component** browse button to open the Component Selection Dialog and want information on using this dialog, see “Using the Component Selection Dialog” (page 498).
- 3 To include service-specific retrieval criteria, from the **Service type** drop-down list, select one of the following service types:

- ATM
- Frame Relay
- IP VPN Access

The service retrieval criteria panel opens. If you select Any, the service-specific retrieval panel does not open.

- 4 Complete the appropriate fields in the service retrieval criteria panel to refine your search.

**Note:** If you wish to search for circuits under a Site or Access Point, select the radio button to the left of the fields to enable the fields. If you wish to search for circuits terminating on a logical interface, select the radio button to the left of the Interface field.

- 5 Click **Retrieve**.

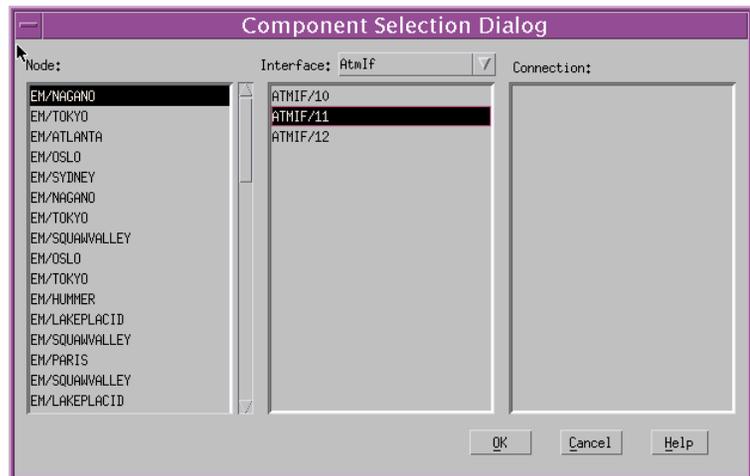
## Using the Component Selection Dialog

Use this dialog to select an interface or connection component to retrieve from the Administration Database.

### Procedure

- 1 In the **Circuit retrieval criteria** panel, click the **Component** browse [...] button.

The Component Selection Dialog opens.



- 2 Select a node by clicking on an entry in the **Node** list.
- 3 In the **Interface** box, select an interface type from the drop down list. The **Interface** list displays a list of interfaces.
- 4 To select an interface, click on an entry in the **Interface** list.
- 5 If needed, to select a connection component:
  - Double-click on an interface to display connection components.
  - Select a connection component in the **Connection** list.
- 6 Click **OK**.

## Sorting a list in the Circuit(s) found panel

Use this procedure to sort the items in the Circuit(s) found panel. You can sort by ascending or descending order.

### Procedure

- 1 If no list of circuits displays in the **Circuit(s) found** panel, specify retrieval criteria. For details, see “Retrieving a list of circuits from the Administration Database” (page 496).
- 2 To sort any column in descending order, position the mouse pointer in the column header and while pressing the Shift key, click the left mouse button.
- 3 To sort any column in ascending order, position the mouse pointer in the column header and click the left mouse button.

## Displaying circuit component information

Use this procedure to display information about nodes, interfaces, connections, states, and traffic management profiles related to a circuit and to view provisional and operational information for a circuit component.

### Related information

The **Circuit components** pane supports a pop-up menu to get additional component information or start other Multiservice Data Manager (MDM) tools. You can customize the lists tools that you can open from this pop-up menu. For details, see the section on customizing menus that start other tools in 241-6001-400 *Preside MDM Administration Database User Guide*.

### Procedure

1 If no list of circuits displays in the **Circuit(s) found** panel, then specify the retrieval criteria. For details, see “Retrieving a list of circuits from the Administration Database” (page 496).

2 Select a circuit from the **Circuit(s) found** list.

3 Click the **Circuit information** tab.

The General circuit information is displayed in the top panel. Circuit specific information is displayed in the bottom panel. For IP VPN Access circuits, the component Id of the Logical Interface is displayed if it is known.

4 Click the **Circuit components** tab.

The Circuit components pane opens. By default, the pane displays component information in text tables.

5 Optionally, you can change the way the information displays in the Circuits component pane.

- To reorder the display of columns in the table, drag and drop columns on the desired location.
- To change the width of a column, drag the boundary line on the right side of the column heading until the column is the desired width.
- To change from a text to a graphical format, click **Circuit Path**. To return to text format, click **Component List**.

6 Optionally, to start another MDM tool in context with the selected circuit, right-click on a component in the **Circuit components** pane to open a pop-up menu. From the pop-up menu, select an appropriate entry from the list of tools.

The selected MDM tool opens.

- 7 Optionally, you can view provisioned or operational attributes of a component. Go to the procedure “Displaying provisioned or operational attributes of a component” (page 502), step 4.

## Displaying provisioned or operational attributes of a component

Use this dialog to view provisioned or operational attributes of a component

- 1 If no list of circuits displays in the **Circuit(s) found** panel, then specify the retrieval criteria. For details, see “Retrieving a list of circuits from the Administration Database” (page 496).
- 2 Select a circuit from the **Circuit(s) found** list.
- 3 Click the **Circuit components** tab.  
The Circuit components pane opens. By default, the pane displays component information in text tables.
- 4 Double-click on a component in the tabular or graphical display. Alternatively, right-click on a component to open a pop-up menu. From the pop-up menu, select **Get Component Information**.

The Components Information dialog opens using information in context from the Circuit Viewer.

The screenshot shows a dialog box titled "Component Information". It is divided into several sections:

- Component login information:** Includes a "Node" field with "EM/ATHENS", a "User name" field with "system", a "Password" field with "\*\*\*\*\*", and a checked "Use Default Logon" checkbox.
- Component retrieval criteria:** Includes a "Component" field with "Atmf/Z11" and an "Information type" dropdown menu set to "Operational". A "Retrieve" button is located to the right of the dropdown.
- Details:** A table with two columns: "Attribute" and "Value". The table is currently empty.

At the bottom of the dialog are "Cancel" and "Help" buttons.

- 5 Provide the appropriate information to log on to a node using one of the following methods:
  - If no logon defaults exist in the current session and none are needed, type the appropriate values in the **User name** and **Password** fields.
  - To set the default logon information for the current session, type the appropriate values in the **User name** and **Password** fields and select the **User Default Logon** check box.

- To reset any existing default logon information for the current session, clear the **User Default Logon** check box and then type the appropriate values in the **User name** and **Password** fields and then select the Use Default Logon check box.
- 6 From the **Information type** drop-down list, select one of the following options:
    - **Operational**
    - **Provisioned**
  - 7 Click **Retrieve**.

The specified component information displays in the **Component Information** dialog.
  - 8 To close the **Component Information** dialog, click **Cancel**.

## Displaying a connection trace

By default, the Circuit Viewer tool displays only the source and, if provisioned, the destination connection components for an SPVC or SPVP. Use this procedure to perform a PNNI connection trace on the source component of an SPVC or SPVP circuit to determine the intermediate components that make up a circuit.

### Prerequisites

You need to supply a Passport user ID and password for a source node that has "config" impact before you can request a trace. If you have not already done so, see the procedure "Setting authentication information" (page 495).

### Procedure

- 1 If no list of circuits displays in the **Circuit(s) found** panel, then specify the retrieval criteria. For details, see "Retrieving a list of circuits from the Administration Database" (page 496).
- 2 In the **Circuit(s) found** panel, click on the SPVC or SPVP circuit for which you want circuit details.
- 3 In the **Circuit detail(s)** panel, click the **Circuit components** tab.  
The SPVC or SPVP endpoints display in the table.
- 4 In the **Circuit detail(s)** panel, click **Trace**.

If you have not already authenticated to the node, the Authentication Dialog opens. See the procedure "Setting authentication information" (page 495) for details about completing the Authentication Dialog.

If you have already authenticated, the trace begins. While the trace is in progress, the Trace button changes to Tracing...

If the trace is successful, the intermediate components display in the table. If state polling is turned on, the states of the intermediate circuit components will also be polled. The results of the trace include the egress components for the source node, the intermediate nodes, and the destination node. The trace does not include ingress virtual connections. If the circuit re-routes, the state of obsolete components displays as "does not exist". You can request another trace at this point, if the circuit re-routes.

If the trace is unsuccessful, a dialog opens and displays the reason for failure.

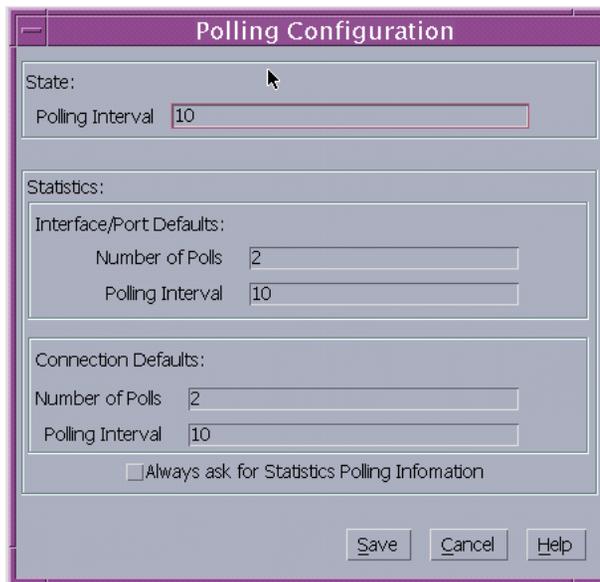
## Setting the polling configuration options

The Polling Configuration dialog lets you set the circuit state polling interval, the number of times the Circuit Viewer tool polls for interface and connection statistics, and the polling interval for interface and connection statistics. Use this procedure to set the configuration options for circuit state and circuit component statistics polling.

### Procedure

- 1 From the **Options** menu, select **Polling Configuration....**

The Polling Configuration dialog opens.



- 2 To change the polling options for circuit state
  - in the **State: Polling Interval** field, type the required number of seconds between polls
- 3 To change the polling options for interface component statistics
  - in the **Interface/Port Defaults: Number of Polls** field, type a value for the required number of polls for interface and port statistics. Leaving this field blank causes polling to continue indefinitely.

- in the **Interface/Port Defaults: Polling Interval** field, type the required number of seconds between polls for interface statistics

**Note:** Port Statistics is only available for ATM circuits.

- 4 To change the polling options for the connection component statistics
  - In the **Connection Defaults: Number of Polls** field, type a value for the required number of polls for connection statistics. Leaving this field blank causes polling to continue indefinitely.
  - in the **Connection Defaults: Polling Interval** field, type the required number of seconds between polls for connection component statistics.
- 5 If you want to have the option of changing the polling options each time you request statistics, select the check box **Always ask for Statistics Polling Information**.

When you request statistics, a Polling Parameters dialog opens with those parameters that are appropriate for the requested statistics.

## Starting state polling

Use this procedure to start the polling of circuit component state. An overall circuit state is determined from the polled component states.

### Prerequisites

Before you can turn on state polling, you need to supply Passport authentication information. For the authentication procedure, see “Setting authentication information” (page 495).

### Procedure

- 1 If no list of circuits displays in the **Circuit(s) found** panel, then specify the retrieval criteria. For details, see “Retrieving a list of circuits from the Administration Database” (page 496).
- 2 In the **Circuit(s) found** panel, right-click on the circuit for which you want the circuit state.  
  
A popup menu opens.
- 3 From the popup menu, select **Start State Polling**.  
  
If you have already authenticated to the node for which you want information, then the circuit state displays in the **Circuit detail(s)** panel.  
  
If you have not already authenticated to the node, the Authentication Dialog opens. See the procedure “Setting authentication information” (page 495) for details about completing the Authentication Dialog. When authentication to the node is successful state polling begins.
- 4 To view the components of a circuit and their states, in the **Circuit detail(s)** panel, click the **Circuit components** tab.
- 5 To view the values of the connection state attributes, in the **Circuit detail(s)** panel, click the **Connection states** tab.

## Stopping state polling

Use this procedure to stop circuit state polling.

### Procedure

- 1 In the **Circuit(s) found** panel, right-click to open the popup menu.
- 2 Stop state polling using one of the following methods:
  - From the popup menu, select **Stop State Polling**  
Circuit state polling stops and the component states change to "not polled".
  - Select another circuit and the polling for the previous circuit will be stopped automatically.

## Viewing circuit component statistics

Use this procedure to view a subset of key statistics for circuit components.

### Expected results

If you have set the polling configuration options to always ask for statistics polling information, the Polling Parameters dialog opens and displays only those parameters that are appropriate to the requested statistics. For information on polling configuration, see the procedure “Setting the polling configuration options” (page 506).

When you request connection statistics, a dialog opens and displays the statistics in tabular format. If the Circuit Viewer tool is unable to retrieve a statistic, "n/a" appears in the table cell and the reason for failure displays in the message panel below the statistics table. The reason for failure is logged in the `/opt/MagellanNMS/data/log/CircuitManagement.log` file

### Requirements

Before you can turn on component statistics polling, you need to supply Passport authentication information. For the authentication procedure, see “Setting authentication information” (page 495).

### Procedure

- 1 If no list of circuits displays in the **Circuit(s) found** panel, then specify the retrieval criteria. For details, see “Retrieving a list of circuits from the Administration Database” (page 496).
- 2 In the **Circuit(s) found** panel, right-click on the circuit for which you want statistical information.  
A popup menu opens.
- 3 From the popup menu, select **Statistics** and then one of the following entries:
  - **Connection Statistics**
  - **Interface Statistics**
  - **Port Statistics**

**Note:** Port Statistics is only available for ATM circuits.

A dialog opens displaying the requested statistics in tabular format.

Node	Interface	Connection	txCell	txCellDiscard	rxCell	rxCellDiscard
EM/SEOUL	AtmIf/30	Vcc/0_309	36818 (56)	0 (0)	36828 (56)	36828 (56)

Total components: 1

Messages:

Stop Polling Close Help

### Statistics dialogs

The Statistics dialogs contain a subset of key circuit component statistics.

When you request statistics, the Circuit Viewer polls for this information.

Each time a poll occurs, the dialog refreshes with the new statistics. Where relevant, changes from the previous poll are shown in brackets (). Polling for statistics continues until the maximum number of polls has been reached or until you click the Stop Polling button. To view or set the maximum number of polls, see “Setting the polling configuration options” (page 506).

While polling is in effect, a Stop Polling button is available. If you click the Stop Polling button or if the number of polls has been reached, the button changes to Re-start Polling. When you restart polling, polling resumes for the specified number of polls.

### Getting more statistics

If you require more comprehensive statistical information, you can start the MDM Data Viewer tool.

- 1 In the Connection Statistics dialog, right-click on a node for which you want detailed statistics.  
A popup menu opens.
- 2 From the popup menu, select Performance -> Data Viewer.

The Data Viewer tool opens with the selected node in context. For information about this tool, see 241-6001-031 *Preside MDM Performance Management User Guide*.

## Putting a component or circuit into context

Context lets you pass component information from Circuit Viewer to other Preside Multiservice Data Manager (MDM) tools that support context. Use this procedure to put a component or circuit into context.

### Procedure

- 1 To put a component into context, in the Circuit details panel, select the Circuit components tab and then select the component you want to put in context from either the text list or the graphical display.
- 2 To put a circuit into context, in the Circuit(s) found list, select the circuit you want to put in context

## Getting a component or circuit from context

Use this procedure to get a component or circuit from context. The Circuit ID and Component fields in the Circuit retrieval panel support the use of context.

### Procedure

- 1 Position the cursor over any of the fields in the **Circuit retrieval** panel that support context and right-click.

A popup menu opens.

- 2 From the popup menu, select **Get Context**.

The Circuit Viewer tool retrieves the value in context and then performs a search based on that value.

## Starting a service provisioning tool without context

Use this procedure to start the a service provisioning tool without context from the Circuit Viewer tool. The service provisioning tool that opens depends on the service type of the selected circuit.

### Related information

For details about the ATM service provisioning tool, see 241-6001-600 *Preside MDM Service Provisioning for ATM User Guide*.

For details about the Frame Relay service provisioning tool, see 241-6001-603 *Preside MDM Service Provisioning for Frame Relay User Guide*.

### Procedure

- 1 From the **Tools** menu, select one of the following:
  - **ATM Service Provisioning**
  - **FR Service Provisioning**

The selected service provisioning window opens.

**Note:** The FR Service Provisioning tool is only launchable when the selected IP VPN Access circuit is in "Normal" status and it has been assigned to an IP Access Point.

## Starting a service provisioning tool with context

Use this procedure to start a service provisioning tool with circuit context from the Circuit Viewer tool.

### Related information

For details about the ATM service provisioning tool, see 241-6001-600 *Preside MDM Service Provisioning for ATM User Guide*.

For details about the Frame Relay service provisioning tool, see 241-6001-603 *Preside MDM Service Provisioning for Frame Relay User Guide*.

### Procedure

- 1 If no list of circuits displays in the **Circuit(s) found** panel, then specify the retrieval criteria. For details, see “Retrieving a list of circuits from the Administration Database” (page 496).
- 2 In the **Circuit(s) found** field, select the circuit that you want to put in context.
- 3 Right-click on the selected circuit to display the popup menu.
- 4 On the popup menu, point to **Launch Service Provisioning** and then select one of the following commands.
  - **Edit Circuit** to start the service provisioning tool in Edit mode.
  - **Delete Circuit** to start the provisioning tool in Delete mode.

The service provisioning tool opens in context to the selected circuit ID.

## Starting the MDM Database Administration tool from Circuit Viewer

Use this procedure to start the MDM Database Administration tool from Circuit Viewer. The MDM Database Administration tool lets you perform administration tasks on a selection of objects in the Administration Database.

### Procedure

- 1 From the Tools menu, select **MDM Database Administration**.

The MDM Database Administration window opens.



## Chapter 14

# HP OpenView NNM desktop

---

This section describes how to start the Hewlett-Packard (HP) OpenView Network Node Manager (NNM) application from Preside Multiservice Data Manager (MDM) and how to access a selection of MDM tools from that application.

This section contains the following topics:

- “HP OpenView NNM overview” (page 519)
- “Root map” (page 520)
- “How HP OpenView NNM desktop displays device names” (page 520)
- “Procedures” (page 523)

### HP OpenView NNM overview

HP OpenView Network Node Manager (NNM) is an optional feature of MDM that provides access to the HP OpenView platform. To run this desktop application, you need HP OpenView and the HP OpenView Desktop for MDM software installed on the MDM workstation. After the required software is installed, you can start the HP OpenView NNM desktop application from the MDM toolset. Then, from the HP OpenView NNM desktop, you can access the following from the MDM software:

- fault management tools
- configuration management tools
- Data Viewer performance management tool
- Customer Database utility for access to customer information databases

- Command Console utility for direct access to a switching element

## Root map

When you start HP OpenView NNM from MDM, a Root map opens, displaying the Nortel Networks symbol and the IP Internet symbol. These symbols indicate the state of their respective networks through color. The standard HP OpenView color scheme is used. To view the standard color representation you can display the legend from the Help menu.

## How HP OpenView NNM desktop displays device names

HP OpenView NNM desktop displays Passport and DPN device names on the Nortel Networks submap.

### Passport devices

For Passport nodes, the icons distinguish between Passport nodes belonging to the 6000, 7000 and 15000 series.

- Icons depicting Passport legacy and 6000 nodes contain P6 or 6.
- Icons depicting Passport 7000 nodes contain P7 or 7.
- Icons depicting Passport 15000 nodes contain P15 or 15.
- Icons depicting unknown Passport nodes contain P? or ?. Although the devices are in the database, it has not yet been configured to identify these devices. To change these icons to identify the Passport type, use the Make Configuration Data File (MCDF) utility. For details see 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Passport nodes also have a label beneath the icon. Passport switches display on the Nortel Networks submap as EM/<device\_name>. For example: EM/EMDEV1

Passport 4400 access device names display on the Nortel Networks submap as MPA /<device\_name>. For example: MPA/MPADEV1

### DPN devices

DPN nodes are depicted by an icon that contains a D or O.

The label for DPN switches display on the Nortel Networks submap as follows, depending on the type of DPN device:

- DPN-100 device names display as  
PM/<device\_name>, for example: PM/PMDEV1
- Passport 4120 device names display as  
PM/<device\_name>, for example: PM/PM/DEV2
- Operating Agents on DPN-100, Passport 4120, or Passport 4400 with LDM cards display as  
OA/<agent\_name>, for example OA/AGENT3

There is no subcomponent submap for DPN devices. To see a list of the subcomponents and their states, use the Component Information Viewer.



## Procedures

This section contains the following procedures to start the HP OpenView Network Node Manager (NNM) application and to access a selection of MDM tools from that application.

### **Starting and stopping the HP OpenView NNM tool**

- “Starting HP OpenView NNM from the MDM toolset” (page 524)
- “Starting HP OpenView NNM from the UNIX command line” (page 525)
- “Quitting HP OpenView NNM” (page 526)

### **Displaying online information**

- “Displaying online documentation” (page 527)
- “Displaying alarm help” (page 528)

### **Starting MDM tools from HP OpenView**

- “Starting MDM Passport tools from the menu bar” (page 529)
- “Starting MDM Passport tools from the node pop-up menu” (page 532)
- “Starting MDM DPN tools from the menu bar” (page 533)
- “Starting MDM DPN tools from the node pop-up menu” (page 535)

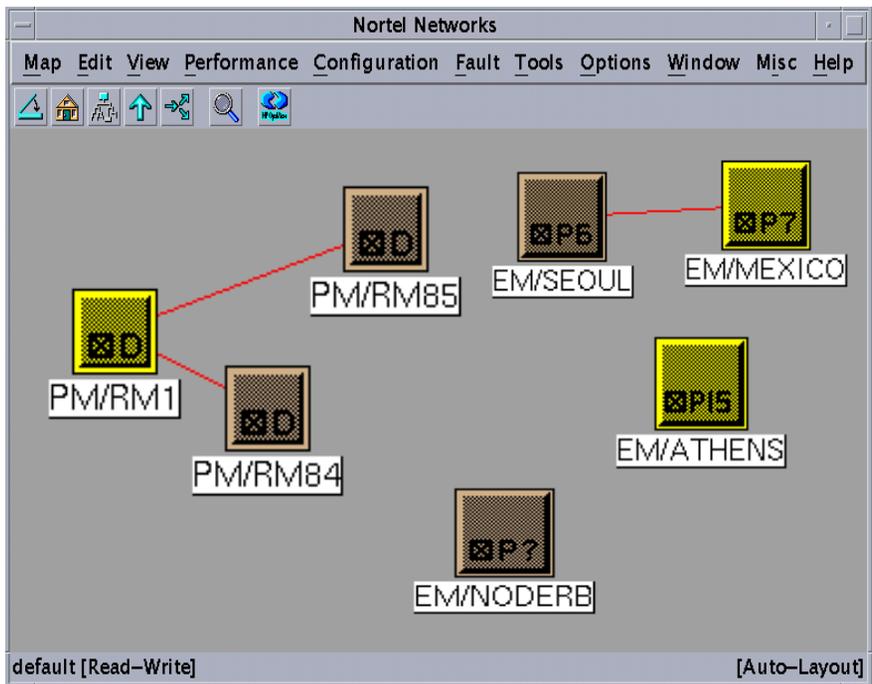
## Starting HP OpenView NNM from the MDM toolset

Start HP OpenView NNM desktop to access the HP OpenView platform.

### Procedure step

- 1 In the Preside MDM window, select **Fault**, **HP OpenView NNM**, and **Network Node Manager**.

The HP OpenView NNM desktop opens.



## Starting HP OpenView NNM from the UNIX command line

Start HP OpenView NNM desktop to access the HP OpenView platform.

### Procedure steps

- 1 In a UNIX window start HP OpenView:

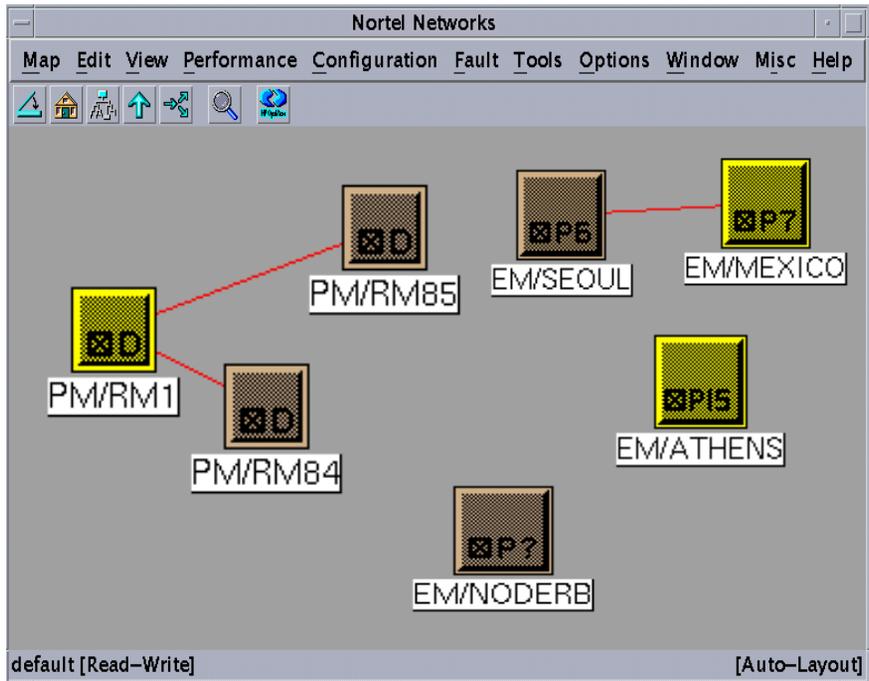
```
/opt/OV/bin/ovw &
```

The About HP OpenView window opens. To close the window, click **Close** or wait for the window to close on its own.

The Alarm Categories window opens. It may display a status message at the bottom, stating the percentage of the trapd.log file that has been loaded.

- 2 To view your network on the Root map, double-click the Nortel Networks symbol.

The Nortel Networks submap opens and displays the network devices.



## Quitting HP OpenView NNM

Use this procedure to quit the HP OpenView NNM application.

### Procedure step

- 1 From the **Map** menu, select **Exit**.

An OpenView Windows Warning dialog opens.

- 2 To exit, click **OK**.

The dialog closes along with the Event Categories window and any open submaps.

## Displaying online documentation

Display online documentation to access MDM and MDP documentation.

### Procedure steps

- 1** From the Root map Help menu or any submap Help menu, select Online Documentation.  
The Netscape browser opens with online documentation.
- 2** In the left pane of the browser, select the MDM or MDP document suite.  
The left pane displays the documentation categories.
- 3** In the left pane, select a document name.  
A table of contents appears. You can now select a topic from the document.
- 4** In the left pane, select the topic you want to view.  
The topic details display in the right frame.

## Displaying alarm help

To view help information for Passport alarms from the HP OpenView NNM desktop, first you need to start the Alarm Help tool from the Preside MDM window. Starting Alarm Help in this manner opens the Netscape browser required for online help. As long as the Netscape Alarm Help window is open, you can request Passport alarm help.

- 1 In the Preside MDM window, select System -> Utilities -> Online Documentation.

The Alarm Help tool opens in a Netscape window.

- 2 On the OpenView submap, select the nodes for which you want alarm help.

- 3 From the Fault menu, select Alarm.

The All Alarms Browser window opens with a list of alarms for the selected nodes.

- 4 From the list of alarms, select one for which you want detail information.

- 5 From the Actions menu, select Additional Actions.

The Additional Actions on All Alarms dialog opens.

- 6 From the Action list, select Help for Passport Alarms.

- 7 Click the OK button.

The Netscape browser window displays the alarm help for the requested alarm

## Starting MDM Passport tools from the menu bar

You can start a selection of MDM Passport tools from HP OpenView NNM menu bar. The table “MDM Passport tools that you can start from HP OpenView NNM” (page 529) provides a list of MDM tools that you can start from HP OpenView and the associated documentation for those tools.

### Procedure steps

- 1 On the OpenView submap, click a Passport node to select it.
- 2 From the **Performance, Configuration, Fault, or Miscellaneous** menu, choose the MDM Passport tool that you want to start.

**Table 68**

**MDM Passport tools that you can start from HP OpenView NNM**

MDM tools	For more information, see...
Performance tools:	
Passport Data Viewer	241-6001-031 <i>Preside MDM Performance Management User Guide</i>
Configuration tools:	
Nodal Provisioning	241-6001-610 <i>Preside MDM Nodal Provisioning User Guide</i>
Software Distribution and Configuration	241-6001-023 <i>Preside MDM Configuration Management for Passport User Guide</i>
Service Integrity Simplification	241-6001-022 <i>Preside MDM Network Reporting System User Guide</i>
Network Activation	241-6001-023 <i>Preside MDM Configuration Management for Passport User Guide</i>
Passport/SNMP Devices Backup and Restore	241-6001-807 <i>Preside MDM Passport/SNMP Devices Backup and Restore User Guide</i>
Fault tools:	
Alarm Display	241-6001-011 <i>Preside MDM Fault Management User Guide</i>
(Sheet 1 of 2)	

**Table 68 (continued)**  
**MDM Passport tools that you can start from HP OpenView NNM**

<b>MDM tools</b>	<b>For more information, see...</b>
Component Information Viewer	241-6001-011 <i>Preside MDM Fault Management User Guide</i>
Component Status Display	241-6001-011 <i>Preside MDM Fault Management User Guide</i>
Network Status Bar	241-6001-011 <i>Preside MDM Fault Management User Guide</i>
Passport Shelf View	241-6001-011 <i>Preside MDM Fault Management User Guide</i>
Miscellaneous utilities:	
Command Console	241-6001-804 <i>Preside MDM Workstation Utilities User Guide</i>
Customer Database	241-6001-804 <i>Preside MDM Workstation Utilities User Guide</i>

(Sheet 2 of 2)



## Starting MDM Passport tools from the node pop-up menu

You can start MDM Passport tools from a node's pop-up menu.

### Procedure steps

- 1 On the OpenView submap, right-click a Passport node to select it.  
The node pop-up menu opens.
- 2 From the node pop-up menu, select one of the following MDM tools:
  - a Passport Configuration tool
  - a Passport Fault tool
  - Data Viewer
  - Command Console
  - Customer Database

## Starting MDM DPN tools from the menu bar

You can start a selection of MDM DPN tools from HP OpenView NNM menu bar. The table “MDM DPN tools that you can start from HP OpenView NNM” (page 533) provides a list of MDM DPN tools that you can start from HP OpenView and the associated documentation for those tools.

### Procedure steps

- 1 On the OpenView submap, click to select a node.
- 2 From the **Performance, Configuration, Fault,** or Miscellaneous menu, choose the MDM Passport tool that you want to start.

**Table 69**

**MDM DPN tools that you can start from HP OpenView NNM**

MDM tools	For more information, see...
Performance tools:	
DPN Performance Viewer	241-6001-031 <i>Preside MDM Performance Management User Guide</i>
Configuration tools:	
Component Provisioning	241-6001-012 <i>Preside MDM Configuration Management for DPN User Guide</i>
Service Data Backup	241-6001-012 <i>Preside MDM Configuration Management for DPN User Guide</i>
Service Data Restore	241-6001-012 <i>Preside MDM Configuration Management for DPN User Guide</i>
Global Data Manager	241-6001-012 <i>Preside MDM Configuration Management for DPN User Guide</i>
Software Distribution	241-6001-012 <i>Preside MDM Configuration Management for DPN User Guide</i>
(Sheet 1 of 2)	

**Table 69 (continued)**  
**MDM DPN tools that you can start from HP OpenView NNM**

<b>MDM tools</b>	<b>For more information, see...</b>
Software Substitution	241-6001-012 <i>Preside MDM Configuration Management for DPN User Guide</i>
Envelope Editor	241-6001-012 <i>Preside MDM Configuration Management for DPN User Guide</i>
Service Data Conversion	241-6001-012 <i>Preside MDM Configuration Management for DPN User Guide</i>
Network Activation	241-6001-012 <i>Preside MDM Configuration Management for DPN User Guide</i>
Service Integrity Simplification	241-6001-022 <i>Preside MDM Network Reporting System User Guide</i>
DPN Fault tools:	
Alarm Display	241-6001-011 <i>Preside MDM Fault Management User Guide</i>
Component Information Viewer	241-6001-011 <i>Preside MDM Fault Management User Guide</i>
Component Status Display	241-6001-011 <i>Preside MDM Fault Management User Guide</i>
Network Status Bar	241-6001-011 <i>Preside MDM Fault Management User Guide</i>
Miscellaneous utilities:	
Command Console	241-6001-804 <i>Preside MDM Workstation Utilities User Guide</i>
Customer Database	241-6001-804 <i>Preside MDM Workstation Utilities User Guide</i>
(Sheet 2 of 2)	

## Starting MDM DPN tools from the node pop-up menu

You can start MDM DPN tools from a node's pop-up menu.

### Procedure steps

- 1 On the OpenView submap, right-click a DPN node to select it.  
The node pop-up menu opens.
- 2 From node pop-up menu, select one of the following MDM tools:
  - a DPN Configuration tool
  - Command Console
  - Customer Database
  - a DPN Fault tool
  - DPN Performance Viewer



---

## Appendix A

# LPDA-2 modem management

---

This appendix describes how you can manage LPDA-2 modems with Preside Multiservice Data Manager (MDM). It explains:

- what the LPDA-2 macros are
- how to use the LPDA-2 macros
- how to update the LPDA-2 macro configuration file

The macros described in this appendix can only be used with modems that support LPDA-2.

### About LPDA-2 commands

LPDA-2 is a protocol that allows diagnostic commands to be sent to modems that support this protocol. You can send LPDA-2 commands using the macro facility of the Command Console. Each macro sends an LPDA-2 command to a modem at a specified port and displays the results of the command in the Command Console utility. For details about the Command Console utility, see 241-6001-804 *Preside MDM Workstation Utilities User Guide*.

The results displayed by the macros include comments on the values being displayed. When it is appropriate, a rating is displayed beside the value received from the modem. For example, the line quality received by the modem can be rated as good, fair, poor, or bad.

The values to which these ratings apply are set in the LPDA configuration file. You can edit this file to customize the display printed by the macros in the Command Console.

### **Modem self-test macro - LPDASLF**

The modem self-test macro sends a command to a modem to perform a series of self-tests. These tests are performed by both local and remote modems. The modem reports the results of these tests and displays them in the Command Console.

### **Modem and line status macro - LPDAMST**

The modem and line status macro sends a command to the modem to report the results of the last self-test performed. The modem reports the results of these tests and displays them in the Command Console.

### **Modem transmit/receive test macro - LPDATRR**

The modem transmit/receive test macro sends a command to the modem that causes the local and remote modems to exchange test sequences. The number of times the modems exchange these sequences is supplied by the operator.

## **Using LPDA-2 macros**

You need to start all macros from the Command Console. Before you can send an LPDA-2 command to a modem, you need to disable the port to which it is attached. You can disable the port from the Command Console using the AM/RM DISABLE command. For details on the command, see *241-1001-303 DPN-100 Operator Commands and Responses - Volume 4*.

#### **Example**

```
RAAS-11 5 2 DISABLE
```

disables port 2 on PE 5 of the RAAS-11 access module.

The length of time the macros can run is limited. If no response is received before the time limit is reached, the macro times out and reports the problem.

You can start all macros that run from the Command Console by using \$ in front of the macro name.

### **Running the LPDASLF macro**

To run the LPDASLF macro, enter the command LPDASLF followed by the routing information that identifies the port being tested.

**Example**

```
$LPDASLF RAAS-11 5 2
```

The test takes a maximum of one minute, the results are displayed in the Command Console window.

**Running the LPDAMST macro**

To run the LPDAMST macro enter the command LPDAMST followed by the routing information that identifies the port being tested.

**Example**

```
$LPDAMST RAAS-11 5 2
```

The test takes a maximum of one minute; the results are displayed in the Command Console window.

**Running the LPDATRR macro**

To run the LPDATRR macro, enter the command LPDATRR followed by the number of test sequences the modems are to exchange, and the routing information that identifies the port being tested.

**Example**

```
$LPDATRR 6 RAAS-11 5 2
```

Here the modems exchange six test sequences and then report the results.

The maximum number of times that the modems can exchange test sequences is ten and the minimum is one. You need to provide a value for the number of exchanges before the routing information.

The time taken to complete the test depends on the number of test sequence exchanges requested. The maximum time for the test is 60 minutes; the results are displayed in the Command Console.

## Updating the LPDA-2 configuration file

The file *lpda.cfg* contains information used by the macros to display the results received from the modem. A copy of this file is in the */opt/MagellanNMS/cfg/macros/nms* directory. You can use this file to change the behavior of the LPDA-2 macros when you

- change the ranges of values that are used to judge the performance of the modem
- change the language in the report printed from the modem
- extend the modem models recognized by the macros

You need to put replacement versions of this file in the Preside Multiservice Data Manager (MDM) user's *\$HOME/MagellanNMS* directory. The macros search this directory for the configuration file before going to the */opt/MagellanNMS/cfg/macros/nms* directory.

If a problem occurs in the user's copy of the configuration file, the error is reported, and the */opt/MagellanNMS/cfg/macros/nms* version is used. If the macros fail to find a valid configuration file, they will print a warning and use a set of default values.

Detailed instructions for altering the configuration file are contained in the file.

## Appendix B

# Common alarm format

The table “Common alarm format” (page 541) describes the Common alarm format parameters.

**Table 70**  
**Common alarm format**

Parameter	Semantics
alarmType	Indicates the type of event (for example, equipmentAlarm, CommunicationsAlarm). This attribute is equivalent to the OSI <b>alarmType</b> parameter.
severity	Indicates the severity of the alarm. This attribute is equivalent to the OSI <b>perceivedSeverity</b> parameter.
probableCause	Standardized cause for the event. This attribute is equivalent to the OSI <b>probableCause</b> parameter.
notificationID	Provides an identifier for the alarm. It may be used by the <b>correlatedNotifications</b> parameter of subsequent alarms.
rawState	The DPN raw state.
commentData	Provides a free form text description of the event.
operatorData	A HEX string specifying operator data.
expertData	A HEX string specifying expert data.
event	An integer specifying the alarm type as being a message, a set, or a clear.
fault codex	A code used to obtain further information concerning the error causing the alarm.
(Sheet 1 of 2)	

**Table 70 (continued)**  
**Common alarm format**

<b>Parameter</b>	<b>Semantics</b>
relatedComponentName	The names of components related to the component originating the alarm.
correlatedNotifications	Identifies alarms that are related to this alarm.
fileNameInformation	Information allowing the determination of the location in source of the alarm generating code.
administrativeState	This attribute is equivalent to the OSI <b>administrativeState</b> parameter.
operationalState	This attribute is equivalent to the OSI <b>operationalState</b> parameter.
usageState	This attribute is equivalent to the OSI <b>usageState</b> parameter.
proceduralStatus	This attribute is equivalent to the OSI <b>proceduralStatus</b> parameter.
availabilityStatus	This attribute is equivalent to the OSI <b>availabilityStatus</b> parameter.
unknownStatus	This attribute is equivalent to the OSI <b>unknownStatus</b> parameter.
(Sheet 2 of 2)	

---

## Index

---

### A

acknowledged state 400, 401  
     putting component into 47, 80, 420  
     taking component out of 81  
 Add/Edit button 269  
 adding alarm codes 271  
 alarm code, adding 271  
 alarm code, editing 271  
 alarm code, searching for 270  
 Alarm Display 34, 222  
     command line arguments 264  
 Alarm Help, buttons 268  
 Alarm Help, documents 268  
 Alarms  
     deleting 48  
     viewing AD alarm files 259  
 Auto Refresh  
     in Alarm Display 240

### C

Cluster and pin 68  
 Command Console 38  
 component filtering 405, 407–408, 410–411  
     changing settings of 421–422  
 Component Information Viewer 36  
     deleting active alarms 229  
 component status 399  
 Component Status Display 37, 397–427  
     choosing an organization 419  
     component filtering 405, 407–408, 410–

411

    changing settings of 421–422  
     component status 399  
     components panel 404–407  
     customizing 425–427  
     error & warning messages 415–417  
     exiting 422  
     keyboard shortcuts 409  
     setting preferences 411–414, 423–425  
     starting 418  
     warning & error messages 415–417  
 components panel 404–407  
 context 56, 405  
     commands 38  
 Customizing  
     Alarm Display Start Tool submenus 256  
     Component Information Viewer Related  
         Components list tools menu 299  
     other resources 262

### D

Deleting an alarm from Alarm Display 229  
 direct discovery 436, 459  
 DPN context 56

### E

editing alarm codes 271

### F

Filtering

- alarms 245
- changing filters 250
- defining filters 245
- saving filters 253
- setting component filter parameters 93
- filtering
  - components 405, 410–411
- filtering components 407–408
- Filters
  - applying filters 251
  - changing filters in Alarm Display 250
  - using previously saved filters 96
- filters
  - changing component filter settings 421–422

## H

- hierarchical maintenance state 400
- hierarchical out-of-service state 400

## I

- in-service states 399, 400
- in-service—troubled 399, 400
- in-service—troubled state 399, 400
- IP Discovery 429–461
  - adding an address 442
  - changing a password 434
  - changing network settings 444
  - creating network settings 443
  - deleting devices 438
  - deleting network settings 445
  - direct discovery 436, 459
  - displaying devices 450
  - failure of a discovery 460
  - location of logs 461
  - moving rows 446
  - process 454
  - route-based discovery 437, 459
  - setting a password 432, 435
  - sorting devices 451
  - starting in insecure mode 431

- starting in secure mode 433
- updating devices 440, 441

## K

- keyboard shortcuts
  - Component Status Display 409

## L

- LPDA-2
  - commands 537
  - LPDAMST 539
  - LPDASLF 538
  - LPDATRR 539
  - updating configuration file 540
- LPDA-2 macros 537
- LPDAMST 538
  - running 539
- LPDASLF 538
  - running 538
- LPDATRR 538
  - running 539

## M

- Macros
  - LPDA-2 537
- maintenance state
  - putting component into 420–421
- maintenance states 400
- Modem and line status macro -
  - LPDAMST 538
- Modem management 537
- Modem self test macro - LPDASLF 538
- Modem transmit - receive test macro -
  - LPDATRR 538

## N

- Network Status Bar 35
- Network Viewer 33, 51
  - displaying component state 78
  - displaying links 69
  - displaying nodes 63

---

- displaying shelf views 72
- organization navigation 85
- Node positioning 67

## O

- out-of-service state 399, 400

## P

- Passwords

- changing for IP Discovery 434
  - setting for IP Discovery 432, 435

- Problems

- fixing 49

- propagated states 399

## R

- raw states 399

- Reset button 268

- route-based discovery 437, 459

## S

- Search Alarm button 269

- Search Text button 269

- Setting the Network Viewer preferences 93

- starting Alarm Help 269

- Starting Component Information Viewer

- from Alarm Display 258

- states 399, 400

- acknowledged 400, 401

- putting component into 47, 420

- hierarchical maintenance 400

- hierarchical out-of-service 400

- in-service 399, 400

- maintenance 400

- putting component into 420–421

- out-of-service 399, 400

- propagated 399

- raw 399

- unknown 399, 400

- Surveillance tasks

- putting component into acknowledged

- state 80

- surveillance tasks

- acknowledging an alarm 48

- changing NV display 49

- clearing an alarm 48

- determining a problem 45

- fault correction 49

- finding troubled components 41

- monitoring selected components 43

- putting component into acknowledged

- state 47

- putting component into maintenance 47

- unacknowledging an alarm 48

## T

- text entry field 269

- text string, searching for 270

- Troubleshooting

- in Network Viewer 113

## U

- unknown state 399, 400

## V

- viewing an alarm code from Alarm

- Display 271





Preside Multiservice Data Manager  
**Fault Management**  
User Guide

R14.3

Copyright © 2003 Nortel Networks.  
All Rights Reserved.

NORTEL, NORTEL NETWORKS, the globemark design, the NORTEL NETWORKS corporate logo, PRESIDE, DPN, and PASSPORT are trademarks of Nortel Networks. SUN and SUNLINK are trademarks of Sun Microsystems Inc. SPARCSTATION is a trademark of Sparc International Inc. UNIX is a trademark licensed exclusively through X/Open Company Ltd..

Publication: 241-6001-011  
Document status: Standard  
Document version: 14.3RSUP  
Document date: December 2003  
Printed in Canada

