NORTEL NETWORKS

Preside Multiservice Data Manager

Administrator Guide

241-6001-303

Preside Multiservice Data Manager

Administrator Guide

Publication: 241-6001-303
Document status: Standard
Document version: 15.1RSUP
Document date: August 2004

Printed in Canada

Publication history

August 2004

15.1RSUP Standard
Commercial availability exept for MPE support which will be available ina future release.

Contents

About this document

The following topics are discussed in this section:

Who should read this document and why

This document contains reference and procedural information about the administrative tasks required to support Preside Multiservice Data Manager software and the workstation on which it runs.

This document is aimed at system administrators who specialize in managing networks.

What you need to know

Users of this document require the following knowledge and skills:

- working knowledge of UNIX and the Solaris operating environment
- knowledge of Nortel Networks products and deployment, and the Preside Multiservice Data Manager and its graphical user interface
- working experience or training in the administration of Sun workstations
- working experience or training in the installation, configuration, and troubleshooting of SunLink X.25, and Frame Relay software products

How this document is organized

241-6001-303 *Preside MDM Administrator Guide* contains the following sections:

- "Administration task areas" (page 33) explains what is meant by Administration as it applies to Preside Multiservice Data Manager (MDM) and points you to guidelines and information sources for performing various administrative tasks.
- "MDM Run Time Environment" (page 41) describes the run-time environment and the file and directory structure for MDM software.
- "Setting up UNIX accounts for MDM" (page 55) contains the instructions for creating new UNIX accounts and modifying existing UNIX accounts to run the MDM software. This includes the root account.
- "Software licensing" (page 69) contains information on deleting and querying licenses.
- "Starting and ending MDM sessions" (page 75) contains the information required to start MDM sessions.
- "Roadmap to the MDM servers" (page 81) lists all of the MDM servers that can be set up in networks that contain Nortel Networks devices, summarizes the purpose of each server, and provides references to instructions for configuring the servers.
- "Configuring servers for DPN switches" (page 93) contains the instructions to configure the servers on a workstation so that it supports network access, surveillance access, and provisioning access for DPN switches.
- "Configuring MDM servers for Passport switches" (page 123) contains the instructions to configure the servers on a workstation so that it supports network access, surveillance access, and provisioning access for Passport switches.
- "Configuring MDM servers for MPE switches" (page 167) contains the instructions to configure the Preside Multiservice Data Manager (MDM) servers to support network access, surveillance access, and provisioning access for Nortel Networks Multiservice Provider Edge (MPE) switches

- "Configuring network access data mediation" (page 211) contains guidelines and instructions for configuring the Network Data Access Mediation (NDAM) server to provide filtered surveillance information to clients such as HP OpenView NNM desktop and to the fault tools.
- "Configuring Multi-nodal Naming Service domains" (page 223) explains the purpose of a Multi-nodal Naming Service (MNS) domain and contains guidelines and instructions for configuring MNS domains.
- "Configuring Multi-nodal Naming Service TCP/UDP port mappings" (page 231) explains the purpose of configuring Multi-nodal Naming Service (MNS) TCP/UDP port mappings.
- "Configuring DPN alarm clearing" (page 233) contains instructions to set up set up alarm clearing on a workstation to allow operators to clear DPN alarms locally on the workstation and to clear DPN alarms globally throughout the network.
- "Configuring server alarm distribution and workstation status probing" (page 261) contains instructions to set up the workstation to do the following:
  - provide workstation server alarms to other workstations through a GMDR server
  - provide workstation server alarms to the Network Control system (NCS) that runs on the DPN switches in your network
  - set up the NCS so that it probes the workstation to determine the workstation's status
- "Configuring workstation surveillance" (page 271) provides information on configuring monitoring thresholds and connectivity logs.
- "Configuring the Disruptive Command Safeguard" (page 277) provides the instructions required to set up the Disruptive Command Safeguard feature. This feature only applies to DPN switches.
- "Synchronizing the network time" (page 283) describes how the Network Time Synchronization feature applies to MDM and contains procedures for setting it up.
- "Configuring remote access" (page 339) contains instructions to set up the Remote Access tool.

- "Configuring automatic DBNL disabling" (page 343) describes the automatic Dial Backup Network Link (DBNL) disabling feature, and contains instructions for configuring the feature and cleaning up any accumulated log files the feature produces.
- "Using the Server Administration tool" (page 359) explains the purpose of the Server Administration tool, provides instructions for using the tool, and for cleaning up log files associated with the Server Administration process.
- "The svmcmd utility" (page 419) provides information on a utility that provides a command line interface with similar functionality to the Server Administration tool.
- "Using the GMDR Administration tool" (page 423) describes the GMDR Administration tool and provides instructions for using the tool to perform administrative tasks.
- "Using the Service Selection tool" (page 467) explains the purpose of the Service Selection tool, and provides procedures for using the Service Selection tool in the MDM Toolset and Operator Client environments.
- "Using the System Log Display tool" (page 499) explains the purpose of the System Log Display tool and provides instructions for using the tool.
- "Managing Passport SDD files" (page 507) contains the instructions to install Passport Service Data Description (SDD) files.
- "Configuring shared memory" (page 517) contains instructions to re-configure the kernel of the Solaris operating system so that it makes sufficient shared memory available to support the Network Models and the Passport Communications Manager (FDTM).
- "Using the Auto-Patch tool" (page 529) describes the purpose of the Auto-Patch tool for Passport nodes and provides the command syntax to control the auto-patching process.
- "MDM log files" (page 539) describes the log files generated by the MDM tools and the logs stored in them.
- "Configuring the OA groups with the oa.config program" (page 557) describes how to configure OA groups using the oa.config tool.

- "Defining Passport hosts and groups with the passport.config script" (page 563) describes how to configure Passport hosts and groups using the passport.config too.l
- "Configuring maximum heap size for shared JVM" (page 523) explains what to do if a dialog opens on your PC indicating that you have run out of shared memory for Java based tools.

What's new in this document

The following feature information was added to this document:

- "MDM OAM and Security Audit Logging" (page 29).
- "MDM Operator Client" (page 29)
- "MDM Auto-Patching for Passport" (page 29)
- "SNMP Proxy Agent (SPA) on MPE 9500" (page 30)

MDM OAM and Security Audit Logging

This feature includes enhancements to the following section:

- "Using the Server Administration tool" (page 359)

MDM Operator Client

The following modifications were made:

- enhancements to "Using the Service Selection tool" (page 467).
- removal of the chapter "Using the Nodal Provisioning Administration tool"

MDM Auto-Patching for Passport

This feature includes a new section:

- "Using the Auto-Patch tool" (page 529).

SNMP Proxy Agent (SPA) on MPE 9500

The SNMP Proxy Agent (SPA) is available on the Nortel Networks Multiservice Provider Edge 9500 (MPE 9500) device. SPA provides a single point of SNMP access to several MPE 9500 devices through an MDM server.The following sections were modified:

- "SNMP proxy agent (SPA) configuration" (page 193)
- "SNMP Proxy Agent (SPA) fundamentals" (page 207)
- "Types of servers" (page 369)

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

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

- |

  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 of 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 /).

Related documents

See the following documents for related information:

- 241-6001-011 *Preside MDM Fault Management User Guide*
- 241-6001-013 *Preside MDM Remote Network Communication System User Guide*
- 241-6001-015 *Preside MDM Network Model Administrator Guide*
- 241-6001-022 *Preside MDM Network Reporting System User Guide*
- 241-6001-100 *Preside MDM Installation*
- 241-6001-101 *Preside MDM Engineering Guide*
- 241-6001-118 *Preside MDM SNMP Surveillance Adapter Guide*
- 241-6001-200 *Preside MDM Application Programming Interface Primer*
- 241-6001-201 *Preside MDM Network Model API Reference Guide*

- 241-6001-203 *Preside MDM Alarm and Status API Reference Guide*
- 241-6001-204 *Preside MDM DPN Provisioning API Reference Guide*
- 241-6001-207 *Preside MDM Passport Provisioning API Reference Guide*
- 241-6001-301 *Preside MDM Customization Administrator Guide*
- 241-6001-304 *Preside MDM Configuration Management for DPN Administration*
- 241-6001-308 *Preside MDM Network Configuration Database for DPN Administrator Guide*
- 241-6001-310 *Preside MDM Server Reference Guide*
- 241-6001-804 *Preside MDM Workstation Utilities User Guide*
- NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*
- NN10600-605 *Passport - MDM Network Security: Operations*

A number of SunSoft applications publications are available, which may prove useful for Administrators. Copies of these documents can be obtained by contacting Sun Microsystems at the following address:

Sun MicroSystems Inc.
2550 Garcia Avenue,
Mountain View,
CA 94043
United States of America

The SunSoft applications publications are as follows:

- *SunSPARCstation Installation Manual*
- *Solaris Advanced Installation Guide*
- *SunLink HSI/P x.x User's Guide*
- *Managing SunLink X.25 9.x*

Chapter 1
Administration task areas

This section explains how administration applies to Preside Multiservice Data Manager (MDM) and gives you guidelines and information sources for performing various administrative tasks.

For more information, see the following:

- "MDM administration" (page 33)
- "Where to find administration information" (page 35)
- "Administration information in this document" (page 36)

MDM administration

Preside Multiservice Data Manager (MDM) administration includes many tasks that must be performed at different stages while using MDM software. The following list describes the main tasks for administering MDM, along with some examples. This list is not exhaustive, but it provides an understanding of the MDM administration.

- Planning and Engineering tasks including
  - — determining the workstation hardware configuration to run MDM
  - — determining X.25 and Frame Relay link requirements to handle messaging between the workstation and nodes in the network
  - — monitoring the performance of MDM tools on the workstation
  - — planning re-configuration of links or workstations to improve the performance of MDM tools, to support expansion in the number of

network elements monitored, or to support an increase in the number of MDM users

- Installation tasks including:
  - — installing and configuring the Solaris operating system, including the Common Desktop Environment (CDE) window manager
  - — installing, configuring, and troubleshooting Sun's communication applications software including: HSI, SunLink X.25, SunLink Frame Relay
  - — installing and configuring MDM software and licences by using the MDM Software Configuration tool
- Configuration maintenance tasks including
  - — creating new MDM user accounts
  - — adding MDM feature sets to an existing installation
  - — upgrading the amount of shared memory to respond to increases in the size of the Network Models and Service Data Descriptions (SDDs)
  - — installing patches and new releases of MDM software (RSUPs)
- Server administration tasks. MDM software is based on a set of servers that can run on one workstation or can be distributed over a number of workstations. Some servers are used to support communications to the network, and others provide information and services to MDM tools. Server administration tasks include configuring, and maintaining these servers.
- Customization tasks. Some aspects of MDM tools and menus can be customized, such as the items displayed in the main window and the menu items that appear in a start tools menu. Customers may write their own cmcmd or snmpCmd macros.
- Special MDM software administration tasks. Some optional MDM systems such as the Management Data Provider and the Network Model require special configuration and configuration maintenance.

To perform these tasks, an administrator must have a working knowledge of MDM products.

Installation tasks involve the use of Sun's Solaris operating system, NFS, and Sun's SunLink X.25 and Frame Relay software. All MDM administrators should have

- working experience in the administration of Sun workstations, or that they take the workstation administration course offered by Sun Microsystems Inc.
- working experience or training in the installation, configuration, and troubleshooting of SunLink X.25, and Frame Relay software products.

Where to find administration information

This document provides information to administer Preside Multiservice Data Manager (MDM). Several other documents contain information about administration tasks.

- Planning and Engineering tasks. For more information, see 241-6001-101 *Preside MDM Engineering Guide*
- Installation tasks. For more information, see 241-6001-100 *Preside MDM Installation*.
- Customization tasks. For more information, see 241-6001-301 *Preside MDM Customization Administrator Guide*.
- Configuration maintenance tasks and server administration tasks. Information about these tasks is contained in this document. For a breakdown of the information, see "Tasks for configuring MDM" (page 36).
- Special MDM software administration tasks. Information about performing special administration on optional MDM systems is contained in a number of Nortel Networks technical publications (NTPs).
  - MDM Configuration, see 241-6001-304 *Preside MDM Configuration Management for DPN Administration*
  - Network Model, see 241-6001-015 *Preside MDM Network Model Administrator Guide*
  - Management Data Provider, see 241-6001-309 *Preside MDM Management Data Provider User Guide*

— Network Configuration Database, see 241-6001-308 *Preside MDM Network Configuration Database for DPN Administrator Guide*

— DPN SNMP Agent, 241-6001-210 *Preside MDM DPN SNMP Agent User Guide*

Administration information in this document

This document contains information about configuration maintenance tasks and server administration tasks for Preside Multiservice Data Manager (MDM). The information falls into three main categories:

- "Tasks for configuring MDM" (page 36)
- "Administration reference information" (page 37)
- "Administration tools available in an MDM session" (page 37)

Tasks for configuring MDM

For information on procedures for configuring Preside Multiservice Data Manager (MDM), see

- "Frequently performed administrative tasks" (page 36)
- "Infrequently performed administrative tasks" (page 37)

Frequently performed administrative tasks

For information about tasks that are performed frequently by most administrators, see

- "Setting up UNIX accounts for MDM" (page 55)
- "Configuring servers for DPN switches" (page 93) (See note)
- "Configuring MDM servers for Passport switches" (page 123) (See note)
- "Configuring Multi-nodal Naming Service domains" (page 223) (See note)
- "Configuring DPN alarm clearing" (page 233) (See note)
- "Configuring server alarm distribution and workstation status probing" (page 261) (See note)
- "Configuring the Disruptive Command Safeguard" (page 277) (See note)

- "Synchronizing the network time" (page 283) (See note)
- "Configuring remote access" (page 339)
- "Configuring automatic DBNL disabling" (page 343)

Note: For initial installation only, these tasks can be performed by using the MDM Software Configuration tool. To configure the MDM software, see 241-6001-100 *Preside MDM Installation*.

Infrequently performed administrative tasks

For information about infrequently performed tasks that deal with advanced administration topics, see

- "Configuring shared memory" (page 517)
- "Managing Passport SDD files" (page 507)
- 241-6001-310 *Preside MDM Server Reference Guide* to configure circuit monitoring

Administration reference information

For reference information about Preside Multiservice Data Manager (MDM) topics, see

- "MDM Run Time Environment" (page 41)
- "Roadmap to the MDM servers" (page 81)
- "MDM log files" (page 539)
- 241-6001-310 *Preside MDM Server Reference Guide*

Administration tools available in an MDM session

From the Preside Multiservice Data Manager (MDM) main window Administration menu, you can access a variety of administration tools.

See the following information:

- "MDM Administration" (page 38)
- "MDM Security" (page 39)

MDM Administration

Preside Multiservice Data Manager (MDM) administration tools let you perform administration tasks on MDM software when it has been installed and configured by a system administrator.

- MDM Software Configuration
  lets root users perform basic configuration on MDM software at initial installation only. This menu is only displayed if you are logged in as root.

  For information about the MDM Software Configuration tool, see 241-6001-100 *Preside MDM Installation*.

- Server Administration
  lets you monitor and control the MDM servers

  See “Using the Server Administration tool” (page 359).

- Service Selection
  at a workstation that is running a Client Set of processes, you can choose the Server Set of processes for the Client Set to use for one of the following service areas: Surveillance, Network Model, DPN Configuration, DPN Network Access, Passport Network Access, and ALL.

  See “Using the Service Selection tool” (page 467)

- GMDR Administration lets you
  - configure a GMDR server to collect surveillance data
  - monitor connections between the GMDR server and the surveillance servers
  - view and reset a GMDR database that contains statistics gathered by the GMDR server
  - view logs about changes in the states of connections to the surveillance servers and about database resets

See “Using the GMDR Administration tool” (page 423).

- Nodal Provisioning Template Editor
  lets you create and modify service templates using a graphical interface.

  See 241-6001-610 *Preside MDM Nodal Provisioning User Guide*.

- Circuit Database Administration
  lets you manage objects in the Administration Database

  See 241-6001-400 *Preside MDM Administration Database User Guide*.

- System Log Display lets you
  display and print logs produced by MDM servers and by the action of MDM tools

  See “Using the System Log Display tool” (page 499).

MDM Security

The Disruptive Command Safeguard tool is for System Administrators who install and configure MDM software. Disruptive Command Safeguard is a command input management facility that intercepts potentially disruptive DPN commands entered from an MDM workstation, and presents a confirm or cancel message to the operator.

See “Configuring the Disruptive Command Safeguard” (page 277)

Chapter 2
MDM Run Time Environment

This section describes the run-time environment and the file and directory structure for Preside Multiservice Data Manager (MDM) software.

See the following topics for more information:

MDM User Environment

Preside Multiservice Data Manager (MDM) software stores its executables in separate directories from the workstation's MDM data and configuration files, and from the Nortel Networks technical publications (NTPs) for MDM. This arrangement provides the following advantages:

- simplifies backup and restore operations
- provides an efficient means of performing software upgrades and release rollbacks
- makes it easy to use NFS to deploy MDM software among workstations on a LAN

For a description of the directory structure, see “Directory structure” (page 42).

MDM software includes a set of skeleton files which you can copy into your home directory. When copied, these skeleton files automatically set up environment variables for MDM, start an MDM session, and open the MDM main window. For a description of these files, see “Default MDM user environment skeleton files” (page 47).

For some existing accounts such as root, it is not always desirable to copy the skeleton files into the account’s home directory. An example of this is when the root account is used to manage workstations other than those used to run MDM software. MDM software includes scripts that you can run from a command line or invoke in the set-up files of the existing account to set up the variables and start a session. For descriptions of these scripts, see “Environment setup scripts” (page 53) and “User session startup scripts” (page 54).

To run properly, MDM software requires the setting of global variables. For accounts into which the skeleton files are copied, these variables are set automatically to their default values. Although some variables are mandatory to allow MDM to run properly, others are optional. For descriptions of the mandatory and optional environment variables, see “Global environment variables” (page 51).

Directory structure

All Preside Multiservice Data Manager (MDM) software is contained in subdirectory /opt. This subdirectory is recommended by Sun for all software other than that created by Sun Microsystems Inc.

For an example of the directory structure for a workstation with MDM software load NMS110DaaS2400, see the figure “Sample directory structure” (page 45).

The subdirectories of /opt/MagellanNMS and their contents are as follows:

/opt/MagellanNMS/loads/

This directory contains the installed Preside Multiservice Data Manager (MDM) software loads. This directory can be exported as a read-only file system that other workstations can mount by using the Network File System (NFS) to gain access to the MDM software.

/opt/MagellanNMS/bin
/opt/MagellanNMS/lib
/opt/MagellanNMS/system
/opt/MagellanNMS/doc

These directories are symbolic links that point to the current MDM software load. They provide access to the following subdirectories:

- bin: MDM executables and scripts
- lib: libraries and configuration file templates. The files found in lib are the original versions and must not be modified. Copy these files to the /opt/MagellanNMS/cfg directory and modify the copied files. Main subdirectories of lib are as follows:
  - app-defaults: multi-lingual resource files
  - cfg: template configuration files
  - macros: macros and sample source files
  - messages: multi-lingual message files
  - model/types: Network Model Schema
  - nrs: schema and script files for the Network Reporting System (NRS)
  - tsets/$LANG/toolsets/<product line>: multi-lingual toolsets menu files. See “LANG” (page 52) for information on resolving the value of $LANG.
  - tsets/$LANG/tools/<application area>: multi-lingual Start Tool menu files. See “LANG” (page 52) for information on resolving the value of $LANG.
- system: system installation and configuration files. Main subdirectories of system are as follows:
  - config: scripts for the MDM Software Configuration tool

  - — init: NMS load initialization scripts
  - — inst: NMS load installation scripts
  - — skel: NMS default user environment system set-up files
- doc: documentation files

  To use a different software load, these symbolic links are redirected to point to the bin, lib, system, and doc directories for a different MDM software load.

/opt/MagellanNMS/ext/bin /opt/MagellanNMS/ext/lib

These directories are local directories for second-party customization packages for Preside Multiservice Data Manager (MDM). These customization packages contain software and configurations that extend MDM and its device support. Their subdirectories are similar to those delivered by MDM. MDM tools and servers recognize these directories as part of their standard search paths. For example, the Network Model looks for customized schema description files in the following order:

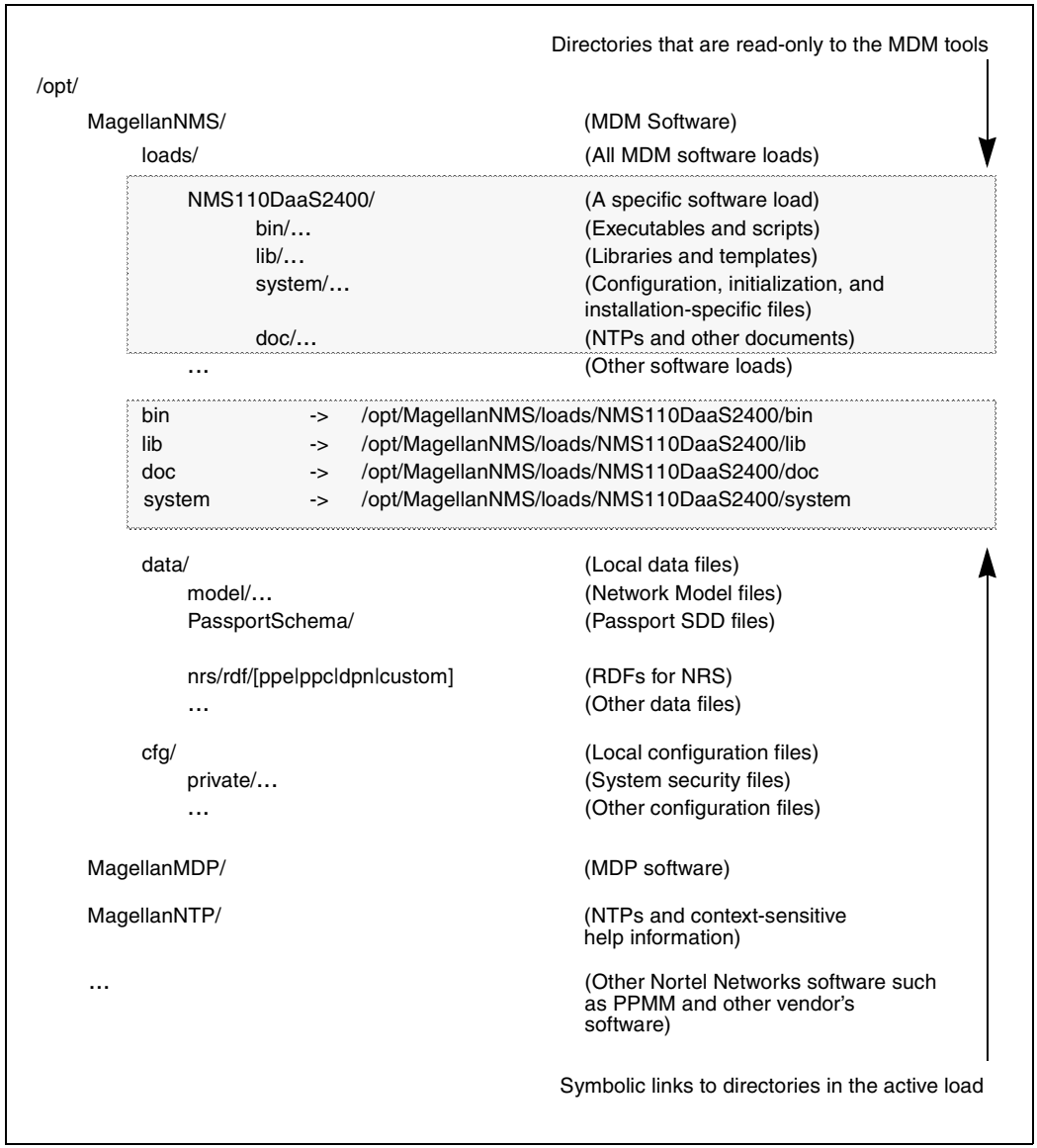
1 /opt/MagellanNMS/data/model/types (end-user or third-party customization)

2 /opt/MagellanNMS/ext/lib/model/types (second-party customization)

3 schema directory delivered with MDM, /opt/MagellanNMS/lib/model/types

Like the main,/opt/MagellanNMS/bin and /opt/MagellanNMS/lib, consider these directories as read-only because they contain Solaris package controlled files.

Figure 1
Sample directory structure



/opt/MagellanNMS/data/ /opt/MagellanNMS/cfg/

These two directories contain the data files and configuration files that are specific to the workstation. These two types of files are independent of the Preside Multiservice Data Manager (MDM) software load.

- Data files contain information manipulated by MDM software such as the network models for Fault, and the Service Data Description (SDD) files. Main subdirectories of the data directory are as follows:
  - model: Network Model related files
  - nrs: NRS data files
  - nvs: Network Viewer views and background maps
  - svm: Server Administration log and error files
- Configuration files contain information that is used to configure the MDM workstation and optionally includes files that override some of the other configurations (For example, Motif resource files and macro files). Main subdirectories of the cfg directory are as follows:
  - PassportSchema: Passport SDD and related files
  - app-defaults: customized resource files
  - macros: customized macros and MDM-provided macros
  - private: private MDM configuration files
  - tsets: customized toolset and tools menu files

/opt/MagellanNTP

This directory contains the source files for online documentation that can be displayed, and for the context-sensitive help that opens when you request help from a Preside Multiservice Data Manager (MDM) tool. This directory is only present when you install the Nortel Networks technical publication (NTP) (English), NTP (Japanese), or NTP (Chinese) software packages on the workstation.

This directory is divided up into the following main subdirectories. In these subdirectories, <release> is the release of software to which the documentation applies. For example, 13.4.

- /NMS/<release>/C contains the English version of the MDM NTPs and context-sensitive help
- /NMS/<release>/ja contains the Japanese version of the MDM NTPs and context-sensitive help
- /NMS/<release>/zh contains the Chinese version of the MDM NTPs and context-sensitive help
- /MDP/<release>/C contains the English version of the Management Data Provider (MDP) NTPs and context-sensitive help
- /MDP/<release>/ja contains the Japanese version of the MDP NTPs and context-sensitive help
- /MDP<release>/zh contains the Chinese version of the MDP NTPs and context-sensitive help

/opt/MagellanMDP

This directory contains the executables, utilities, schemas, spool, dump and backup files for the Management Data Provider (MDP) software. This directory is only present when the MDP software package is installed.

$HOME/MagellanNMS/

This is a subdirectory of a UNIX user's home directory which contains the user-specific Preside Multiservice Data Manager (MDM) configuration and preferences files.

Default MDM user environment skeleton files

The Preside Multiservice Data Manager (MDM) software includes skeleton files that can be copied into the home directory of a UNIX account to provide the default MDM user environment. MDM provides the following scripts to do the copying:

- /opt/MagellanNMS/bin/nmsuser to copy the skeleton files for an MDM user account
- /opt/MagellanNMS/bin/rncs to copy the files for an RNCS user account

The skeleton files are all located in directory /opt/MagellanNMS/system/skel. To display a list of the files in this directory, enter the ls command with the -a option. Because all of the filenames of the skeleton files begin with a period, they are hidden unless you include the -a option.

Once copied into the user's home directory, these files automatically start an MDM session and open a the MDM main window when the user logs in. By default, these files provide the user with access to the English language set of MDM tools defined in file /opt/MagellanNMS/lib/tsets/C/Full.tsets. You can select a different toolset by setting the NMSTSETS environment variable in the user account's set-up files. For more information on customizing the toolsets and Start Tool menus, see 241-6001-301 *Preside MDM Customization Administrator Guide*.

The skeleton files listed in this section are not needed for every user account. The files required depend on factors that include the type of shell associated with the user account and the window manager. For a list of the files needed for a given user account, see the table "Use of skeleton files for UNIX user accounts" (page 48).

Table 1
Use of skeleton files for UNIX user accounts

Bourne or Korn shell			**C-shell**		
SDK Motif	**OpenWin**	**CDE**	**SDK Motif**	**OpenWIn**	**CDE**
.profile	.profile	.profile	.login	.login	.login
			.cshrc	.cshrc	.cshrc
.Xdefaults	.Xdefaults	.Xdefaults	.Xdefaults	.Xdefaults	.Xdefaults
.mwmrc			.mwmrc		
.modmap	.modmap	.modmap	.modmap	.modmap	.modmap
.xsession	.xinitrc	.dtprofile	.xsession	.xinitrc	.dtprofile
		.sessionetc (See note)			.sessionetc (See note)

(Sheet 1 of 2)

Table 1 (Continued)
Use of skeleton files for UNIX user accounts

Bourne or Korn shell			C-shell		
SDK Motif	**OpenWin**	**CDE**	**SDK Motif**	**OpenWIn**	**CDE**
		.sessionexit (See note)			.sessionexit (See note)
Note: The *.sessionetc* and *.sessionexit* files are automatically copied into the user account's *$HOME/.dt* directory by *.dtprofile* when the user logs in to Common Desktop Environment (CDE) for the first time.					
(Sheet 2 of 2)					

The skeleton files and their contents are as follows:

/opt/MagellanNMS/system/skel/.cshrc

This file contains the startup script that sets up the shell environment and the Preside Multiservice Data Manager environment variables for UNIX accounts that run C-shell.See “Global environment variables” (page 51).

/opt/MagellanNMS/system/skel/.login

This file contains the login script for accounts that run C-shell and provides a prompt to start up one of the installed window environments (SDK Motif, OpenWin, or CDE), or to fall back on a plain console session, if none is installed.

/opt/MagellanNMS/system/skel/.profile

This file contains the equivalent of the .cshrc and .login scripts combined for accounts that run Bourne shell or Korn shell. For a description of the environment variables that are set up in this file, see “Global environment variables” (page 51).

/opt/MagellanNMS/system/skel/.Xdefaults

This file contains customized Motif resources. The initial contents of this file provide for SDK Motif, a look and feel that is similar to release 9 NMS software.

/opt/MagellanNMS/system/skel/.mwmrc

This file defines the SDK Motif Window Manager menu, keyboard, and mouse actions to correspond with those used in release 9 NMS.

/opt/MagellanNMS/system/skel/.modmap

This file defines X11 keyboard mappings for the user account.

/opt/MagellanNMS/system/skel/.xsession

This file contains a script that automatically

- starts a Preside Multiservice Data Manager (MDM) session (runs nmssession)
- opens an MDM window (runs nmstool)
- opens a console window on the desktop for user accounts that run the SDK Motif Window Manager

The script also ensures that the MDM session and the main window are removed at exit.

/opt/MagellanNMS/system/skel/.xinitrc

This file contains a script that automatically

- starts a Preside Multiservice Data Manager (MDM) session (runs nmssession)
- opens an MDM window (runs nmstool)
- pens a console window on the desktop for user accounts that run OpenWin

The script also ensures that the MDM session and main window are removed at exit.

/opt/MagellanNMS/system/skel/.dtprofile

This file contains a script that automatically starts a Preside Multiservice Data Manager (MDM) session (runs nmssession) and opens a MDM window (runs nmstool) when a CDE session is started by sessionetc and sessionexit scripts.

/opt/MagellanNMS/system/skel/.sessionetc

This file is automatically copied to directory ${HOME}/.dt/sessionetc when you log in for the first time using CDE. This file ensures that nmssession and nmstool are started.

/opt/MagellanNMS/system/skel/.sessionexit

This file is automatically copied to directory ${HOME}/.dt/sessionexit for a CDE session when you log in for the first time using CDE to ensure that nmssession and nmstool are terminated upon exit.

Global environment variables

To use Preside Multiservice Data Manager (MDM) software with the Solaris operating system, several global environment variables must be set up to provide access to the MDM executables and Motif resource files. These variables can be set up by

- entering the setenv command with the variable name and its new value as arguments for accounts that run C-shell
- entering the <variable>=<value> ; export <variable> commands for accounts that run Bourne or Korn shell
- inserting the variables into set-up files
- running one of the two scripts described in “Environment setup scripts” (page 53)

There are two sets of variables: mandatory variables that must be set up for the MDM software to perform correctly and optional symbol variables. The following sections describe these two sets of variables.

Mandatory variables

The following variables must be set for Preside Multiservice Data Manager (MDM) software to operate correctly. In the skeleton files that are provided with the MDM software, these variables are set by file .cshrc for user accounts that use C-shell or set-up file .profile for user accounts that use Korn or Bourne shell.

DISPLAY

DISPLAY is the name of the X-Windows display and is usually set by the login system (XDM, DTLOGIN). If the display is not set, MDM assumes a console login and sets the DISPLAY variable to :0.0.

LANG

LANG identifies the local language (the Locale). If not set, MDM sets the value of this variable to C. This value represents traditional UNIX and English. Other values that can be used with Solaris and with the MDM software are ja for Japanese and zh for Chinese.

USMSERVER

USMSERVER is used internally by some MDM tools and is set to the same value as DISPLAY.

PATH/path

PATH/path lets you invoke MDM tools without specifying the full path name when you enter the startup command. MDM appends its macros and bin directories to it (/opt/MagellanNMS/cfg/macros/user/opt/MagellanNMS/cfg/macros/nms and /opt/MagellanNMS/bin).

XUSERFILESEARCHPATH

This is the Motif Resource lookup path. Preside Multiservice Data Manager (MDM) appends its resource paths to it (/opt/MagellanNMS/cfg/app-defaults/%L/%N and /opt/MagellanNMS/lib/app-defaults/%L/%N). For an explanation of %L and %N, see the man pages for the X command.

CAUTION

Inability of MDM tools to run correctly

This variable must be set with at least these two paths for MDM tools to run properly.

Optional variables

The following variables are optional and are not set in the skeleton files supplied with the default Preside Multiservice Data Manager (MDM) environment. The recommended place to set them is in file .cshrc for C-shell accounts and file .profile for Bourne or Korn shell accounts.

NMSXTERM

NMSXTERM is the path for the preferred terminal console tool that the Preside Multiservice Data Manager (MDM) software uses whenever it needs to start a terminal window for UNIX Access or to execute a macro. If this

variable is not set, MDM software uses dtterm for the Common Desktop Environment (CDE) window manager, and xterm for other window managers.

NMSTSETS

NMSTSETS is the toolsets definition file which is used to open a Preside Multiservice Data Manager (MDM) window. If this variable is not set, MDM software uses the English language toolset definition file /opt/MagellanNMS/lib/tsets/C/Full.tsets. For a list and description of the toolset definition filenames you can use for this variable, see 241-6001-301 *Preside MDM Customization Administrator Guide*.

LPDEST

LPDEST is the name of the default printer for the user account. The values of the LPDEST and PRINTER environment variables must be identical to ensure the same results with BSD and SVR4 style applications.

Environment setup scripts

The Preside Multiservice Data Manager (MDM) software contains two scripts to set up the MDM environment. These scripts can be run from the command line, or from within set-up files of a UNIX user account, as described in “Setting up UNIX accounts for MDM” (page 55).

In the skeleton files that are provided with the MDM software, these scripts are called in file *.cshrc* for user accounts that use C-shell or in set-up file *.profile* for user accounts that use Korn or Bourne shell.

The scripts are as follows:

/opt/MagellanNMS/bin/nmscsh

This script sets up environmental variables for user accounts that run C-shell. Invoke this script from a non-default .cshrc file (source /opt/MagellanNMS/bin/nmscsh) to establish the Preside Multiservice Data Manager (MDM) environment.

/opt/MagellanNMS/bin/nmssh

This script sets up environmental variables for user accounts that run Korn shell or Bourne shell. Run this script from a non-default .profile file (. /opt/MagellanNMS/bin/nmssh) to establish the MDM environment.

User session startup scripts

The Preside Multiservice Data Manager (MDM) software contains two scripts to start an MDM session and open an MDM window. These scripts can be run from the command line, or can be called from within set-up files of a UNIX user account, as described in "Setting up UNIX accounts for MDM" (page 55).

In the skeleton files that are provided with the MDM software, these scripts are invoked in file .xsession for accounts that run the SDK Motif Window Manager, in file .xinitrc for accounts that run OpenWin, and in files .dtprofile, .sessionetc, and .sessionexit for accounts that run the Common Desktop Environment (CDE).

The scripts are as follows:

/opt/MagellanNMS/bin/nmssession

This script starts a Preside Multiservice Data Manager session and maintains it and its session servers. This script must be run once per DISPLAY session and terminated when the session is terminated.

> ***Note:*** Do not call this script if nmstool is already running.

/opt/MagellanNMS/bin/nmstool

This script opens a Preside Multiservice Data Manager window. By default this script starts the English language toolset Full.tsets. For the instructions to use a different toolset, see 241-6001-301 *Preside MDM Customization Administrator Guide*.

Chapter 3
Setting up UNIX accounts for MDM

This section contains instructions to create new UNIX accounts and modify root and existing UNIX accounts to run the Preside Multiservice Data Manager (MDM) software.

See the following sections for more information:

- "Creating a new UNIX user account with the default MDM user environment" (page 55)
- "Setting up the root account to run MDM software" (page 62)
- "Adding the default MDM user environment to an existing UNIX user account" (page 64)
- "Creating an RNCS user account" (page 66)
- "Ensuring that MDM dialog boxes are visible" (page 68)

Creating a new UNIX user account with the default MDM user environment

The procedures in this section describe how to create a UNIX group dedicated to Preside Multiservice Data Manager (MDM) users, and to create a new user account that runs the default user environment provided with the MDM software.

Creating a UNIX group for MDM

Use the procedures in this section to create a UNIX group dedicated to user accounts to run the Preside Multiservice Data Manager (MDM) software. Creating a UNIX group dedicated to MDM user accounts prevents unauthorized use of the MDM tools.

Create a UNIX group dedicated to MDM users with the *groupadd* command, or with Sun's administration tools. Sun provides a default admintool that comes with Solaris and an optional Server Administration tool suite. This section contains procedures for creating a UNIX group using the groupadd command, and using the Sun's default admintool.

Service parameters to set up a UNIX group

The following service parameters are required to set up a UNIX group dedicated to user accounts to run MDM software:

```
<group ID>
```

is a unique numerical identifier for the UNIX group that is greater than 99. Numbers 0 to 99 are reserved for special Sun applications. Use group ID 101 as a starting point.

```
<group name>
```

is the name of the group. This identifier must be unique and can consist of two to eight letters or numbers. The group name nmsop is recommended.

Creating a group using the groupadd command

1 Log on as root.

2 Enter the following command to create the group.

`/usr/sbin/groupadd -g <group ID> <group name>`

For an explanation of the parameters, see "Service parameters to set up a UNIX group" (page 56).

3 Display the return code to determine if the group was added successfully:

- If the root account is running C-shell, enter:

`echo $status`

- If the root account is running Korn shell or Bourne shell, enter:

```
echo $?
```

A return code is displayed that indicates success or failure of the command. The return codes are as follows:

0 The group has been successfully created.

2 The syntax of the command you entered is incorrect.

3 An invalid parameter was entered with the command.

4 The group ID entered is not unique.

9 The group name is not unique.

10 File /etc/group cannot be updated. The most common causes are: you are not logged on as root or file permissions are set so that you cannot write to this file.

You may now create one or more UNIX user accounts for Preside Multiservice Data Manager.

Creating a group using Sun's admintool

1. Log on as root.
2. Using the Common Desktop Environment (CDE) window manager, open a UNIX window.
3. Enter the following command to start Sun's admintool:

   ```
   /usr/bin/admintool &
   ```

   The tool's main window opens.
4. From Browse, select Group.
5. From Edit, select Add.

   The Add Group dialog opens.
6. Type the Group Name and Group ID in the dialog. You do not need to type any information in the Members List field. For descriptions of the Group name and Group ID parameters, see "Service parameters to set up a UNIX group" (page 56).
7. Click OK.

The Add Group dialog closes.

You can now create one or more UNIX user accounts for MDM.

Creating a UNIX account with the default MDM user environment

Use the following procedures to create a UNIX user account with the default Preside Multiservice Data Manager (MDM) user environment that is provided with the MDM software.

Create a UNIX account using the default MDM user environment with the useradd command, or by using the Sun administration tools. This section contains procedures to create a UNIX account with the useradd command, and to create a user account with Sun default admintool.

Creating the UNIX user account consists of entering the data required to set up the new user account and copying a set of skeleton files to the user account home directory. The skeleton files are included with the MDM software. The skeleton files are used to set up the UNIX user account environment to start an MDM session and to open the MDM main window when the user logs in. The skeleton files include the following set-up files: .login, .profile, .Xdefaults, and .mwmrc. The environment provided by using the skeleton files is the default MDM user environment. For descriptions of the skeleton files, see “Default MDM user environment skeleton files” (page 47).

Service parameters to create a UNIX account with the default MDM user environment

The following service parameters are required to create a UNIX user account with the default Preside Multiservice Data Manager (MDM) user environment:

`<Login Shell>`

is the full pathname of the program used as the user account shell when you log in. Values are /bin/csh for C-shell, /bin/sh for Bourne shell, and /bin/ksh for Korn shell. C-shell is the preferred.

`<Password>`

is the password for the new user account

<Path>

is the full path name for the home directory of the new user account. For example, /localdisk/<user name>. Solaris configures /HOME as an auto-mounted partition. Refer to the Sun Solaris Administrator Guide for information about the correct way to use /HOME.

<Primary Group>

is the group ID set up for UNIX user accounts that are dedicated to running MDM software. This is the number or name you entered when you set up the group in "Creating a UNIX group for MDM" (page 56).

<Skeleton Path>

is the full path name of the directory that contains skeleton information which can be copied into the user account's home directory to get the MDM user environment. That path name is /opt/MagellanNMS/system/skel.

<User ID>

is a numerical unique identifier greater than 99 for the new user account. Numbers 0 to 99 are reserved for special Sun applications.

<User Name>

is a unique name for the new user account consisting of from two to eight numbers or letters.

Creating a UNIX account with the default MDM user environment by using the useradd command

1 Log on as root.

2 Set up the user account and copy the skeleton files into the home directory of the new user account:

```
/usr/sbin/useradd \
-u <User ID> \
-g <Primary Group> \
```

```
-s <Login Shell> \
-d <Path> \
-m \
-k <Skeleton Path> \
<User Name>
```

For an explanation of the parameters to enter with this command, see "Service parameters to create a UNIX account with the default MDM user environment" (page 58).

3 Set the password:

```
passwd <user name>
```

You are prompted for a new password twice.

4 Enter the new password twice.

5 The new user account is set up to run the default MDM user environment and provides the user with access to the default English language toolset, called Full.tsets. This toolset provides access to the full set of MDM tools, except those for administration.

- If you wish to use this toolset, continue at step 6.
- If you wish to use a different toolset, including a toolset for languages other than English, change the default toolset definition file, as described in 241-6001-301 *Preside MDM Customization Administrator Guide*.

6 Provide the new user with the password you set up in step 3, and ask the user to log in. When the user logs in, an MDM session starts and the main window opens on the desk top.

Creating a UNIX account with the MDM user environment using the Sun default admintool

1 If the Sun admintool is already displayed on the screen, go to step 5. Otherwise, go to step 2.

2 Log on as root.

3 Using the CDE window manager, open a UNIX window.

4 Start the Sun admintool:

```
/usr/bin/admintool &
```

The tool's main window opens.

5 From Browse, select User.

6 From Edit, select Add.

The Add User dialog opens.

7 Type the following information in the fields:

`User Name:`
`User ID:`
`Primary Group`

identify the new user account and the UNIX group to which the account belongs. See “Service parameters to create a UNIX account with the default MDM user environment” (page 58).

`Secondary Groups:`

specifies a subgroup. Do not enter any information in this field.

`Comment:`

is an optional field that may contain information about the user account, such as the user’s full name and telephone number.

`Login Shell:`

identifies the shell for the user account. See “Service parameters to create a UNIX account with the default MDM user environment” (page 58).

`Password:`

is a field to select a method for setting the password for the new user account. Set the password by moving to the Password field, clicking the mouse, and selecting Normal Password. Enter the new password and click *OK*.

`Min Change:`
`Max Change:`
`Max Inactive:`
`Expiration Date:`
`Warning:`

are optional fields to set password expiration date and warning parameters

`Path:`

sets the home path for the user account. See “Service parameters to create a UNIX account with the default MDM user environment” (page 58).

8 Verify that the information is correct, and click *OK*.

The dialog closes.

9 In the main window of the admintool, select File -> Exit.

The admintool main window closes.

10 In the UNIX access window, run a script that copies the skeleton files into the home directory of the new user account:

```
/opt/MagellanNMS/bin/nmsuser <User Name>
```

11 The new user account is set up to run the default MDM user environment and provides the user access to the default English language toolset, called Full.tsets. This toolset provides access to the full set of MDM tools, except those for administration.

- If you wish to use Full.tsets, go to step 12.
- If you wish to use a different toolset, including a toolset for a language other than English, change the default toolset definition file, as described in 241-6001-301 *Preside MDM Customization Administrator Guide*.

12 Provide the new user with the password you set up in step 7. Verify that the user can log in, and that a MDM session starts, and the main window opens.

Setting up the root account to run MDM software

Use the information in this section to set up the *root* account to run Preside Multiservice Data Manager (MDM) software. The *root* user account is used for installing, configuring, and maintaining the MDM software. Access to some of the configuration files and operations required for these purposes are restricted to the root account.

To use the root account to install, configure, and maintain MDM software, the root account must be able to run the default MDM user environment. Ensure this happens

- temporarily, by entering a sequence of commands. If the user logs out or the session terminates, the user must enter the commands again after logging back in.

- permanently, by modifying the set-up files for the root account. When this is done, the root account always attempts to start an MDM session and open the main window when the user logs in. Modifying the set-up files for the root account is not recommended if the root account is used for managing workstations other than those that run MDM.

Choose the approach that suits the purposes for which your root account is used, then perform one of the two following procedures according to your choice.

Setting up the root account temporarily by entering a sequence of commands

1. Enter one of the following commands to source the Preside Multiservice Data Manager (MDM) user environment according to the login shell that the root account is running:

   - If the root account is running Bourne shell or Korn shell, enter:

   . /opt/MagellanNMS/bin/nmssh

   - If the root account is running C-shell, enter:

   source /opt/MagellanNMS/bin/nmscsh

2. Enter commands to start an MDM session according to the instructions in “Starting a local MDM session” (page 75) or “Starting a remote MDM session” (page 77).

Setting up the root account permanently by modifying set-up files

1. Log in as root.
2. Add the skeleton files to the existing user account by entering the following command:

   `/opt/MagellanNMS/bin/nmsuser root`

   The skeleton files are copied into the existing user account. Any existing set-up files that have the same names as the skeleton files are saved with the extension .old before the skeleton files are copied into the account.

3. The root account can now run the default MDM user environment and provides the user access to the default MDM toolset, called Full.tsets. This toolset provides access to the full set of tools, except those for administration.

   - If you wish to use this toolset, go to step 4.

- If you wish to use a different toolset, change the default toolset definition file in 241-6001-301 *Preside MDM Customization Administrator Guide*

4 Log out and log back in again. When you log back in, an MDM session starts and the main window opens on the desk top.

Adding the default MDM user environment to an existing UNIX user account

This section describes how to update an root and existing UNIX user accounts to use the default Preside Multiservice Data Manager (MDM) user environment.

Add the default MDM user environment to an existing UNIX user account by one of the following methods:

- by adding the skeleton files for the default MDM user environment to the existing user account
- by modifying the existing account's set-up files to access the default MDM user environment

Updating an existing UNIX user account by adding the skeleton files

This procedure adds skeleton files to an existing user account.

Note: Although the procedure is intended to be performed while you are logged in as root, other UNIX users can also perform this procedure to add the skeleton files to their accounts when their accounts have been created.

1 Log in as root.

2 Add the skeleton files to the existing user account:

```
/opt/MagellanNMS/bin/nmsuser <User Name>
```

The skeleton files are copied into the existing user account. Any existing set-up files that have the same names as the skeleton files are saved with the extension .old before the skeleton files are copied into the account.

The new user account is set up with the default Preside Multiservice Data Manager (MDM) user environment. When the user logs in, an MDM session starts automatically and the main window opens.

Updating an existing UNIX user account by modifying the account's set-up files

This section describes how to modify the existing user account's set-up files to access the Preside Multiservice Data Manager (MDM) user environment.

Use the MDM skeleton set-up files (.login, .cshrc, and so on) in directory /opt/MagellanNMS/system/skel as a model when modifying the set-up files for the existing account. For descriptions of these skeleton set-up files, see "Default MDM user environment skeleton files" (page 47).

The MDM software contains two scripts that you can source in the user account's setup files to supply the user account's environment with the symbols and values needed to run MDM. The script you choose depends on the shell that the user account runs on:

- if the account runs Korn or Bourne shell, add a statement to set-up file .profile that includes the source command:

  ```
  . /opt/MagellanNMS/bin/nmssh
  ```

- if the account runs C-shell, add a statement to set-up file .cshrc that includes the source command:

  ```
  /opt/MagellanNMS/bin/nmscsh
  ```

Because these scripts augment the user environment with the symbols and values for MDM, add the statements to source the symbols and values after all other statements that set up the user account environment. For a description of the values and symbols for MDM, see "Default MDM user environment skeleton files" (page 47).

When you have updated the existing account to source the MDM user environment, you must provide a means to start an MDM session. The recommended approach is to modify the .dtprofile file (for CDE) so that it automatically starts a session and opens the main window when the user logs in. Use the skeleton files for making these modifications.

Creating an RNCS user account

Use the information in this section to create a UNIX user account that lets a user at an ASCII terminal manage the network from a Remote Network Communication System (RNCS).

This section contains procedures to create an RNCS user account with the useradd command, and to create the account with the Sun default admintool. The steps to create an RNCS user account are similar to those for creating a UNIX account that has the Preside Multiservice Data Manager (MDM) user environment, except that you specify /opt/MagellanNMS/bin/rncs as the login shell path for the new user account.

Creating an RNCS user account using the useradd command

1. If you have not done so, create a UNIX group for Preside Multiservice Data Manager (MDM) users, as described in.“Creating a UNIX group for MDM” (page 56).
2. Perform the procedure “Creating a UNIX account with the default MDM user environment” (page 58). In step 2, specify */opt/MagellanNMS/bin/rncs* for parameter -s <login shell>.

Creating an RNCS user account using Sun’s admintool

1. Log on as root.
2. If you have not done so, create a UNIX group for Preside Multiservice Data Manager (MDM) users, as described in.“Creating a UNIX group for MDM” (page 56).
3. If the Sun admintool is already displayed on the screen, go to step 6. Otherwise, go to step 4.
4. Using the CDE window manager, open a UNIX window.
5. Start the Sun admintool:

   ```
   /usr/bin/admintool &
   ```

   The tool’s main window opens.
6. From Browse, select User.
7. From Edit, select Add.

   The Add User dialog opens.
8. Type information in all of the following fields. Do not enter any information in the Login Shell field.

`User Name:`
`User ID:`
`Primary Group`

identify the new user account and the UNIX group to which the account belongs. For explanations of these parameters, see “Service parameters to create a UNIX account with the default MDM user environment” (page 58).

`Secondary Groups:`

specifies a subgroup. Do not enter any information in this field.

`Comment:`

is an optional field that can contain information about the user account, such as the user’s full name and telephone number.

`Password:`

is a field to select a method for setting the password for the new user account. Set the password by selecting Normal Password. Enter the new password and click OK.

`Min Change:`
`Max Change:`
`Max Inactive:`
`Expiration Date:`
`Warning:`

are optional fields that can be used to set password expiration date and warning parameters

`Path:`

sets the home path for the user account. For an explanation of this parameter, see “Service parameters to create a UNIX account with the default MDM user environment” (page 58).

9 Move to the Login Shell field, press the menu mouse button and select Other.

A field for specifying the login shell path opens in the dialog.

10 Enter the following login shell path name:

`/opt/MagellanNMS/bin/rncs [-T <idle timeout>]`

where:

`-T` indicates a timeout value. RNCS automatically terminates if no command input occurs during the specified number of minutes.

11 Verify that the information in the add user dialog is correct, and click OK.

12 Copy the skeleton files into the home directory of the new RNCS user account:

`/opt/MagellanNMS/bin/rncsuser <username> <home directory> <unix access> <CID>`

where

`<username>`

is the userid for the new RNCS user

`<home directory>`

is the full pathname of the new RNCS user's home directory

`<unix access>`

specifies whether the RNCS user account is to have UNIX access. The values are Y or N.

`<CID>`

is the customer network management identifier (CNMID) associated with the RNCS account. The range of values is 0 to 8191.
If you are dealing with a subnetwork, enter instead a subnetwork identifier or a subnetwork virtual private network identifier.

The new RNCS user account is now set up with the environment required to allow a user to access the network. See 241-6001-013 *Preside MDM Remote Network Communication System User Guide* for the instructions to establish an RNCS session.

Ensuring that MDM dialog boxes are visible

Change a Solaris Common Desktop Environment (CDE) window manager setting to prevent dialog boxes from being hidden.

1 Click on the **Style Manager** icon on the CDE tool bar.

2 Click on **Window.**

3 Disable **Allow Primary Windows On Top.**

Chapter 4
Software licensing

This section contains information to delete and query Preside Multiservice Data Manager (MDM) licenses. Several commands are available for verifying licensing information. This section consists of the following topics:

Generating a temporary license key

Preside Multiservice Data Manager (MDM) software provides a means to generate a temporary license to run MDM. This license is valid for 30 days but is not renewable. At the end of the 30 days you must install a new license key obtained from Nortel Networks.

Procedure

1. Log in as root.
2. Start the c-shell:

   ```
   csh
   ```

3 Enter the following command:

```
/opt/MagellanNMS/system/config/nmsTmpInstall
```

Adding a new license key

Use this procedure to add a new license key if you receive a new license key from Nortel Networks to an installed version of Preside Multiservice Data Manager (MDM)

Procedure

1 Log in as root.

2 Start the c-shell:

```
csh
```

3 Access the license directory:

```
cd /etc/opt/Magellan
```

4 Open the following file with a UNIX editor such as vi:

```
licenses.cfg
```

5 Add the license key to the file.

6 Check what you have entered twice.

7 Save the file and exit from the file.

8 Have all users end their MDM sessions and restart them again.

Deleting license keys

If you delete a license key from the license key file and then rollback to a previous release of Preside Multiservice Data Manager, the software will not run until the license key is restored to the license key file. To avoid difficulty in rolling back to a previous software release, never delete license keys from the license key file. License keys occupy very little disk space, so the penalty (in terms of storage space) for preserving them is small.

Listing the packages represented by an options bitmap

To determine which packages are represented by a given options bitmap, type

```
/opt/MagellanNMS/system/config/nms_list_options
<bitmap>
```

where:

<bitmap> is a set of hexadecimal codes in the <options> field of the license key that represents the packages of Preside Multiservice Data Manager (MDM) software that your license entitles you to run.

For example, enter the following command:

```
nms_list_options 336
```

For more information about MDM software sets, refer to 241-6001-102 *Preside MDM Planning Guide*.

Verifying the customer name in the license key and customer identifier files

The customer name must match in both files for the Preside Multiservice Data Manager (MDM) software in order to run. Display the customer name entered in the license key file and in the customer identifier file as follows:

```
/opt/MagellanNMS/system/config/nms_list_cust_names
```

This command produces a response similar to

```
Customer name written in the MDM customer name file:
 MDMDEV

Customer names occurring in the license file for
product MDM:
MDMDEV
```

Displaying all license keys, their validity, and deleting invalid licenses

To display a report of the license keys and determine if the licenses are still valid, type

```
/opt/MagellanNMS/system/config/nms_file_report [-c]
```

where:

[-c] prompts you for permission to delete expired licenses. You must be logged in as root.

The report produced indicates if the license is valid, or why it is invalid. The reasons a license is invalid include the following:

```
License for customer other than <cust_id>
```

The customer name does not match in files /etc/opt/Magellan/LICcustName.cfg and /etc/opt/Magellan/LIClicenses.cfg.

```
License for release other than <release>
```

The encrypted license information applies to a release other than the one entered into the <release> field of the license key.

```
Invalid license password
```

A non-valid password entered into the password field

```
Invalid date
```

The syntax of the date entered in the <start_date> or <expiry date> field is incorrect.

```
Invalid option bitmap
```

An unrecognized bitmap is entered into the <options> field.

```
License not yet valid
```

The date entered in the <start_date> field has not yet arrived.

```
License expired
```

The date entered in the <expiry date> field has passed.

Entering the command without the -c option may produce a response similar to the following example:

```
LICENSES:
________

NMS R12 NMSDEV ANY 19991124 20300101 FFFFFFFF
C77G6102052
         License for non-MDM product
NMS R13 NMSDEV ANY 20001204 20300101 FFFFFFFF
076A76F515G
         License for non-MDM product
MDM R13 NMSDEV ANY 20010119 20300101 FFFFFFFF
F893H7352257
         License currently valid
```

Entering the command with the -c option while logged in as root displays each non-valid license, one at a time, followed by the prompt:

```
Do you want to delete this entry? (y on n [n])
```

Enter *y* to delete the license or *n* to keep it.

When the command has run through all of the non-valid licenses in the file, the following response appears:

```
You have made some changes to the licenses file
The modified file has been written in /etc/opt/
Magellan/LICLicenses.new
Please execute the following steps to activate it:
1- type: cd /etc/opt/Magellan
2- type: cat LICLicenses.new
3- if the contents are satisfactory, type:
      cp LICLicenses.cfg LICLicenses.old
      mv LICLicenses.new LICLicenses.cfg
```

Log in as root and follow the prompts.

Listing the packages that your licenses allow you to run

To display a list of the packages (options) that the license keys entitle you to run, enter the following command:

`/opt/MagellanNMS/system/config/nms_list_activ_opt`

For more information about MDM software sets, refer to 241-6001-102 *Preside MDM Planning Guide*.

Chapter 5
Starting and ending MDM sessions

This section contains the information required to start Preside Multiservice Data Manager(MDM) sessions.

See the following sections for more information:

- "Starting a local MDM session" (page 75)
- "Starting a remote MDM session" (page 77)
- "Ending an MDM session" (page 79)

Starting a local MDM session

Use the procedure in this section to start a Preside Multiservice Data Manager (MDM) session on a local workstation and to open the main window.

You do not need to use the information in this section to start a local MDM session if the UNIX user account is one of the following:

- an existing account to which the default MDM user environment has been added. For these accounts, the session starts automatically and the main window opens when you log in.
- a new user account that is created to run the default MDM user environment. For these accounts, the session starts automatically and the main window opens when you log in.
- an RNCS user account. For these accounts the user environment is set up to allow you to access the network through RNCS.

Prerequisites

Before performing the following procedure, ensure that you have sourced the MDM user environment by entering commands, or by modifying the user account's set-up files as described in "Adding the default MDM user environment to an existing UNIX user account" (page 64).

Using commands to start an MDM session and open the main window

1 Open the main window by

```
/opt/MagellanNMS/bin/nmstool \
[Motif resource parameters] [toolset file] &
```

where:

`[Motif resource arguments]`

are used to specify Motif resources and X-command line arguments such as the size of the MDM window and its location on the screen. For example, -geometry +0+0.

`[toolset file]`

is the filename or the full pathname of a toolset definition file. A toolset definition file specifies the set of MDM tools that a user may access at login. For descriptions of the toolset definition files provided with the MDM software, see 241-6001-301 *Preside MDM Customization Administrator Guide*.

If you omit this parameter, the toolset file specified in the set-up files by the value of environment variable NMSTSETS is used. The default value of this variable is the English language toolset Full.tsets.

This toolset file provides access to all MDM tools except those intended for an administrator. For an administrator (root account) enter Admin.tsets for this parameter.

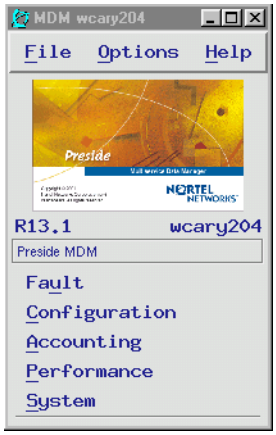
You can also create your own toolset definition files. For the instructions to customize the toolset menus, see 241-6001-301 *Preside MDM Customization Administrator Guide*.

The copyright dialog opens.

2 Click OK.

The copyright dialog closes.

The main window opens.



Starting a remote MDM session

This section describes how to start a Preside Multiservice Data Manager (MDM) session on a remote workstation and display the MDM window on the local workstation.

You can do this if following conditions exist:

- the workstations are running MDM
- the local workstation is running X-Windows
- the two workstations are linked by a TCP/IP connection (including over Ethernet, Token Ring, IP over WAN)
- the user account must be shared through NFS or cloned (same user name, ID, and environment) between the two workstations

You can only run one MDM session and open one window for a given user-session (for a given DISPLAY variable and value).
From a given terminal window or console, you can run only one MDM session per workstation, including remote workstations. See the figure “Examples of multiple sessions” (page 80) for an illustration that helps explain this guideline.

This does not mean that a workstation only supports one MDM session. A workstation can host many sessions (one for the console, one for each X-terminal window, and one for each remotely connected session). An operator can have concurrent sessions on the local workstation as well as on remote (regional) ones. See the figure "Examples of multiple sessions" (page 80).

Starting a remote session on trusted workstations

Trusted Preside Multiservice Data Manager (MDM) workstations are workstations that allow remote login to occur without security checks. They must be trusted because the remote shell command (rsh) is used to invoke the remote MDM session.

To configure workstations as trusted, you must add information about the hosts to files /etc/hosts.equiv and/or <home directory> /.rhosts file(s). For information on this procedure, refer to the man pages for hosts.equiv and rsh.

1 Enter the following command:

```
/opt/MagellanNMS/bin/nmstool \
-host <remote hostname> \
[-user <remote user>] ...\
[Motif resource parameters] \
[toolset file] &
```

where:

`<remote hostname>`

is the hostname of a remote workstation on which you wish to run the MDM tool. If you omit this parameter, the workstation is assumed to be this workstation (localhost).

`<remote user>`

is the remote user account name. You can use this option when the remote user account name to use is different from the current name.

Note: Similar remote MDM sessions can be established by selecting System -> Utilities -> Remote Access.

Starting a remote session on non-trusted workstations

Use the following procedure to start a remote Preside Multiservice Data Manager (MDM) session if the workstations are not trusted, or if you need to log into a remote workstation from a different
user account than the one on the local MDM workstation.

1 Allow information generated on the remote workstation to be displayed on the local workstation:

```
xhost +<remote host name>
```

2 Log in to the remote workstation by using rlogin or Telnet.

3 Enter the following command while logged in:

```
/opt/MagellanNMS/bin/nmstool -display \
<local display> \
[<Motif arguments>] \
[<toolset>]
```

where:

<local display>

is the value of the DISPLAY environment variable for the local workstation [not the variable for the remote MDM session.

Example:

To set up a remote session on workstation MDM 1 for workstation MDM 2, first remote login in to MDM 2, then enter: /opt/MagellanNMS/bin/nmstool -display NMS1:0.0

4 When the session is over and you have logged out, enter the following command to prevent any more information generated on the remote workstation from being displayed on the local workstation:

```
xhost -
```

Ending an MDM session

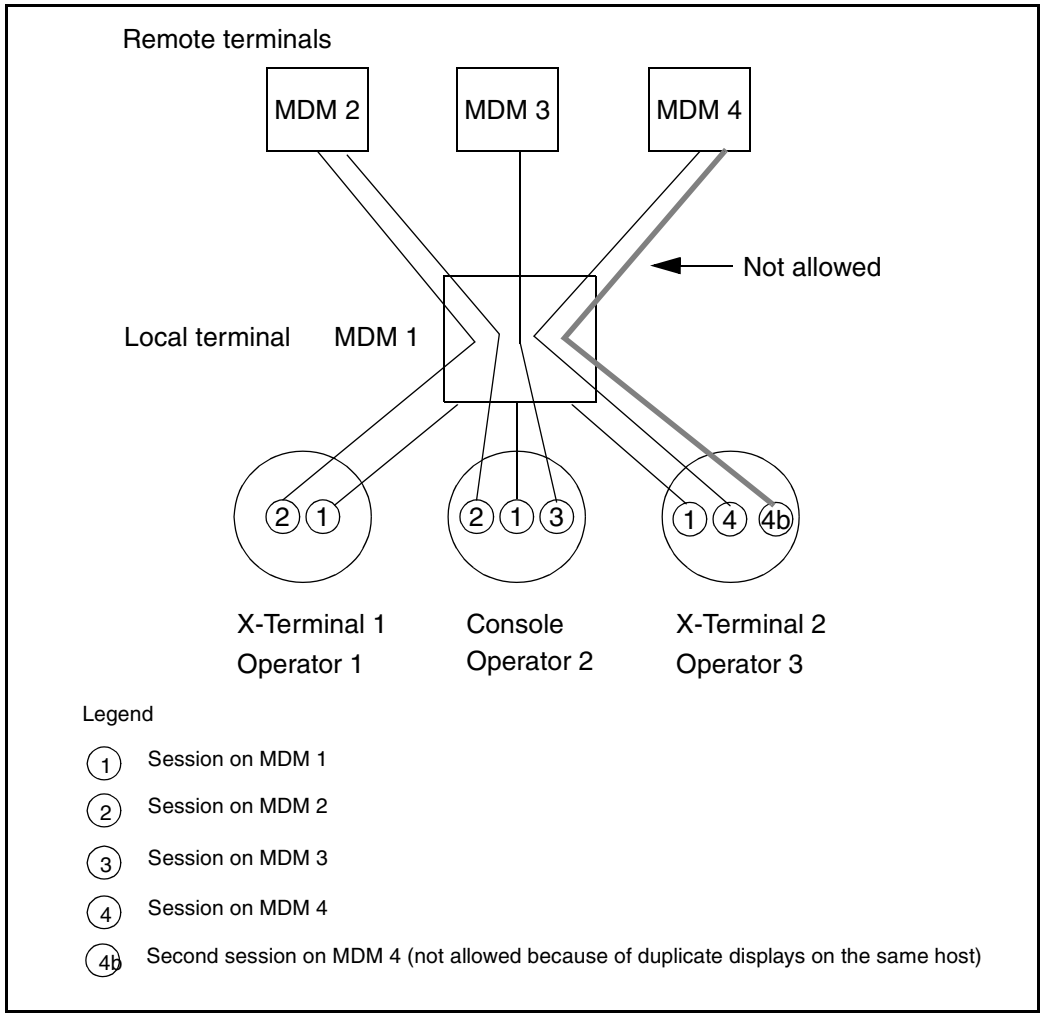
To end an active Preside Multiservice Data Manager (MDM) session, from the main window menu select File -> Exit.

For remote sessions the window, the corresponding mdmsession, and the remote connection are terminated.

For local sessions, the mdmsession remains active until you log out.

While the mdmsession is still active, the connections to the network are preserved, and you can open an MDM window without re-establishing these connections.

Figure 2
Examples of multiple sessions



Chapter 6
Roadmap to the MDM servers

This section lists the Preside Multiservice Data Manager (MDM) servers that can be set up in networks that contain Data Packet Network (DPN) and Passport switches. Refer to the section that applies to the types of switches in your network. If your network contains both DPN and Passport switches, refer to both sections for information about the servers to configure and to locate the instructions needed to configure them.

- "Servers in networks that contain DPN switches" (page 81)
- "Servers in networks that contain Passport and MPE switches" (page 86)

Servers in networks that contain DPN switches

The table "Servers in networks that contain DPN switches" (page 81) lists the Preside Multiservice Data Manager (MDM) servers that can be configured in networks that contain DPN switches. The table groups the servers according to the functions they support.

Some of the MDM servers listed in the table are common to networks that contain both switches and that are configured the same way. These servers are labelled common in the table.

Table 2
Servers for networks that contain DPN switches

Function and related servers	Description and references
Basic servers (common):	
MDM Log Collector (OAMC)	collects MDM logs from software processes and makes them available to the System Log Display tool The OAMC server is started automatically. You do not need to configure the server. For information about the OAMC server, see 241-6001-310 *Preside MDM Server Reference Guide*.
MDM Context Server (CTXSVR)	provides a way for software processes running on a workstation to communicate with each other by putting values into context, or by getting values that were previously put into context. The CTXSVR server is started automatically. You do not need to configure the server. For information about the CTXSVR server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Multi-Nodal Naming Server (MNSD)	provides a way for software processes to register so they can locate each other. There are level 1 and level 2 servers. Level 1 lets processes on the same workstation to locate each other. Level 2 lets processes on different workstations on a LAN locate each other. The level 1 server starts automatically. You do not need to configure a level 1 server. If there is more than one workstation on the LAN and the workstations share processes (servers), you must configure and start a level 2 MNSD server on at least one of the workstations on the LAN. For the instructions to configure a level 2 MNSD server, see “Configuring Multi-nodal Naming Service domains” (page 223). For information about the MNSD server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Servers that support DPN network access:	
(Sheet 1 of 5)	

Table 2 (Continued)
Servers for networks that contain DPN switches

Function and related servers	Description and references
Host Group Directory Server (HGDS)	provides NCS OA access parameters and grouping information to other servers and processes. This information is used to access the OAs in the Network Control System (NCS) for the DPN switches. For the instructions to configure the server for DPN network access, see “Configuring servers for DPN switches” (page 93). For information about the HGDS server, see 241-6001-310 *Preside MDM Server Reference Guide*.
NCS Communications Manager (NCSMGR)	lets the workstation communicate with destinations in the Network Control System (NCS) of a DPN network. The types of communications include: sending commands to NCS; receiving responses; and collecting logs, alarms, and component status records. For the instructions to configure the server for DPN network access, see “Configuring servers for DPN switches” (page 93). For information about the NCSMGR server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Servers that support DPN surveillance access (See Note 1)	
DPN Management Data Router (DMDR)	processes raw surveillance data received from the OAs in the NCS, calculates the states of DPN components based on the raw data, and forwards the processed results to the GMDR server. To configure the server for surveillance, see “Configuring servers for DPN switches” (page 93). For information about the DMDR server, see 241-6001-310 *Preside MDM Server Reference Guide*.

(Sheet 2 of 5)

Table 2 (Continued)
Servers for networks that contain DPN switches

Function and related servers	Description and references
General Management Data Router (GMDR)	routes processed surveillance data for the MDM-supported switches in the network to the surveillance tools and to the Alarms and Status API Provider. It also collects and stores surveillance information. For the instructions to configure the server for surveillance, see "Configuring servers for DPN switches" (page 93). For information about the GMDR server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Data Manager Agent (DMA)	performs server surveillance and forwards workstation server alarms through an IMDR server to a GMDR server or to the NCS, performs workstation surveillance through NCS status probing, and performs global clearing in the NCS. To configure the server to support server surveillance and workstation surveillance see "Configuring server alarm distribution and workstation status probing" (page 261). To configure the server to support global alarm clearing, see "Configuring DPN alarm clearing" (page 233). For information about the DMA server, see 241-6001-310 *Preside MDM Server Reference Guide*.
DBNL auto-disabling server daemon (DBNLWatch)	monitors alarms from DPN switches. When it detects an alarm indicating the activation of a Dial Backup Network Link (DBNL), it sets up a watch on the primary link. When the primary link comes up and remains stable, for a specified period, *DBNLWatch* optionally deactivates the DBNL. For information about the DBNL Watch server, see 241-6001-310 *Preside MDM Server Reference Guide*.

(Sheet 3 of 5)

Table 2 (Continued)
Servers for networks that contain DPN switches

Function and related servers	Description and references
Servers that support the Network Model and state-based surveillance (common) (See note 2):	
	For the instructions to configure the network model, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.
Network Model Coordinator (DNMNMC)	coordinates access to the Network Model and allocates the shared memory segment used by the Network Model
	For information about the DNMNMC server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Network Model Server (NMSERVER)	provides access to the Network Model information to the Fault tools and to the Network Model API Provider
	For information about the NMSERVER server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Network Model Editing Server (EDSERVER)	lets you edit the Network Model from the Network Viewer tool
	For information about the EDSERVER, see 241-6001-310 *Preside MDM Server Reference Guide*.
Surveillance Network Model Updater (SURNUP)	maintains the active Network Model and updates it with current state information. SURNUP receives its update information from the GMDR server.
	For information about the SURNUP server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Servers that support DPN provisioning access:	
PM File Access Server (PFAS)	manages provisioning access and file transfers between the MDM workstation and DPN modules, including backup and restore mcfs
	To configure this server for provisioning access, see “Configuring servers for DPN switches” (page 93).
	For information about the PFAS server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Servers that support various data collection feature packages (common):	

(Sheet 4 of 5)

Table 2 (Continued)
Servers for networks that contain DPN switches

Function and related servers	Description and references
Network Configuration Database Server (NCD)	provides access to a repository of network-wide key service data, such as DNAs, NAMS IDs, and GATEWAY-IDs. The server stores this data in a database to support network-wide semantic checks. To configure NCD and for information about the startup command for this server, see 241-6001-308 *Preside MDM Network Configuration Database for DPN Administrator Guide*.
Note 1: To support alarm-based surveillance, the servers that support DPN network access must be started first. That is: NCSMGR and HGDS.	
Note 2: To support the network model and state-based surveillance, the servers that support DPN network access and DPN surveillance must be started first. That is: NCSMGR, HGDS, DMDR, GMDR, and DMA.	
(Sheet 5 of 5)	

Servers in networks that contain Passport and MPE switches

The table "Servers in networks that contain Passport and MPE switches" (page 86) lists the servers that can be configured on Preside Multiservice Data Manager (MDM) workstations in networks that contain Passport and MPE switches. The table groups the servers according to the functions they support.

Some of the servers listed in the table are common to networks that contain DPN, Passport and MPE switches and that are configured the same way. These servers are labelled (common) in the table.

Table 3
Servers for networks that contain Passport and MPE switches

Function and related servers	Description and references
Basic servers (common):	
(Sheet 1 of 6)	

Table 3 (Continued)
Servers for networks that contain Passport and MPE switches

Function and related servers	Description and references
MDM Log Collector (OAMC)	collects MDM logs from software processes and makes them available to the System Log Display tool The OAMC server starts automatically. You do not need to configure this server. For information about the OAMC server, see 241-6001-310 *Preside MDM Server Reference Guide*.
MDM Context Server (CTXSVR)	provides a way for software processes running on a workstation to communicate with each other by putting values into context, or by getting values that were previously put into context. The CTXSVR server starts automatically. You do not need to configure this server. For information about the CTXSVR server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Multi-Nodal Naming Server (MNSD)	provides software processes with a place to register so that they can locate one another. There are level 1 and level 2 servers. Level 1 server lets processes on the same workstation locate. Level 2 lets processes on different workstations on a LAN locate one another. The level 1 server starts automatically. You do not need to configure a level 1 server. If there is more than one workstation on the LAN and the workstations share processes (servers), you must configure and start a level 2 MNSD on at least one of the workstations on the LAN. To configure a level 2 MNSD server, see “Configuring Multi-nodal Naming Service domains” (page 223). For information about the MNSD server, see 241-6001-310 *Preside MDM Server Reference Guide*.

(Sheet 2 of 6)

Table 3 (Continued)
Servers for networks that contain Passport and MPE switches

Function and related servers	Description and references
Servers that support Passport network access:	
Host Group Directory Server (HGDS)	provides information for network access and groups to access the Passport switches. To configure the server for Passport network access, see "Configuring MDM servers for Passport switches" (page 123). For information about the HGDS server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Passport Communications Manager (FDTM)	manages the Data Translation (FDTR) process, which translates messages into a format that can be used by other MDM servers and tools. To configure this server for network access, see "Configuring MDM servers for Passport switches" (page 123). For information about the FDTM server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Servers that support Passport surveillance access (See Note 1):	
FMIP Management Data Router (FMDR)	routes alarm and state change notification event reports from a group of Passport switches to the GMDR server To configure this server for surveillance, see "Configuring MDM servers for Passport switches" (page 123). For information about the FMDR server, see 241-6001-310 *Preside MDM Server Reference Guide*.
General Management Data Router (GMDR)	routes processed surveillance data for the MDM-supported switches in the network to the Fault tools and to the Alarms and Status API Provider. It also collects and stores surveillance information. To configure this server for surveillance, see "Configuring MDM servers for Passport switches" (page 123). For information about the GMDR server, see 241-6001-310 *Preside MDM Server Reference Guide*.

(Sheet 3 of 6)

Table 3 (Continued)
Servers for networks that contain Passport and MPE switches

Function and related servers	Description and references
Data Manager Agent (DMA)	performs server surveillance and forwards workstation server alarms through an IMDR server to the GMDR server. To configure the server to support server surveillance through GMDR, see “Configuring DPN alarm clearing” (page 233). For information about the DMA server, see 241-6001-310 *Preside MDM Server Reference Guide*.
(Sheet 4 of 6)	

Table 3 (Continued)
Servers for networks that contain Passport and MPE switches

Function and related servers	Description and references
Servers that support MPE network access:	
Host Group Directory Server (HGDS)	provides information for network access and groups to access the Passport switches. To configure the server for Passport network access, see "Configuring MDM servers for MPE switches" (page 167). For information about the HGDS server, see 241-6001-310 *Preside MDM Server Reference Guide*.
MPE Communications Manager (NDTM)	manages the Data Translation (NDTR) process, which translates messages into a format that can be used by other MDM servers and tools. To configure this server for network access, see "Configuring MDM servers for MPE switches" (page 167). For information about the NDTM server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Servers that support MPE surveillance access (See Note 1):	
MPE Management Data Router (NMDR)	routes alarm and state change notification event reports from a group of MPE switches to the GMDR server To configure this server for surveillance, see "Configuring MDM servers for MPE switches" (page 167). For information about the NMDR server, see 241-6001-310 *Preside MDM Server Reference Guide*.
General Management Data Router (GMDR)	routes processed surveillance data for the MDM-supported switches in the network to the Fault tools and to the Alarms and Status API Provider. It also collects and stores surveillance information. To configure this server for surveillance, see "Configuring MDM servers for MPE switches" (page 167). For information about the GMDR server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Servers that support the Network Model and state-based surveillance (common) (See note 2):	

(Sheet 5 of 6)

Table 3 (Continued)
Servers for networks that contain Passport and MPE switches

Function and related servers	Description and references
	For the instructions to configure the network model, see 241-6001-015 *Preside MDM Network Model Administrator Guide*.
Network Model Coordinator (DNMNMC)	coordinates access to the Network Model and allocates the shared memory segment used by the Network Model For information about the DNMNMC server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Network Model Server (NMSERVER)	provides access to the Network Model information to the Fault tools and to the Network Model API Provider For information about the NMSERVER server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Network Model Editing Server (EDSERVER)	lets users edit the Network Model from the Network Viewer tool For information about the EDSERVER server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Surveillance Network Model Updater (SURNUP)	maintains the active Network Model and updates the current state information. SURNUP receives its update information from the GMDR server. For information about the SURNUP server, see 241-6001-310 *Preside MDM Server Reference Guide*.
Servers that support various data collection feature packages (common):	
End-to-end Server	acts an intermediary between all the service provisioning tools and the MDM Command Console Functional Process (CMCFUN) server.The CMCFUN server forwards operator commands to Passport devices for execution.
Note 1: To support alarm-based surveillance, the FDTM and HGDS servers that support Passport network access must be started first.	
Note 2: To support the Network Model and state-based surveillance, the FDTM, HGDS, FMDR, GMDR and DMA servers that support Passport network access and surveillance must be started first.	

(Sheet 6 of 6)

Chapter 7
Configuring servers for DPN switches

This section describes how to configure Preside Multiservice Data Manager (MDM) servers on a workstation to support the following basic functions in networks that contain DPN switches:

- network access: lets users log on to Operations Agents (OAs) in the Network Control System (NCS) to perform operations such as provisioning or troubleshooting
- surveillance access: lets MDM software gather alarm-based surveillance information automatically from NCS
- provisioning access: lets users upload and download Master Control Files (MCFs) from switches

Although it is possible to configure servers to support one or two of these functions, all three are required in most installations. For information about servers, see “Roadmap to the MDM servers” (page 81).

This section contains the following information:

- "Task list for configuring servers" (page 106)
- "Configuring the NCS hierarchy for surveillance" (page 107)
- "Configuring the NCS hierarchy for surveillance" (page 107)
- "Configuring and starting the servers" (page 115)
- "Setting up special processing of alarms" (page 118)
- "Preloading CNMIDs to filter status records" (page 119)
- "Setting up CNMIDs for VPNs" (page 121)

Servers required to support network access, surveillance access, and provisioning access

The figure "Interdependencies of servers in networks containing DPN switches" (page 96) shows the Preside Multiservice Data Manager (MDM) servers that need to be configured to support the basic functions of DPN network, surveillance, and provisioning access, and it illustrates the dependencies between the servers.

The servers that need to be configured to support these functions are as follows:

- NCS Communications Manager (NCSMGR)
- Host Group Directory Server (HGDS)
- DPN Management Data Router (DMDR)
- General Management Data Router (GMDR)
- Data Manager Agent (DMA)
- Provisioning File Access Server (PFAS)
- Provisioning File Access Server (PFAS) for software download

For detailed descriptions of these servers, see 241-6001-310 *Preside MDM Server Reference Guide*.

Planning OA groups

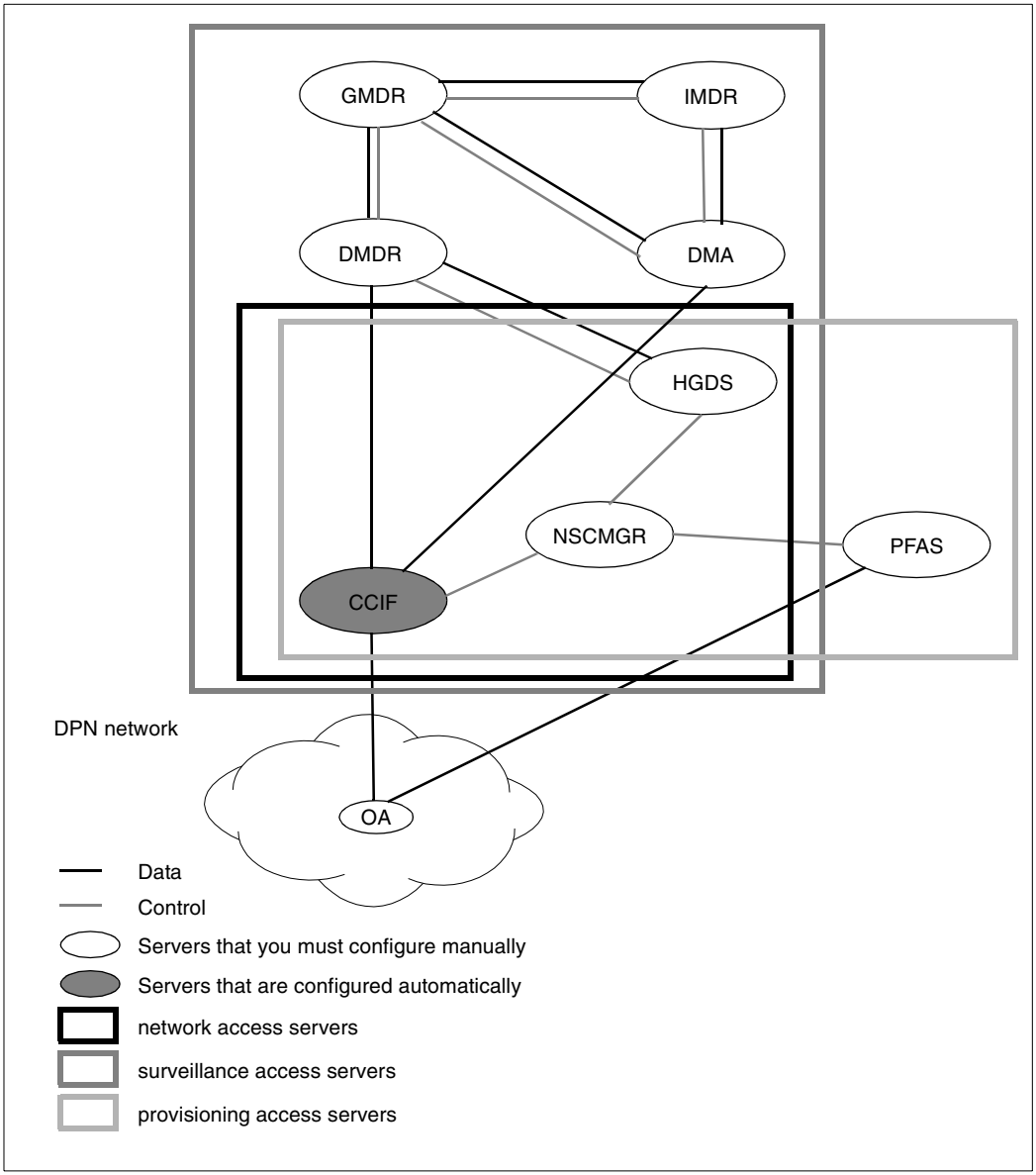
This section explains the reasons for setting up (OA) groups and provides guidelines to plan OA groups.

Access is required to OAs in the network for

- network access: to let an operator or an administrator log on to an OA from the Command Console and perform operations, such as provisioning or troubleshooting
- surveillance access: to let the DPN Management Data Router (DMDR) server log on to OAs to obtain alarms and status records (alarm-based surveillance information) from the DPN switches in the network

An OA group is a set of OAs that are defined as a group in the configuration files of the Preside Multiservice Data Manager (MDM) software. The following sections describe how to arrange OAs into groups for network and surveillance access.

Figure 3
Interdependencies of servers in networks containing DPN switches



Grouping OAs for network access

The concept of an Operations Agents (OA) group containing OAs that have a common NCS capability ID and password only applies to OAs used for surveillance access. A user at the Command Console may view a list of individual OAs to log into using separate NCS Capability IDs and passwords. A list of OA groups that a user can log into is not displayed on the Command Console.

To be managed by Preside Multiservice Data Manager (MDM) software all OAs must belong to an OA group. You must define at least one OA group for network access and this OA group must contain at least one OA as its member.

There is no advantage in creating more than one group of OAs for network access because the Command Console only displays the names of individual OAs you can log in to. Define only one OA group for network access, called for example ALLOAS, that has all OAs in the network as its members.

Grouping OAs for surveillance access

Grouping OAs for surveillance access requires an understanding of how surveillance information is obtained from the network. This section outlines how the network obtains surveillance information from the OAs in the network, and contains guidelines for grouping OAs.

How surveillance information is obtained from the network

The figure "How the filtering of surveillance information is set up" (page 99) shows the sequence followed to obtain alarms and status records information from the OAs in a surveillance group.

1 The DMDR server logs in to all of the OAs in a surveillance group with a common NCS capability ID and password that it obtains from arguments in its startup command.

2 The NCS on each OA authenticates the user id and password, and returns a customer network identifier (CNMID).

To perform its filtering function, a DMDR server needs to obtain alarms and status records from all devices monitored by all OAs in the surveillance group. For a DMDR server to receive them, the common

NCS capability ID and password must be defined on all OAs for it to be able to obtain the required surveillance information and cause all OAs to return a CNMID of 0.

When you are logged in, the DMDR server receives alarms and status records automatically from all of the OAs in the surveillance group.

3 To obtain surveillance information from a DMDR server, a client application, such as the GMDR server, registers with the DMDR server. This registration request also includes an NCS capability ID and password which can set up using the GMDR Administration tool.

4 The DMDR server passes the NCS capability ID and password contained in the registration request to one of the OAs in the surveillance group for authentication.

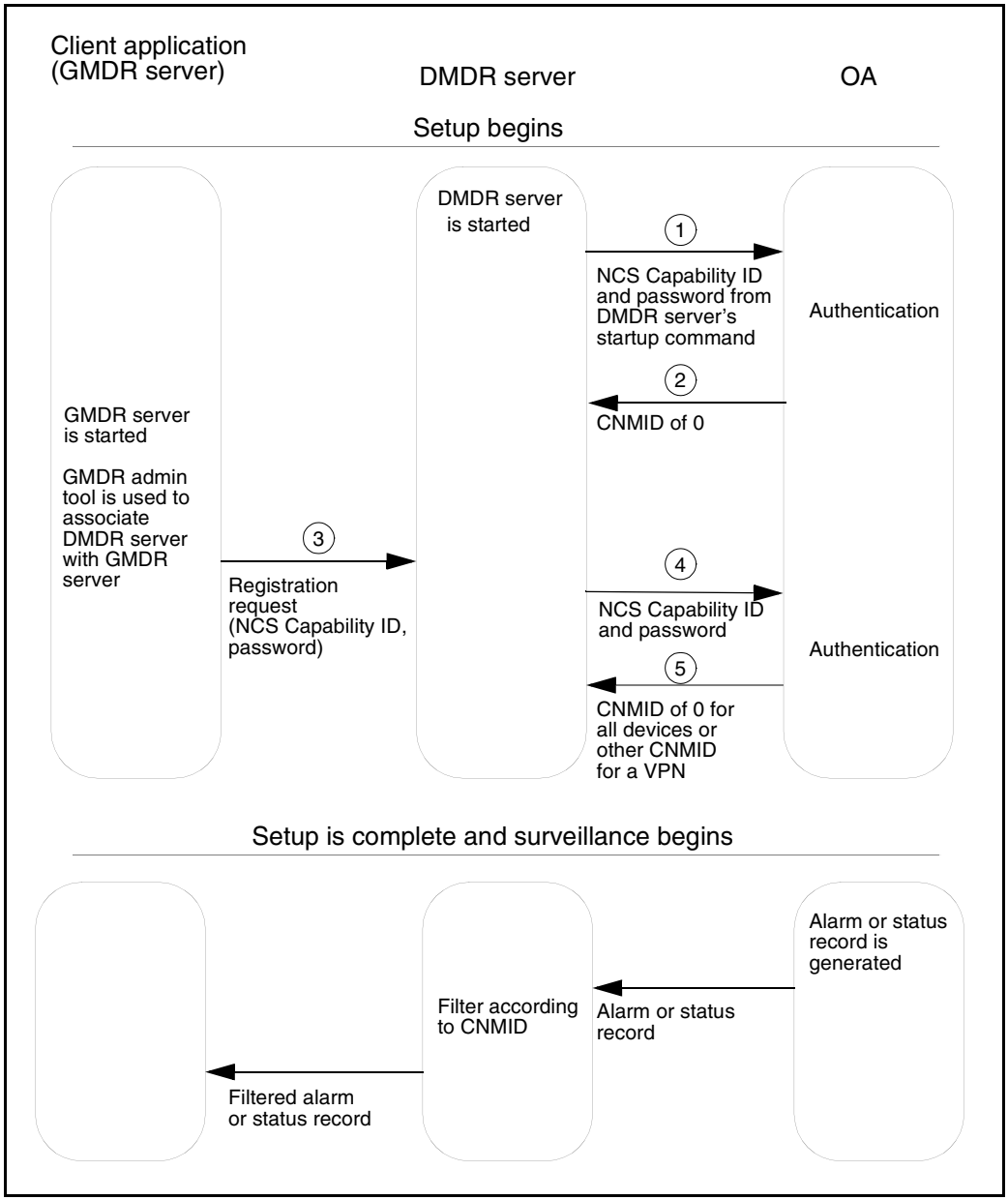
5 The NCS authenticates the NCS capability ID and password, and returns a customer network identifier (CNMID) to the DMDR server. The DMDR server stores the CNMID for filtering purposes.

The set up is now complete.

The OA then forwards surveillance information to the Preside Multiservice Data Manager workstation. The DMDR server filters the surveillance information for the client application (GMDR) according to client application's CNMID.

For a client application to receive surveillance information from devices monitored by the OAs in the surveillance group, the NCS capability ID and password provided by the client application must cause the OA to return a CNMID of 0. For virtual private networks (VPN) where a customer only receives information about the devices in the VPN, the NCS capability ID and password must cause the OA to return a CNMID other than 0, and one that is unique to the VPN.

Figure 4
How the filtering of surveillance information is set up



Guidelines for grouping OAs for surveillance access

The guidelines for the number of groups are as follows:

- You must define at least one surveillance group.
- You can define more than one surveillance group.

  Dividing OAs into several surveillance groups allows you to split up surveillance gathering into regions. This maintains the performance of surveillance gathering activities in large networks that contain many OAs. To manage surveillance on a regional basis, you could define surveillance groups that gathers alarms and surveillance information in the east network and the west network. This setup provides redundancy for surveillance gathering activities, if a DMDR server fails. A method for providing redundancy is described in "Adding DMDR server redundancy for surveillance access" (page 103).

The guidelines for NCS capability IDs and passwords are as follows:

- At least one common NCS capability ID and password must be defined on all OAs in a surveillance group. This common NCS capability ID and password must authenticate in the same way on all OAs. On all OAs it must be defined with the same scope and impact, and return the same CNMID.

  For security reasons, the minimum impact let the DMDR server obtain alarms and status records is passive.

- For the DMDR server to receive alarms and status records from all components monitored by the OAs in its surveillance group, the CNMID returned in response to the common NCS capability ID and password in a DMDR server's startup command must be CNMID 0.

- For a client application to receive alarms and status records from all components monitored by the OAs in a surveillance group, the CNMID returned in response to the client applications NCS capability ID and password must also be CNMID 0.

  For a client application which monitors components in a virtual private network to only obtains alarms and status records from the components that belong to the customer's VPN, the CNMID returned in response to the client application's NCS capability ID must be a CNMID other than 0. The CNMID must also be unique to the customer's VPN.

- When the DMDR server and the client application (GMDR) need to receive the information from the components monitored by all OAs in a surveillance group, you can use the same NCS capability ID and password for the DMDR server's startup command and for the surveillance access by the client application (GMDR). The CNMID returned by the NCS capability ID and password must be CNMID 0.

  When the client application obtains surveillance information for a VPN, and only needs to receive this information from the components in that VPN, the NCS capability ID and password provided by the client application cannot be the same as the NCS capability ID and password in the DMDR server's startup command. The NCS capability ID and password provided by the client application must be different, and must authenticate in the same way on all OAs on which it is defined The CMNID it returns must also be a CNMID other than 0.

The guidelines for DMDR servers are as follows:

- There must be one DMDR server for each surveillance group.
- The names of surveillance groups must be unique on a workstation. For example, you cannot have two groups called EAST on the same workstation. You can, however, duplicate the names of surveillance groups on different workstations.

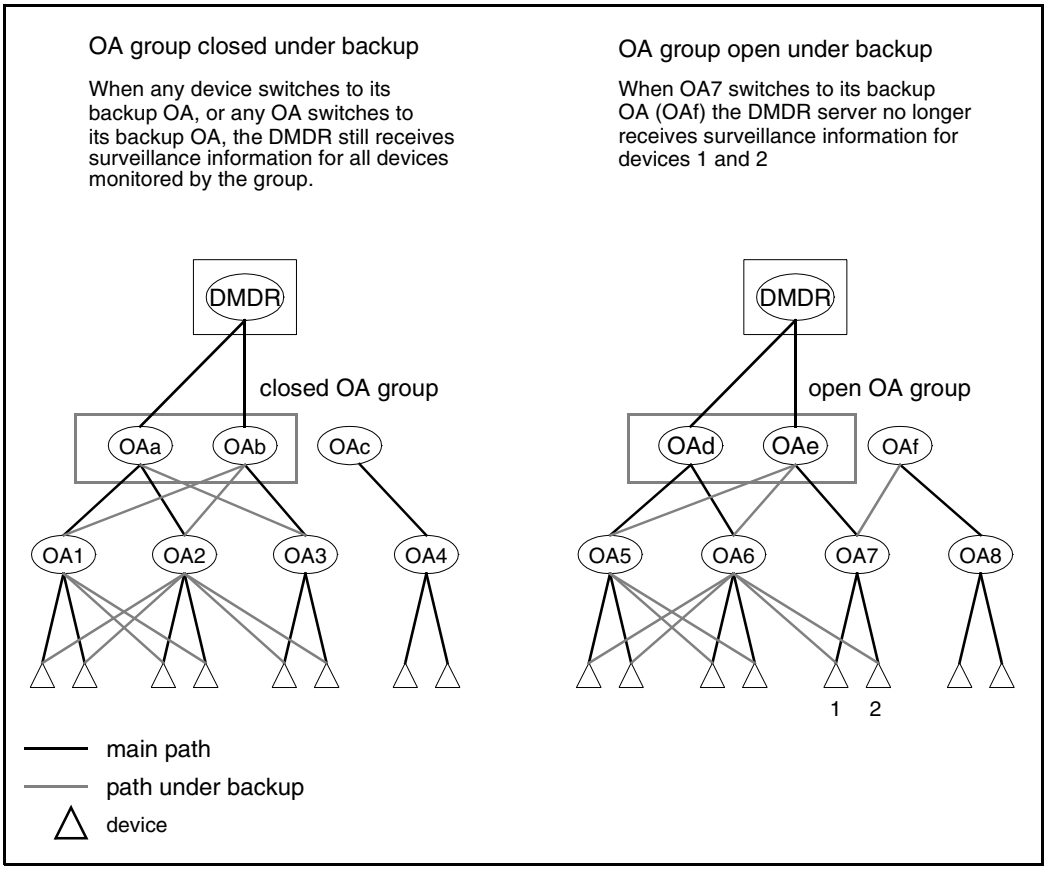
The guidelines for OA hierarchy are as follows;

- To ensure that a DMDR server continues to receive surveillance information when a device or OA switches to a backup OA, the group of OAs being accessed by the DMDR server must be closed under backup.

When any device or OA being monitored through the DMDR server switches to its backup OA, the server must still be able to obtain alarms and status records through the backup OA. For examples of OA groups, see the figure "Simple examples of OA groups that are closed and open under backup" (page 103)

- To keep the transfer of duplicate status records to a minimum, an OA and its backup OA should be at the same level in the OA hierarchy.
- Ensure that OAs you choose to form a surveillance group actually provide status records for all of the components to be surveilled. As status records percolate up an OA hierarchy, some of them may be filtered out at various OAs.
- All OAs that provide surveillance information to a surveillance group must be configured so that they have an Active Alarm List (AAL).

Figure 5
Simple examples of OA groups that are closed and open under backup



Adding DMDR server redundancy for surveillance access

If you have two or more Preside Multiservice Data Manager workstations that are connected by a LAN, you can add redundancy for surveillance gathering by discarding duplicate surveillance information that the GMDR server receives from DMDR servers.

To achieve redundancy, you can create duplicate surveillance groups on each workstation, and run a separate DMDR server on each workstation, as shown in the figure "DMDR server redundancy" (page 105). Then, using the GMDR Administration tool, you can set up the GMDR server on each workstation to

gather surveillance information from the DMDR servers on both workstations. See “Using the GMDR Administration tool” (page 423) for more information.

The GMDR server receives alarms from the DMDR servers on both workstations, and displays the alarms once. The GMDR server discards duplicate alarm notifications. If one of the DMDR servers fail, the GMDR server continues to receive surveillance data from its redundant DMDR server, without producing an impact on the fault tools that rely on this information.

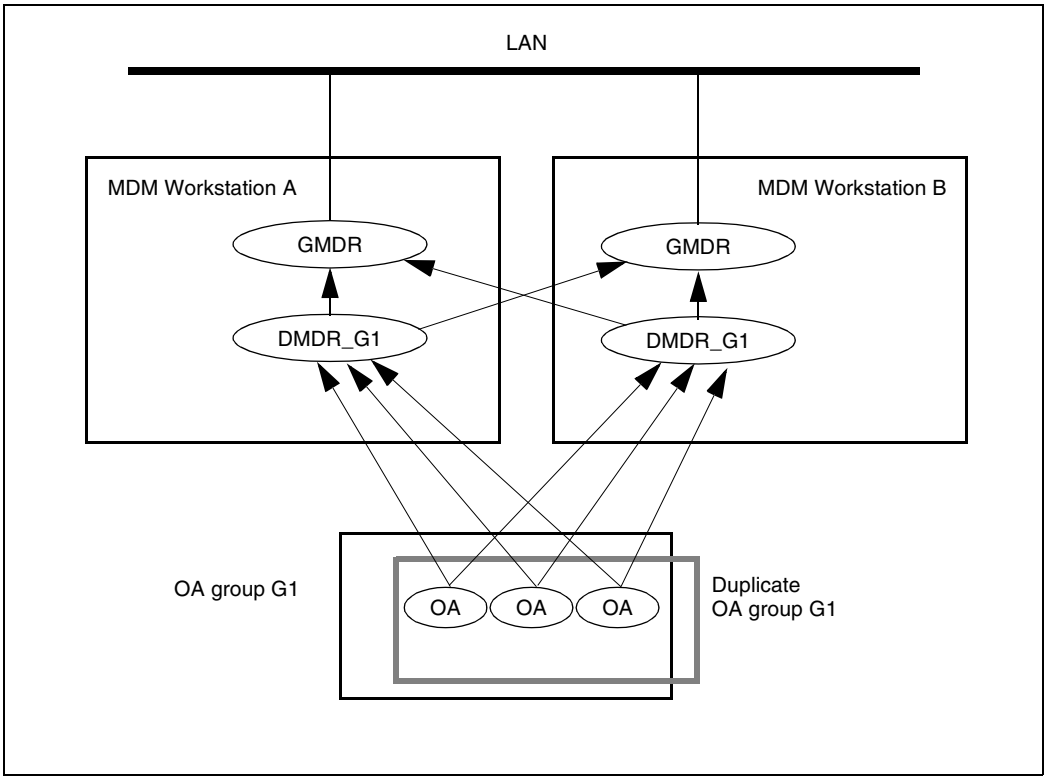
Example: Adding DMDR server redundancy

The figure “DMDR server redundancy” (page 105) shows a network containing three OAs that are monitored by two standalone Preside Multiservice Data Manager (MDM) workstations connected by a LAN. Identical groups called G1 are defined on both workstations. Separate DMDR servers are on each started workstation to retrieve surveillance data from the groups. The startup command for each DMDR server includes the server name DMDR-G1.

Using the GMDR Administration tool, each GMDR server is configured to receive surveillance data from the DMDR server on its own workstation and from the DMDR server on the redundant workstation through the LAN connection.

The GMDR server on workstation A discards duplicate data from the DMDR servers. If server DMDR_G1 fail on workstation A, the GMDR server on workstation A still gets the same surveillance data from the redundant DMDR server through its LAN connection to workstation B. Similar but opposite redundancy applies to the GMDR server on workstation B.

Figure 6
DMDR server redundancy



Distributing servers among workstations on a LAN

For small networks, all of the servers that support DPN network access, surveillance access, and provisioning access can run on the same workstation.

For medium and large networks, servers can be deployed among workstations connected by the same Ethernet LAN or by a WAN IP connection. This is can be done to

- distribute the workload over workstations to improve performance
- permit effective use of older, less powerful workstations with new more powerful workstations
- add redundancy and resiliency for fault management

The following guidelines apply to deploying the servers for DPN network access, surveillance, and provisioning access over multiple workstations:

- The following servers must run on a workstation that provides network access (a workstation that has an X25 link to the network): HGDS, NCSMGR, and PFAS.
- The DMDR server must run on the workstation that provides network access by default. You can run it on another workstation, provided that you specify the hostname of the workstation that runs the network access server, as part of the DMDR server's startup command. However doing so is not recommended because of the increase in network traffic (X.25 and IP) traffic that is entailed by this arrangement.
- The GMDR server can run on any workstation on the LAN, provided the workstation can handle traffic to the server. To ensure that the GMDR server receives surveillance information, you must use the GMDR Administration tool to specify the DMDR server (or servers) from which the GMDR server is to obtain the surveillance information.
- The DMA server can perform server surveillance, workstation surveillance, or global alarm clearing. For information on the DMA server, see 241-6001-310 *Preside MDM Server Reference Guide*.
  - — If the DMA server performs workstation surveillance or global alarm clearing, it must reside on a workstation that provides network access.
  - — If the DMA server only performs workstation server surveillance, it can reside on any workstation, but its startup command must indicate the location of the IMDR server to which it is providing the workstation's server alarms.

Task list for configuring servers

Use the following procedure to locate the tasks needed to configure servers to support DPN network access, surveillance, and provisioning access. For initial installations, you can use this procedure, or you can use the Preside Multiservice Data Manager (MDM) Software Configuration tool, as described in 241-6001-100 *Preside MDM Installation*.

Before you begin this procedure, you must have installed and configured SunLink X.25 software on the workstation.

Procedure steps

1. Plan the OA groups for DPN network access and DPN surveillance. See "Planning OA groups" (page 94).
2. Configure the NCS hierarchy to support DPN surveillance. See "Configuring the NCS hierarchy for surveillance" (page 107).
3. Create the OA groups. See "Defining the OA groups and OA members" (page 108).
4. Configure and start the NCSMGR, HGDS, DMDR, GMDR, DMA, and PFAS servers. See "Configuring and starting the servers" (page 115).

Configuring the NCS hierarchy for surveillance

1. Read "Grouping OAs for surveillance access" (page 97).
2. Choose the level in the OA level in the hierarchy at which the DMDR server is going to connect. Assume that all the OAs at the level you selected are going to form one surveillance group.
3. Ensure that each OA and its backup OA are at the same level in the NCS hierarchy. Redefine the structure of the hierarchy if necessary.
4. Ensure that an Active Alarm List (AAL) is configured on each OA in the surveillance group.
5. Ensure that at least one common NCS capability ID and password is assigned on all OAs in the group, and that all OAs authenticate it in the same way.
6. Verify that the OAs at the level you selected to form the surveillance group are closed under backup by looking at each device and OA and pretend that it is using its backup OA. The DMDR server should still get alarms and status records from the device or OA. If not, add or remove OAs from the group until this criteria is met. See the figure, "Simple examples of OA groups that are closed and open under backup" (page 103).
7. If a network is large and it contains many OAs, you can split surveillance gathering between DMDR servers on different workstations to preserve surveillance gathering performance. You must verify that all the OAs are closed under backup.

You are now ready to create OA groups. See "Defining the OA groups and OA members" (page 108).

Defining the OA groups and OA members

This section describes how to define the DPN-100 network configuration on a Preside Multiservice Data Manager (MDM) host using the Host Group Administration tool.

The following topics are discussed in this section

Launching the Host Group Administration tool

Launch the Host Group Administration tool using one of these methods.

Note: The Host Group Administration tool does not allow simultaneous administration sessions.

Access from the MDM window

1 From the Preside Multiservice Data Manager (MDM) main window, select **System -> Administration -> Host Group Administration**.

Note: If the userID used to launch MDM is not the userID **root**, this menu item is not available for selection.

The Host Group Administration window opens.

If the file /opt/MagellanNMS/cfg/HGDS.cfg exists, the contents are displayed.

Access from the command line

1 From a UNIX xterm, as the userID root, type

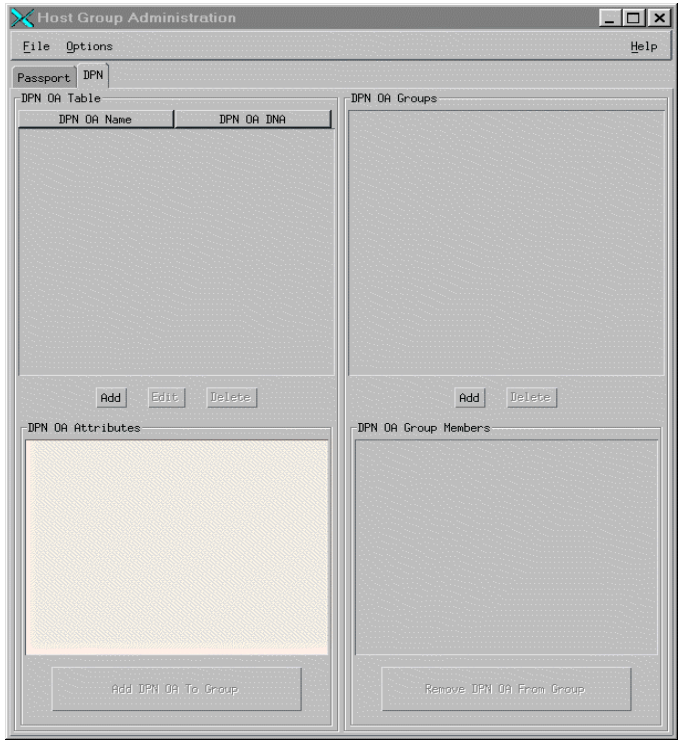
```
/opt/MagellanNMS/bin/hgadmin &
```

The Host Group Administration window opens.

If the file /opt/MagellanNMS/cfg/HGDS.cfg exists, the contents are displayed.

Figure "Host Group Administration window" (page 109) shows an example of this window.

Figure 7
Host Group Administration window



Loading and merging a remote HGDS file

1. Select the **DPN** tab.
2. Select **File -> Load and Merge Remote Host Group File**.

   The **Load and Merge Remote Host Group File** dialog opens.
3. Type the name of the remote MDM host in the data entry box **Remote Workstation**.
4. Type a userID to access the remote MDM host in the data entry box **User ID**.
5. Type a password for the User ID in the data entry box **Password**.
6. Click **OK**.

   The Load and Merge Remote Host Group File dialog closes.

The remote HGDS file information is displayed.

If a local HGDS file is currently displayed, the Host Group Administration tool merges the HGDS information from the remote host with the HGDS information on the local host. Merge conflicts are identified. You are provided the option of accepting the new information or retaining the current window contents.

Clearing the window data

1. Select the **DPN** tab.
2. Select **File -> Clear All Data**.

   The **Clear All Data** dialog opens.
3. Click **OK**.

   The Clear All Data dialog closes.

   All of the Host Group Administration window panels are cleared of data.

Adding a DPN OA

1. Select the **DPN** tab.
2. Click **Add** below the panel **DPN OA Table**
   (or select Options -> DPN OA Table Options -> Add DPN OA).

   The **Add New DPN OA** dialog opens.
3. Type the OA member name in the data entry box **OAMember**.
4. Type the Workstation Management Data Interface (WS_MDI) in the data entry box **NAME**.
5. Type the Data Network Address (DNA) used to access the WS_MDI in the data entry box **DNA**.
6. Type the Closed User Group (CUG) to which the WS-MDI belongs in the data entry box **CUG**.
7. Type the default size of data packets transmitted between the Preside Multiservice Data Manager (MDM) host and the WS-MDI.in the data entry box **PktSz**.

   The packet size is one of: 128, 256, or 512. The default is 256.
8. X.75 links are used to interconnect two packet network, either public or private.

   If the connection between the MDM host and the OA passes through an X.75 link type **Y** in the data entry box **X75**.

If the connection between the MDM host and the OA does not pass through an X.75 link type **N** in the data entry box **X75**.

9 Type the Recognized Private Operating Agency (RPOA) that owns the X.75 link to the WS-MDI in the data entry box **RPOA**.

This data entry box can only be updated if an X75 link was specified in step 8.

10 Click **OK**.

The Add New DPN OA dialog closes.

The new DPN OA is added to the DPN OA Table.

Changing a DPN OA definition

1 Select the **DPN** tab.

2 Select the DPN OA in the **DPN OA Tabl**e.

3 Click **Edit** below the panel DPN OA Table
(or select Options -> DPN OA Table Options -> Edit OA).

The **Edit DPN OA** dialog opens.

4 Type the OA member name in the data entry box **OAMember**.

5 Type the Workstation Management Data Interface (WS_MDI) in the data entry box **NAME**.

6 Type the Data Network Address (DNA) used to access the WS_MDI in the data entry box **DNA**.

7 Type the Closed User Group (CUG) to which the WS-MDI belongs in the data entry box **CUG**.

8 Type the default size of data packets transmitted between the Preside Multiservice Data Manager (MDM) host and the WS-MDI.in the data entry box **PktSz**.

The packet size is one of: 128, 256, or 512. The default is 256.

9 X.75 links are used to interconnect two packet network, either public or private.

If the connection between the MDM host and the OA passes through an X.75 link type **Y** in the data entry box **X75**.

If the connection between the MDM host and the OA does not pass through an X.75 link type **N** in the data entry box **X75**.

10 Type the Recognized Private Operating Agency (RPOA) that owns the X.75 link to the WS-MDI in the data entry box **RPOA**.

This data entry box can only be updated if an X75 link was specified in step 8.

11 Click **OK**.

The Edit DPN OA dialog closes.

The updated DPN OA information is replaced in the DPN OA Table and in all of the DPN OA groups of which it is a member.

Removing a DPN OA

1 Select the **DPN** tab.

2 Select the DPN OA in the **DPN OA Table**.

3 Click **Delete** below the panel DPN OA Table
(or select Options -> DPN OA Table Options -> Delete DPN OA).

The **Delete DPN OA** dialog opens.

4 Click **OK**.

The Delete DPN OA dialog closes.

Note: The DPN OA is removed from the DPN OA Table and from all of the DPN OA groups of which it is a member.

Displaying DPN OA attributes

1 Select the **DPN** tab.

2 Select the DPN OA in the **DPN OA Table**.

The following DPN OA attributes are displayed in the **DPN OA Attributes** panel:

- OA member name
- Workstation Management Data Interface (WS_MDI)
- Data Network Address (DNA)
- Closed User Group (CUG)
- the default size of data packets
- the X75 setting
- the Recognized Private Operating Agency (RPOA)
- DPN OA groups that include this DPN OA as a member

Adding a DPN OA group

1. Select the **DPN** tab.
2. Click **Add** below the panel **DPN OA Groups** panel
   (or select Options -> DPN OA Group Options -> Add DPN OA group).

   The **Add New DPN OA Group** dialog opens.
3. Type the DPN OA group name in the data entry box **DPN OA Group Name**.
4. Click **OK**.

   The Add New DPN OA Group dialog closes.

   The new DPN OA group is added to the DPN OA Groups panel.

Adding a DPN OA to a DPN OA group

1. Select the **DPN** tab.
2. Select the DPN OA in the **DPN OA Table**.
3. Select the DPN OA group in the **DPN OA Groups** panel.

   The button **Add DPN OA <DPN OA> to group <group_name>** below the **DPN OA Attributes** panel is activated.
4. Click **Add DPN OA <DPN OA> to group <group_name>**
   (or select Options -> DPN OA Table Options -> Add DPN OA to Group).

   The DPN OA is added to the group and is displayed in the **DPN OA Group Members** panel.

   There is no restrictions on the number of DPN OAs in a group.

Removing a DPN OA from a DPN OA group

1. Select the **DPN** tab.
2. Select the DPN OA group in the **DPN OA Groups** panel.

   The DPN OAs that belong to the selected group are displayed in the **DPN OA Group Members** panel.
3. Select the DPN OA in the **DPN OA Group Members** panel.

   The button **Remove DPN OA <DPN OA> from group <group_name>** below the **DPN OA Group Members** panel is activated.

4 Click **Remove DPN OA <DPN OA> from group <group_name>** (or select Options -> DPN OA Group Options -> Remove DPN OA from Group).

The **Remove DPN OA from group** dialog opens.

5 Click **OK**.

The Remove DPN OA from group dialog closes.

The DPN OA is removed from the group and is no longer displayed in the **DPN OA Group Members** panel.

Note: Removing a DPN OA from a group does not remove the DPN OA from other groups and does not remove the DPN OA from the DPN OA Table.

Removing a DPN OA group

1 Select the **DPN** tab.

2 Select the DPN OA group in the **DPN OA Groups** panel.

The DPN OAs that belong to the selected group are displayed in the **DPN OA Group Members** panel.

3 Click **Delete** below the panel DPN OA Groups panel (or select Options -> DPN OA Group Options -> Delete Group).

The **Delete DPN OA Group** dialog opens.

4 Click **OK**.

The Delete DPN OA Group dialog closes.

The DPN OA group is no longer displayed in the **DPN OA Groups** panel.

Note: Removing a group does not remove the group members from other groups and does not remove the group members from the DPN OA Table.

Saving the HGDS file

1 Select the **DPN** tab.

2 Select **File -> Save**.

The **Save Host Group File** dialog opens.

3 If there is a DPN entry that does not belong to a group, you are prompted whether you wish to keep this DPN.

4 Click **Keep** or if there is more than one DPN that you wish to keep, click **Keep All**.

5 Click **OK**.

The Save Host Group File dialog closes.

The current version of the file /opt/MagellanNMS/cfg/HGDS.cfg is saved with a time-stamped suffix.

The contents of the Host Group Administration window are written to the file /opt/MagellanNMS/cfg/HGDS.cfg on the local Preside Multiservice Data Manager (MDM) host and the file is saved.

The HGDS.cfg data is loaded with the HGDS the next time the HGDS is started.

Note: The Host Group Administration tool will not allow the file HGDS.cfg to be updated if mandatory data is missing or is incorrect.

6 If the HGDS is currently running, the **Reload HGDS Configuration** dialog opens with the prompt

```
Do you want to signal the related MDM servers to reload
the HGDS configuration now?

Click Yes to restart the servers.

Click No to restart the servers at another time using
the Preside MDM Server Administration (SVMADM) tool.
```

Closing the Host Group Administration tool

1 Select the **DPN** tab.

2 Select **File -> Exit**.

If no updates have been made to the Host Group Administration window contents, the **Host Group Administration** window closes.

If updates have been made to the Host Group Administration window contents, the **Save Host Group File** dialog opens (see “Saving the HGDS file” (page 114)).

Configuring and starting the servers

Use the following procedure to configure and start the servers required to support DPN network access, surveillance, and provisioning access.

For initial installations, use this procedure, or you can use the Preside Multiservice Data Manager (MDM) Software Configuration tool, as described in 241-6001-100 *Preside MDM Installation*.

1 If you have several workstations running MDM software that are connected to the same LAN, read the following sections before you begin:

- "Adding DMDR server redundancy for surveillance access" (page 103)
- "Distributing servers among workstations on a LAN" (page 105)

2 Log in as root.

Note: The root account must be set up to run MDM software as described in "Setting up the root account to run MDM software" (page 62).

3 Using the Server Administration tool, set up the NCSMGR, HGDS, GMDR, IMDR, DMA and PFAS servers to start up automatically when the workstation is rebooted. See "Adding a new server" (page 367).

See 241-6001-310 *Preside MDM Server Reference Guide* for the server startup commands:

- NCSMGR
- HGDS
- GMDR
- IMDR
- DMA

For more information on the DMA server, see the following:

"Configuring DPN alarm clearing" (page 233) describes how to configure the DMA server to support global alarm clearing

"Configuring server alarm distribution and workstation status probing" (page 261) describes how to configure DMA for server surveillance and workstation surveillance.

- PFAS

If you are going to be performing software downloading, start a second instance of the PFAS server using the -n swdld option in the PFAS server's startup command.

4 Using the Server Administration tool, create one DMDR server for each OA group for network access and one DMDR server for each surveillance group. Ensure that you set them to start automatically when the workstation is rebooted.

For each DMDR server, include the following parameters in its startup command:

-g <OA group name> -c <NCS Capability ID> -p <password>

where:

<OA group name>

is the name of the surveillance group that the DMDR server monitors

<NCS Capability ID> and <password>

are the NCS capability ID and password for the common account that the DMDR server uses to obtain surveillance information from the OAs in the surveillance group

For a full set of the parameters that can be used in the startup command for the DMDR server, see 241-6001-310 *Preside MDM Server Reference Guide*.

5 Using the GMDR Administration tool, configure GMDR to access the servers you created to obtain surveillance information.

- For each DMDR server, you must provide

Server Name the name of the surveillance data (DMDR) server in the form DMDR_<group_name>

Host Name the host name or the IP address of the workstation on which the DMDR server is running

User/CapabilityID and Password the NCS capability ID and password to be used by the GMDR server for authentication upon connection to the OAs in the surveillance group

- For a subordinate GMDR server you must provide

Server Name the name of the subordinate GMDR server in the form GMDR or GMDR_<service name>

Host Name the host name or the IP address of the workstation on which the GMDR server is running

User/CapabilityID and Password not required

- For each IMDR server you must provide

Server Name the name of the IMDR server in the form IMDR or IMDR_<service name>

Host Name the host name or the IP address of the workstation on which the IMDR server is running

User/CapabilityID and Password not required

- For a DMA server that is providing global alarm clearing for DPN, you must provide:

  `Server Name` DMASERVER

  `Host Name` localhost or the IP address of the workstation on which the GMDR server is running

  `User/CapabilityID and Password` not required

  See "Configuring GMDR to access the surveillance servers" (page 450) for the instructions to complete this task.

Configuring the servers to support DPN network access, surveillance, and provisioning access is complete. For a list of the servers that can be configured to support other functions, see "Roadmap to the MDM servers" (page 81).

Setting up special processing of alarms

Use the procedure in this section to set up a DMDR server to perform special processing treatments on alarms received from the NCS.

Some alarms require special processing for reasons, such as

- the DPN switch associates a special meaning to the fault code. For example, for Dial Backup Network Link (DBNL) deactivation alarms.
- customer management practices require that an alarm be assigned a different severity than the one set by the DPN switch

The DMDR server provides a method to use the information stored in an alarm exceptions file to perform special processing on incoming alarms. By default, the DMDR server uses the information stored in alarm exceptions file /opt/MagellanNMS/cfg/DMDRAlarmExcep.cfg. For the DMDR server to use an alarm exceptions file other than the default, start the DMDR server with the argument -e <exceptions file name>, where <exceptions file name> is the absolute path name for the alarm exceptions file.

For information about the structure of the entries in the alarm exceptions file, see the section on configuring the file /opt/MagellanNMS/cfg/DMDRAlarmExcep.cfg in 241-6001-310 *Preside MDM Server Reference Guide*.

Procedure steps

1 Log in as root.

Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in “Setting up the root account to run MDM software” (page 62).

2 Using a UNIX editor such as vi, edit the contents of the alarm exceptions file so that it performs the special alarm treatment you require.To configure the file /opt/MagellanNMS/cfg/DMDRAlarmExcep.cfg, see 241-6001-310 *Preside MDM Server Reference Guide*.

3 Using the Server Administration tool, stop the DMDR server.

To stop a server using the Server Administration tool, see “Logging out as administrator and accessing view mode” (page 379).

4 To use an alarm exceptions file other than the default, edit the startup command for the DMDR server with the Server Administration tool so that the startup command includes the absolute path name of your alarm exceptions file. To use the default alarm exceptions file (/opt/MagellanNMS/cfg/AlarmExcepts.cfg), skip this step.

To edit a server with the Server Administration tool, see “Editing a server” (page 377).

5 Using the Server Administration tool, restart the DMDR server.

Preloading CNMIDs to filter status records

Use the procedure in this section to preload CNMIDs into a file to provide a DMDR server with the means to begin filtering status records from components that belong to a customer’s virtual private network (VPN) without first having to receive alarms from those components.

To obtain surveillance information from a DMDR server, a client application such as the GMDR server registers with the DMDR server. This registration request includes an NCS capability ID and a password. These parameters are passed on to an OA in the surveillance group for authentication. The NCS authenticates the NCS capability ID and password, and returns a customer network identifier (CNMID) to the client application.

For client applications that receive surveillance information from all components monitored by the OAs in a surveillance group, the NCS capability ID and password returns a CNMID of 0. For virtual private

networks, in which a customer only gets information about the components that belong to the VPN, the NCS capability ID and password return a CNMID other than 0, and that is unique to the customer's VPN.

Once DMDR has the CNMID, it begins filtering surveillance information based on that CNMID. There are two types of surveillance information: status records and alarms. Alarms received from the OAs in the group include a CNMID as part of the alarm message, but status records do not.

If an alarm arrives from a component before a status record arrives from that same component, the DMDR server extracts the CNMID and the component identifier from the alarm message and stores them. When a subsequent status record arrives from the same component, the DMDR server uses the component identifier contained in the status record to look up the corresponding CNMID and uses that CNMID to filter the status record and provide it to the correct client application.

If a status record arrives from a component before an alarm arrives from that same component, the DMDR server cannot determine what CNMID to use for filtering because the status record does not contain a CNMID. By default, DMDR server assumes that the CNMID is 0 and passes the status record on to client applications. For client applications that surveil all components in the network (their NCS capability ID and password returns a CNMID of 0) this produces a slight delay. However, for client applications whose CNMID is not 0, which is the case for components in a VPN, this presents a difficulty. In a network that contains two or more VPNs all client applications receive the status record, whether or not the component belongs to the VPN.

To overcome any delays and the possibility of a status record being distributed to all client applications, in all VPNs, the DMDR server uses information contained in a CNMID file. You can preload this file with information that maps CNMIDs to their corresponding component identifiers.

By default, the CNMID file is /opt/MagellanNMS/cfg/DMDRCnmid.cfg. To get a DMDR server to use a CNMID file other than the default, you must start the DMDR server with the argument -C <CNMID file name>, where <CNMID file name> is the absolute path name for the CNMID file.

For information about the structure of the entries in the CNMID file, see 241-6001-310 *Preside MDM Server Reference Guide*. Refer to the section to configure the file /opt/MagellanNMS/cfg/DMDRCnmid.cfg.

Setting up CNMIDs for VPNs

1 Log in as root.

Note: The root account must be set up to run Preside Multiservice Data Manager(MDM) software as described in “Setting up the root account to run MDM software” (page 62).

2 Using a UNIX editor such as vi, edit the contents of the CNMID file to allow it to map components to CNMIDs.

For a description of the structure of the alarm exceptions file, and the fields in the file, see 241-6001-310 *Preside MDM Server Reference Guide*. Refer to the section to configure the file /opt/MagellanNMS/cfg/DMDRCnmid.cfg.

3 Using the Server Administration tool, stop the DMDR server.

To stop a server using the Server Administration tool, see “Logging out as administrator and accessing view mode” (page 379).

4 If you are not using the default CNMID file (/opt/MagellanNMS/cfg/DMDRCnmid.cfg), use the Server Administration tool to edit the startup command for the DMDR server.

To edit a server with the Server Administration tool, see “Editing a server” (page 377).

Using the Server Administration tool, restart the DMDR server.

Chapter 8
Configuring MDM servers for Passport switches

This section contains the instructions to configure the Preside Multiservice Data Manager (MDM) servers to support the three following basic functions for networks that contain Passport (Passport) switches:

- network access: allows users to log on to Passport switches and enter commands to perform operations such as troubleshooting
- surveillance access: allows the MDM software to gather surveillance information from Passport switches
- provisioning access: allows users to configure Passport switches and upload Service Data Descriptions (SDD) to the workstation

For information about servers other than those that support these basic functions, and for references to the instructions for configuring them, see "Roadmap to the MDM servers" (page 81).

See the following sections for more information:

- "Servers required to support Passport network access, surveillance, and provisioning access" (page 124)
- "Groups of Passport for network access" (page 127)
- "Reasons for Passport groups and guidelines for setting them up" (page 125)
- "Groups of Passport for network access" (page 127)

- "Guidelines to group Passport switches for surveillance access" (page 131)
- "FMDR server redundancy for surveillance access" (page 134)
- "Configuring servers for network access, surveillance access, and provisioning access" (page 136)
- "Defining the groups and hosts" (page 141)
- "Defining Passport hosts and groups with scripts" (page 147)
- "Deleting a switch" (page 164)

Servers required to support Passport network access, surveillance, and provisioning access

The figure "Interdependencies of servers that support basic functions, networks containing Passport switches" (page 126) shows the servers that need to be configured to support the basic functions of Passport (Passport) network access, surveillance access, and provisioning access, and it illustrates the dependencies between these servers.

The servers that need to be configured to support these functions are as follows:

- Passport Communication Manager (FDTM)
- Host Group Directory Server (HGDS)
- FMIP Management Data Router (FMDR)
- Data Manager Agent (DMA)
- General Management Data Router (GMDR)

For detailed descriptions of these servers, see 241-6001-310 *Preside MDM Server Reference Guide*.

Reasons for Passport groups and guidelines for setting them up

A Passport (Passport) group is a set of Passport switches that share a least one common user ID and password for performing a common management role such as network access, surveillance, or provisioning, and which is defined as a group in the configuration files of the Preside Multiservice Data Manager (MDM) software.

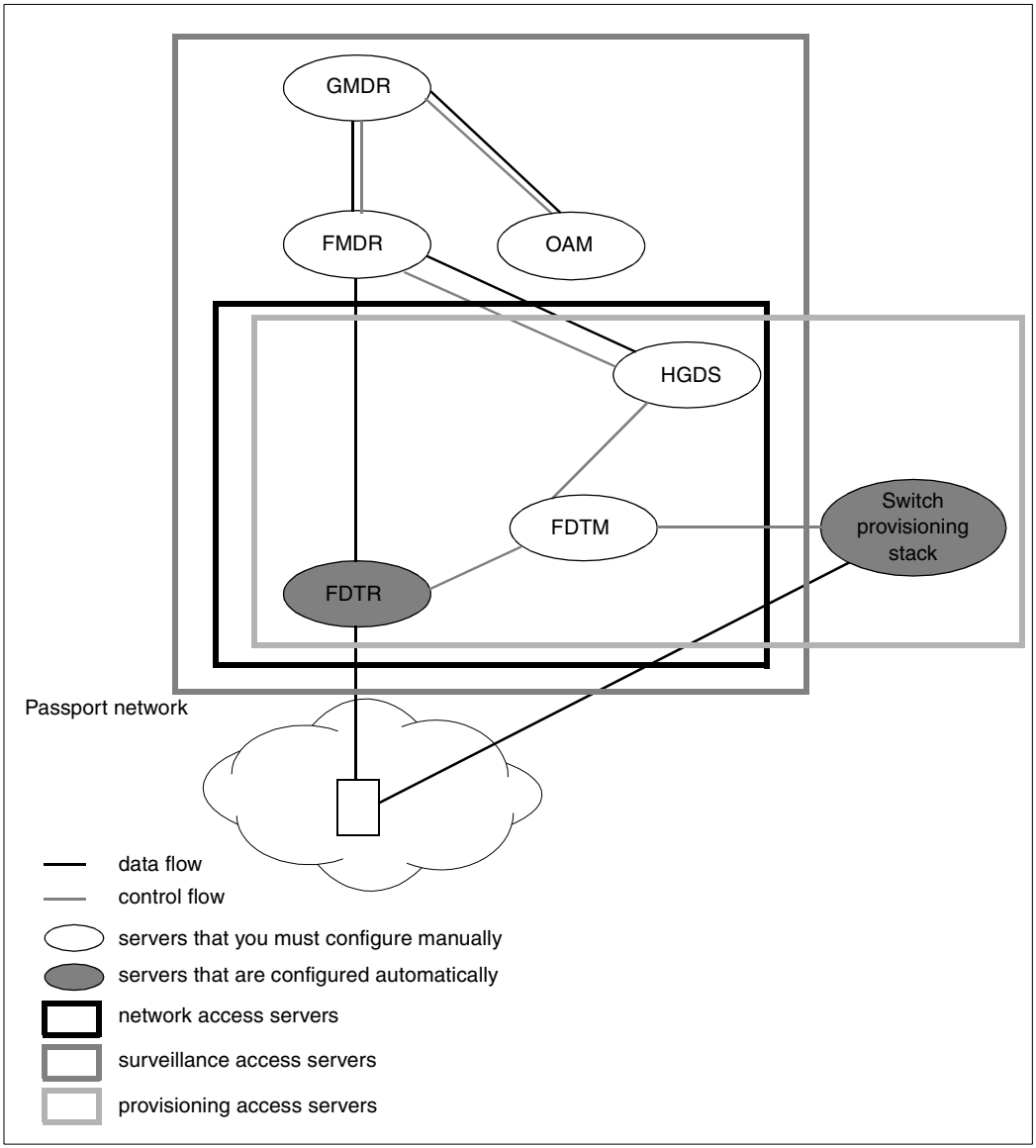
Because the user ID defines the administrative capability (scope and impact) of a user, you can use groups to control access to the administrative functions on a switch. When a user logs on with a user ID, the user has access to all of the switches defined in the group and can perform any administrative functions allowed by the administrative capability of the user ID.

Passport groups are therefore used to control access to the network. Access is required for two main reasons:

- network access: to allow an operator or administrator to log onto a switch with the Command Console or to perform provisioning operations
- surveillance access: to allow the FMIP Management Data Router (FMDR) server to log on to a group of switches and obtain surveillance information

A Passport switch can belong to several groups, so that it can be accessed by different user IDs for different tasks. For example, the same switch can be accessed by an operator for surveillance, and by a network administrator for provisioning.

Figure 8
Interdependencies of servers that support basic functions, networks containing Passport switches



Groups of Passport for network access

You can define groups that allow users, such as operators or administrators, to access all of the Passport (Passport) switches in a group of switches and perform operations such as provisioning or troubleshooting. When a user logs on to a group with a user ID defined on all switches in the group, the user has access to all of the switches and can perform all of the functions that the scope and impact of the user ID allows.

Guidelines for grouping switches to provide network access are as follows:

- At least one common user ID and password must be defined on all the switches in a group for performing network access functions. This common user ID and password must authenticate in the same way on all the switches in the group. That is, the user ID and password must be defined with the same scope and impact, and all of the switches must return the same CNMID.
- You are not limited to defining just one common user ID and password. You can define several common user IDs and passwords on the switches in a group, and dedicate each to a different function. For example, one user ID could have access privileges for provisioning, while another could have access privileges for performing maintenance functions. However, any common user ID and password must authenticate in the same way on all of the switches in the group.
- A switch can be included in more than one group.

For an example of grouping switches, see “Do not create groups containing more than 60 switches for surveillance access.” (page 132).

Grouping Passport for surveillance access

To use the guidelines in this section to group Passport (Passport) switches for surveillance access, you first require an understanding of how surveillance information is obtained from the network. This section is therefore divided into two parts:

- “At startup time” (page 128)
- “At run time” (page 129)

At startup time

To obtain surveillance information the following sequence occurs. See the figure "How the filtering of surveillance information is set up" (page 130) for an illustration of this sequence.

1 The FMDR server on a Preside Multiservice Data Manager workstation logs in to all of the switches in a surveillance group with a common user ID and password that it obtains from arguments in its startup command.

2 Each switch authenticates the user ID and password, and returns a customer network identifier (CNMID).

To perform its filtering function, an FMDR server needs to receive surveillance information from all of the devices on all of the switches in the surveillance group. For an FMDR server to receive the information, the common user ID and password must be defined on all the switches such that is has a scope impact sufficient to obtain the required surveillance information, and that it causes all the switches to return a CNMID of 0.

Once logged in, the FMDR server is ready to receive alarms and status records automatically from all of the switches in the surveillance group.

3 To obtain surveillance information from an FMDR server, a client application, such as the GMDR server, registers with the FMDR server. This registration request also includes a user ID and password, which can set up by means of the GMDR Administration tool.

4 The FMDR server passes the user ID and password contained in the registration request to one of the switches in the surveillance group for authentication.

5 The switch authenticates the user ID and password, and returns a customer network identifier (CNMID) to the FMDR server. The FMDR server stores this CNMID for filtering purposes.

6 The FMDR initiates a state walk-through to obtain the states of all components that it surveils. It also contains information about links that terminate on TRK components and DPNGATE components and sets the initial state of these links to in-service.

Note: The Network Model Server determines and sets the actual states of these links based on the states of components at both ends of each link.

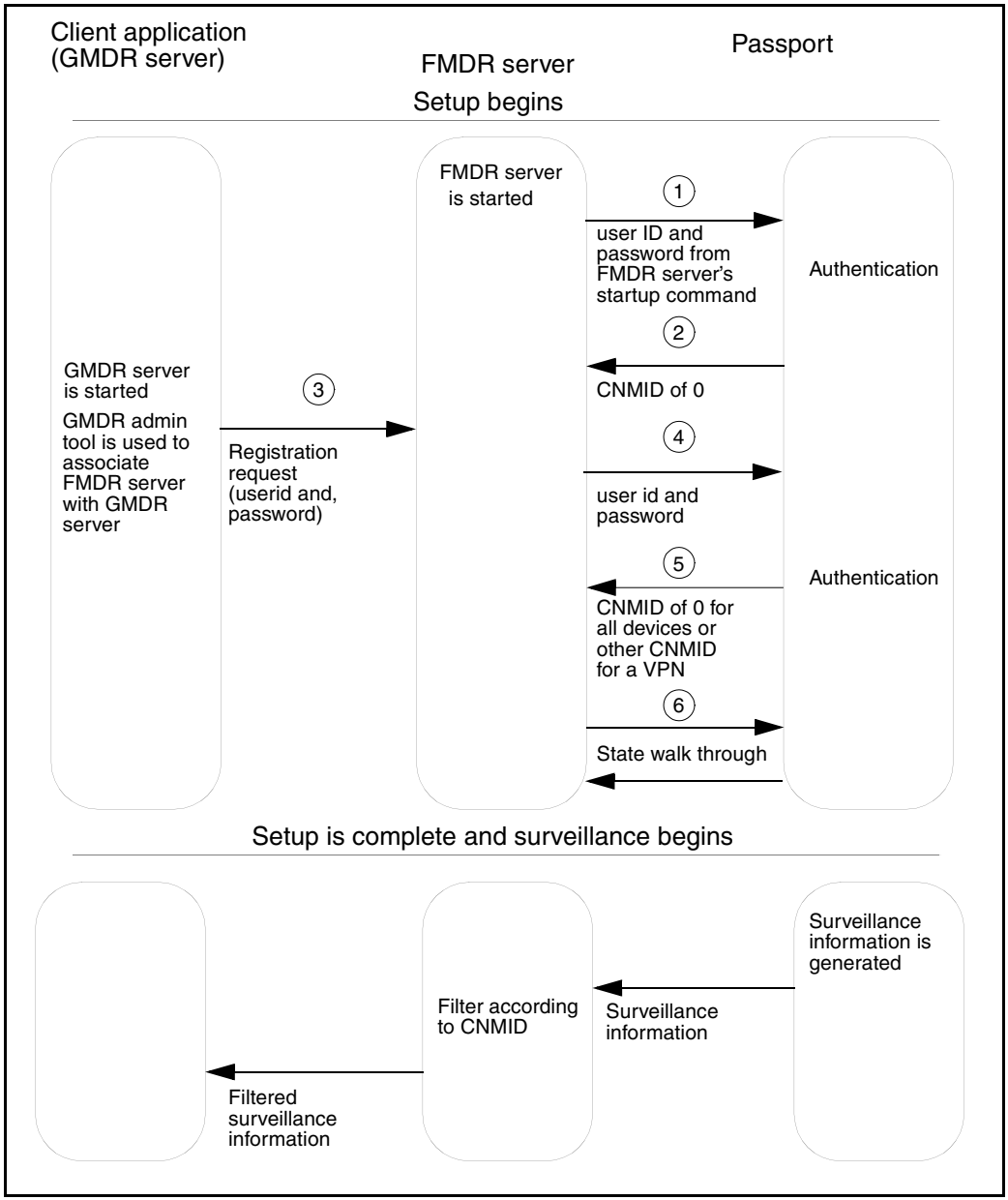
The setup is now complete.

At run time

When setup is complete and a switch forwards surveillance information to the MDM workstation, the FMDR server filters the surveillance information for the client application (GMDR) according to client application's stored CNMID.

For a client application (GMDR) to be able to receive surveillance information from all devices on all switches in the surveillance group, the user ID and password provided by the client application (GMDR) must cause the switch to return a CNMID of 0. For virtual private networks (VPN), in which a customer should only receive information about the devices in the VPN, the user ID and password must cause the switches to return a CNMID other than 0, and that is unique to the customer's VPN.

Figure 9
How the filtering of surveillance information is set up



Guidelines to group Passport switches for surveillance access

Guidelines to group Passport (Passport) switches for surveillance access are as follows:

User IDs and passwords

- All switches in a surveillance group must support at least one common user ID and password for surveillance purposes. This common user ID and password must authenticate in the same way on all switches. That is, it must have the same scope and impact, and must return the same CNMID.
- For security reasons, a common user ID and password for surveillance purposes must have the lowest possible scope and impact that still allows the user to obtain surveillance information. The scope to do this is Network and the impact is Passive.
- To ensure that an FMDR server receives surveillance information from all components in its group, the CNMID returned in response to the user ID and password in the FMDR server's startup command must be CNMID 0, also known as netman.
- To ensure that a client application (GMDR) receives surveillance information from all components in a surveillance group, the CNMID returned in response to the user ID and password that the client application provides must also return a CNMID of 0.

  To ensure that a client application (GMDR) which monitors components in a VPN only obtains surveillance information for the components that belong to the VPN, the CNMID returned in response to the user ID and password that the client application provides must be a CNMID other than 0, and it must be unique to that VPN.

- For cases in which the FMDR server and the client application both need to obtain surveillance information from all components on all switches in a surveillance group, they can use the same user ID and password. The CNMID returned must be CNMID 0.

  For cases in which the client application obtains surveillance information for a VPN, and only needs to receive surveillance information from the components in that VPN, the user ID and password provided by the client

application cannot be the same as the user ID password in the FMDR server's startup command. The user ID and password provided by the client application must also authenticate in the same way on all switches on which it is defined, and the CMNID returned must also be a CNMID other than 0.

FMDR servers and groups:

- For surveillance, you must define at least one surveillance group.
- A switch can be included in more than one group.
- There must be one FMDR server for each surveillance group.
- The names of surveillance groups must be unique on a given Preside Multiservice Data Manager (MDM) workstation. For example, you cannot have two groups called TOTO on the same workstation. You can, however, duplicate the names of surveillance groups on different workstations.

Do not create groups containing more than 60 switches for surveillance access.

CAUTION

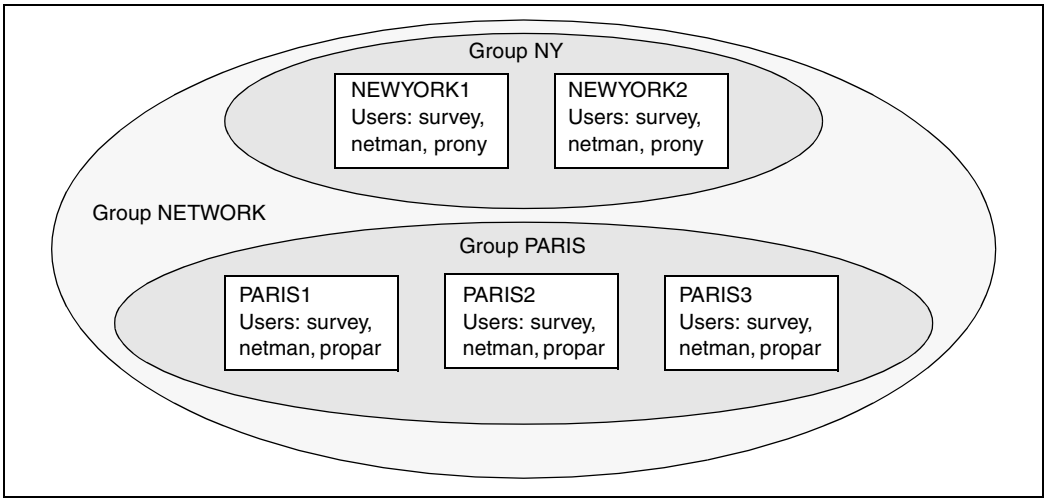
Risk of difficulty in obtaining surveillance information

Defining groups with more than 60 members for surveillance access may cause difficulty in connecting to all of the switches in the group to obtain surveillance information.

Grouping switches, a simple example

The figure "Passport groups" (page 133) contains a simple example of grouping in a network that contains five switches. Two of the switches (NEWYORK1 and NEWYORK2) are located in New York, and the other three are located in Paris (PARIS1, PARIS2, and PARIS3).

Figure 10
Passport groups



Network administrative requirements

The network has the following administrative requirements:

- User survey needs to access all switches in the network for surveillance.
- User prony needs to perform provisioning on all of the switches in New York and user propar needs to perform provisioning on all of the switches in Paris; node provisioning is performed locally.
- User netman needs to access all switches in the network for network management purposes.

Group setup

Administering this network requires three groups:

- a group that contains all of the switches (NETWORK) that can be accessed by users survey and netman
- a group that contains only the New York-based switches (NY) that can be accessed by user prony
- a group that contains all of the Paris-based switches (PARIS) that can be accessed by user propar

For a detailed description of how you can share servers among Preside Multiservice Data Manager (MDM) workstations that are connected to an Ethernet LAN, see “Using the Service Selection tool” (page 467).

FMDR server redundancy for surveillance access

If you have two or more Preside Multiservice Data Manager (MDM) workstations that are connected by a LAN, one of the ways to add redundancy for surveillance gathering is to take advantage of the ability of a GMDR server to discard duplicate surveillance information that it receives from FMDR servers.

To achieve redundancy, you can create duplicate surveillance groups on each of the workstations and run a separate FMDR server on each workstation, as shown in the figure “FMDR server redundancy” (page 135). Then, using the GMDR Administration tool, as described in “Using the GMDR Administration tool” (page 423), you can set up the GMDR server on each workstation to gather surveillance information from the FMDR servers on both workstations.

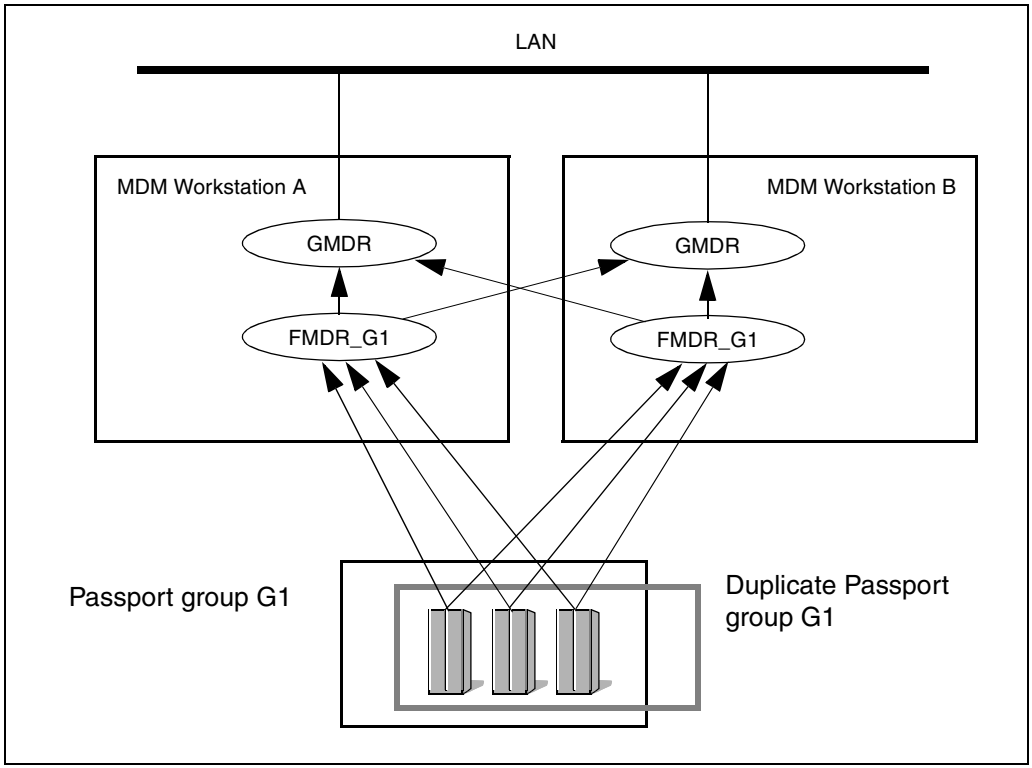
The GMDR server receives alarms from the FMDR servers on both workstations but only displays the alarms once, because the GMDR server discards duplicate alarm notifications. Therefore, should one of the FMDR servers fail, the GMDR server continues to receive surveillance data from its redundant FMDR server without producing an impact on the Fault tools that rely on this information.

The figure “FMDR server redundancy” (page 135) shows a network containing three switches that are monitored by two standalone MDM workstations connected by a LAN. Identical groups called G1 are defined on both workstations. Separate FMDR servers are started to retrieve surveillance data from the groups. The startup command for each FMDR server includes the server name FMDR_G1.

Using the GMDR Administration tool, each GMDR server is configured to receive surveillance data from the FMDR server on its own workstation and from the FMDR server on the redundant workstation through the LAN connection.

The GMDR server on workstation A discards duplicate data from the FMDR servers. Should server FMDR_G1 fail on workstation A, the GMDR server on workstation A still gets the same surveillance information from the redundant FMDR through its LAN connection to workstation B.

Figure 11
FMDR server redundancy



Distribution of servers among workstations on a LAN in big networks

For small networks, all of the servers that support Passport (Passport) network access, surveillance access, and provisioning access can run on the same workstation.

For medium and large networks, servers can be deployed among Preside Multiservice Data Manager (MDM) workstations connected by the same Ethernet LAN or by a WAN IP connection. This is can be done for a number of reasons including the following:

- to distribute the workload over a number of MDM workstations to improve performance
- to permit effective use of older less powerful workstations along with new more powerful workstations
- to add redundancy and resiliency for fault management

The following guidelines apply to deploying the servers for Passport network access, surveillance, and provisioning access over multiple workstations:

- The following servers must run on a workstation that provides network access (a workstation that has an X25 or Frame Relay link to the network): HGDS, FDTM, and FDTR.
- The FMDR server must run on the workstation that provides network access by default. You can run it on another workstation, provided that you specify the hostname of the workstation that runs the network access server, as part of the FMDR server's startup command.
- The GMDR server can run on any workstation on the LAN, provided the workstation can handle traffic to the server. To ensure that the GMDR server receives surveillance information, you must use the GMDR Administration tool to specify the FMDR server (or servers) from which the GMDR server is to obtain the surveillance information for switches.

Configuring servers for network access, surveillance access, and provisioning access

1 Ensure you have done the following tasks:

Switches to be managed	Connection from MDM to switches	Tasks you need to have done
DPN and Passport	IP over switched virtual circuit on an X.25 connection to DPN which that acts as a gateway to switches in the network.	Installed and configured SunLink X.25 software Installed a High Speed Interface (HSI) card and software driver.
Passport only	IP over Frame Relay	Installed a High Speed Interface (HSI) card and software driver Installed SunLink Frame Relay software
Passport only	IP over ATM	Installed an ATM network interface card and software driver Installed SunLink ATM software
Passport only configured as an ILS	IP over Ethernet	No extra communications hardware or software needs to be installed.

For the procedures to perform these tasks, see 241-6001-100 *Preside MDM Installation*.

2 Plan your groups, user IDS and passwords. See “Reasons for Passport groups and guidelines for setting them up” (page 125).

3 Assign the user IDS and passwords on the switches. Refer to the chapter on security in NN10600-605 *Passport - MDM Network Security: Operations* for instructions.

4 Log on as root.

Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in “Setting up the root account to run MDM software” (page 62).

5 Install the latest Passport-MDM Service Data Description (SDD) files as described in “Managing Passport SDD files” (page 507).

6 Use the Server Administration tool to create an FDTM server that starts automatically when the workstation reboots, then start the server. For the instructions to do this, see “Adding a new server” (page 367).

The basic startup command follows. For all possible parameters that can be used in the startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

```
/opt/MagellanNMS/bin/fdtm
```

7 Using the Server Administration tool, create an HGDS server that starts automatically when the MDM workstation reboots, then start the server.

The basic startup command is as follows. For all possible parameters that can be used with the startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

```
/opt/MagellanNMS/bin/hgds
```

8 If you need to perform circuit monitoring, add the necessary entries to the configuration file /opt/MagellanNMS/cfg/FMDR_pollingSurveillance.cfg. For more information on configuring circuit monitoring and File FMDR_pollingSurveillance.cfg, see 241-6001-310 *Preside MDM Server Reference Guide*.

9 Create and start one FMDR server for each group. When creating these servers, ensure that you set them to start automatically when the workstation reboots.

Note: Some groups are created for command access or provisioning access, do not need an FMDR created for them.

CAUTION

Inability to connect to switches

Do not define groups for surveillance that contain more than 60 switches. Doing so may cause difficulty in connecting to all of the switches in the group to obtain surveillance information. You can create larger groups for other purposes such as network access.

For each FMDR server, you must include the following parameters in its startup command:

```
-g <group name> -u <userid> -p <password>
```

where:

`<group name>` is the name of the surveillance group that the FMDR server monitors

`<userid>` and `<password>` are the user ID and password for the common account that the FMDR server uses to obtain surveillance

information from the switches in the surveillance group.

The password can also be the full path name of the file that contains the encrypted password. Password files are stored in the directory: `/opt/MagellanNMS/cfg/private`. See "Generating secure passwords for Preside MDM Servers" in NN10600-605 *Passport - MDM Network Security: Operations*.

10 Use one of the following procedures to define the groups in the Host Group Directory file (/opt/MagellanNMS/cfg/HGDS.cfg):

Switches to be managed	Connection from MDM workstation to switches	Procedure
DPN and Passport	IP over switched virtual circuit on an X.25 connection to DPN which that acts as a gateway to Passport switches in the network.	"Defining the groups and hosts" on page 141
Passport only	IP over Frame Relay	"Defining Passport hosts and groups with the passport.frconfig script" on page 148
Passport only	IP over ATM	"Defining hosts and groups with the passport.atmconfig script" on page 156
Passport only configured as an ILS	IP over Ethernet	"Defining the groups and hosts" on page 141

11 Use the Server Administration tool to create a GMDR server that starts automatically whenever the MDM workstation reboots, then start the server. For instructions to do this, see “Adding a new server” (page 367).

The basic startup command is as follows. For all possible parameters that can be used in the startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

```
/opt/MagellanNMS/bin/gmdr
```

12 Use the Server Administration tool to create an OAMC server that starts automatically when the MDM workstation reboots, then start the server. For instructions to do this, see “Adding a new server” (page 367).

The basic startup command is as follows. For all possible parameters that can be used in the startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

/opt/MagellanNMS/bin/OAMC

13 Use the Server Administration tool to create a DMA server that starts automatically whenever the MDM workstation reboots, then start the server. For instructions to do this, see “Adding a new server” (page 367).

The basic startup command is as follows. For all possible parameters that can be used in the startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

/opt/MagellanNMS/bin/dma

For instructions on how to configure a DMA server for server surveillance and workstation surveillance, see “About server alarm distribution and workstation status probing” (page 262).

14 Use the GMDR Administration tool to configure the GMDR server to access the servers that you created to gather surveillance data.

- For each FMDR server you must provide:

`Server Name` is the name of the surveillance data (FMDR) server in the form FMDR_<group_name>

`Host Name` is the host name or IP address of the workstation on which the FMDR server is running

`User/CapabilityID and Password` is the user ID and password to be used for authentication on connection

- For a subordinate GMDR server you must provide:

`Server Name` is the name of the subordinate GMDR server in the form GMDR or GMDR_<service name>

`Host Name` is the host name or the IP address of the MDM workstation on which the GMDR server is running

`User/CapabilityID and Password` are not required.

- For each OAMC server you must provide:

`Server Name` is the name of the OAMC server in the form OAMC or OAMC <service name>.

`Host Name` is the host name or the IP address of the MDM workstation on which the OAMC server is running

`User/CapabilityID and Password` are not required.

See “Configuring GMDR to access the surveillance servers” (page 450) for the instructions to complete this task.

Defining the groups and hosts

This section describes how to define the Passport (Passport) network configuration on a Preside Multiservice Data Manager (MDM) host using the Host Group Administration tool.

The following topics are contained in this section

Launching the Host Group Administration tool

Launch the Host Group Administration tool using one of these methods.

Note: The Host Group Administration tool does not allow simultaneous administration sessions.

Access from the MDM window

1 From the Preside Multiservice Data Manager (MDM) main window, select **System -> Administration -> Host Group Administration**.

Note: If the user ID used to launch MDM is not the user ID root, this menu item is not available for selection.

The Host Group Administration window opens.

If the file /opt/MagellanNMS/cfg/HGDS.cfg exists, the contents are displayed.

Access from the command line

1 From a UNIX xterm, as the userID root, type

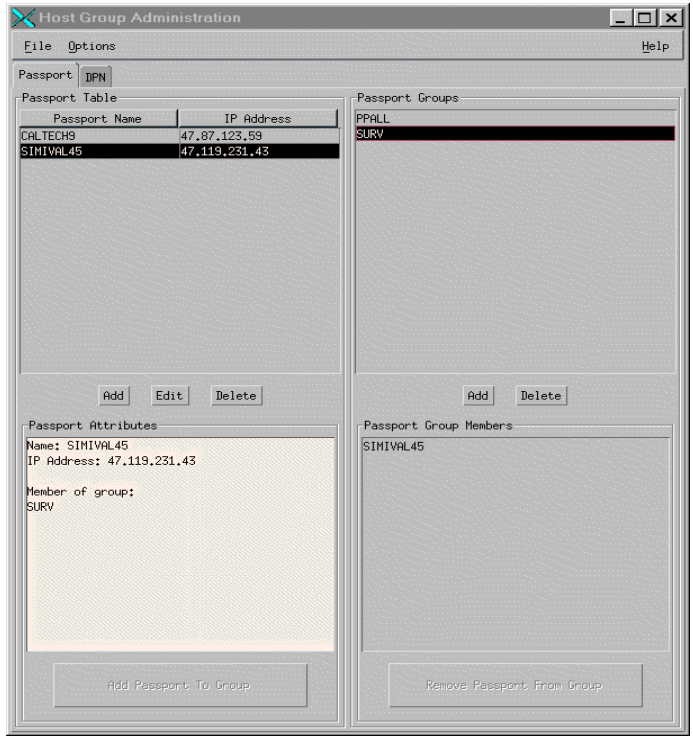
```
/opt/MagellanNMS/bin/hgadmin &
```

The Host Group Administration window opens.

If the file /opt/MagellanNMS/cfg/HGDS.cfg exists, the contents are displayed.

The figure “Host Group Administration window” (page 142) shows an example of this window.

Figure 12
Host Group Administration window



Loading and merging a remote HGDS file

1. Select the **Passport** tab.
2. Select File -> Load and Merge Remote Host Group File.

   The **Load and Merge Remote Host Group File** dialog opens.
3. Type the name of the remote Preside Multiservice Data Manager (MDM) host in the data entry box **Remote Workstation**.
4. Type a user ID to access the remote MDM host in the data entry box **User ID**.
5. Type a password for the User ID in the data entry box **Password**.
6. Click **OK**.

The Load and Merge Remote Host Group File dialog closes.

The remote HGDS file information is displayed.

If a local HGDS file is currently displayed, the Host Group Administration tool merges the HGDS information from the remote host with the HGDS information on the local host. Merge conflicts (for example, the same Passport Names with different IP addresses) are identified. You are provided the option of accepting the new information or retaining the current window contents.

Clearing the window data

1. Select the **Passport** tab.
2. Select **File -> Clear All Data**.

   The **Clear All Data** dialog opens.
3. Click **OK**.

   The Clear All Data dialog closes.

   All of the Host Group Administration window panels are cleared of data.

Adding a Passport node

1. Select the **Passport** tab.
2. Click **Add** below the panel **Passport Table**
   (or select Options -> Passport Table Options -> Add Passport).

   The **Add New Passport** dialog opens.
3. Type the node name in the data entry box **Passport Name**.
4. Type the Passport IP address in the data entry box **IP Address**.
5. Click **OK**.

   The Add New Passport dialog closes and the new node is added to the Passport Table in order according to it's IP Address.

Changing a node definition

1. Select the **Passport** tab.
2. Select the node in the **Passport Table**.
3. Click **Edit** below the panel Passport Table
   (or select Options -> Passport Table Options -> Edit Passport).

   The **Edit Passport** dialog opens.

4 Type the node name in the data entry box **Passport Name**.

5 Type the Passport IP address in the data entry box **IP Address**.

6 Click **OK**.

The Edit Passport dialog closes.

The updated node information is replaced in the Passport Table, and in all of the groups of which it is a member.

Removing a node

1 Select the **Passport** tab.

2 Select the node in the **Passport Table**.

3 Click **Delete** below the panel Passport Table
(or select Options -> Passport Table Options -> Delete Passport).

The **Delete Passport** dialog opens.

4 Click **OK**.

The Delete Passport dialog closes.

Note: The node is removed from the Passport Table and from all of the groups of which it is a member.

Displaying node attributes

1 Select the **Passport** tab.

2 Select the node in the **Passport Table**.

The following node attributes are displayed in the **Passport Attributes** panel:

- nodename
- IP address
- groups that include this node as a member

Note: You can reorder the list of nodes, according to the above attributes, by double-clicking on the table headers. For example, you can list the nodes in alphabetical order according to node name by double-clicking on the node name header. If you double-click on the node name header a second time, the nodes are reordered in reverse alphabetical order. If you double-click on the IP address, the nodes are reordered according to their IP address.

Adding a Passport group

1. Select the **Passport** tab.
2. Click **Add** below the panel **Passport Groups** panel
   (or select Options -> Passport Group Options -> Add Passport group).

   The **Add New Passport Group** dialog opens.
3. Type the group name in the data entry box **Passport Group Name**.
4. Click **OK**.

   The Add New Passport Group dialog closes.

   The new group is added to the Passport Groups panel.

Adding a node to a group

1. Select the **Passport** tab.
2. Select the node in the **Passport Table**.
3. Select the group in the **Passport Groups** panel.

   The button **Add Passport <nodename> to group <group_name>** below the **Passport Attributes** panel is activated.
4. Click **Add Passport <nodename> to group <group_name>**
   (or select Options -> Passport Table Options -> Add Passport to Group).

   The node is added to the group and is displayed in the **Passport Group Members** panel.

   There is no restrictions on the number of nodes in a group.

Removing a node from a group

1. Select the **Passport** tab.
2. Select the group in the **Passport Groups** panel.

   The nodes that belong to the selected group are displayed in the **Passport Group Members** panel.
3. Select the node in the **Passport Group Members** panel.

   The button **Remove Passport <nodename> from group <group_name>** below the **Passport Group Members** panel is activated.
4. Click **Remove Passport <nodename> from group <group_name>**
   (or select Options -> Passport Group Options -> Remove Passport from Group).

The **Remove Passport from group** dialog opens.

5 Click **OK**.

The Remove Passport from group dialog closes.

The node is removed from the group and is no longer displayed in the **Passport Group Members** panel.

Note: Removing a node from a group does not remove the node from other groups and does not remove the node from the Passport Table.

Removing a group

1 Select the **Passport** tab.

2 Select the Passport group in the **Passport Groups** panel.

The nodes that belong to the selected group are displayed in the **Passport Group Members** panel.

3 Click **Delete** below the panel Passport Groups panel (or select Options -> Passport Group Options -> Delete Group).

The **Delete Passport Group** dialog opens.

4 Click **OK**.

The Delete Passport Group dialog closes.

The group is no longer displayed in the **Passport Groups** panel.

Note: Removing a group does not remove the group members from other groups and does not remove the group members from the Passport Table.

Saving the HGDS file

1 Select the **Passport** tab.

2 Select File -> Save.

The **Save Host Group File** dialog opens.

3 Click **OK**.

The Save Host Group File dialog closes.

The current version of the file /opt/MagellanNMS/cfg/HGDS.cfg is saved with a time-stamped suffix.

The contents of the Host Group Administration window are written to the file /opt/MagellanNMS/cfg/HGDS.cfg on the local Preside Multiservice Data Manager (MDM) host and the file is saved.

The HGDS.cfg data is loaded with the HGDS the next time the HGDS is started.

Note: The Host Group Administration tool will not allow the file HGDS.cfg to be updated if mandatory data is missing or is incorrect.

4 If the HGDS is currently running, the **Reload HGDS Configuration** dialog opens with the prompt

```
Do you want to signal the related MDM servers to reload
the HGDS configuration now?
```

Click **Yes** to restart the servers.

Click **No** to restart the servers at another time using the MDM Server Administration (SVMADM) tool.

Closing the Host Group Administration tool

1 Select the **Passport** tab.

2 Select **File -> Exit**.

If no updates have been made to the Host Group Administration window contents, the **Host Group Administration** window closes**.**

If updates have been made to the Host Group Administration window contents, the **Save Host Group File** dialog opens (see “Saving the HGDS file” (page 146)).

Defining Passport hosts and groups with scripts

The Preside Multiservice Data Manager (MDM) software includes three scripts for configuring Passport (Passport) hosts and groups. See the following table to determine which script to use.

Switches to be managed	Connection from MDM workstation to switches	Script
Passport only	IP over Frame Relay	passport.frconfig "Defining Passport hosts and groups with the passport.frconfig script" (page 148)
Passport only	IP over ATM	passport.atmconfig "Defining hosts and groups with the passport.atmconfig script" (page 156)

Defining Passport hosts and groups with the passport.frconfig script

Use the procedures in this section to configure Passport (Passport) hosts and groups in networks that only contain switches and use an IP over Frame Relay link to connect the Preside Multiservice Data Manager (MDM) workstation to nodes in the network.

You must be logged in as root to run the passport.frconfig script.

You can use the passport.frconfig script to do the following:

- add a new switch to an existing group or to a new group
- add an existing switch to an existing group or to a new group
- add information about the IP address, port, and DLCI number used for the Frame Relay connection to the switch
- start the Frame Relay connection

You cannot use the passport.frconfig script to perform the following functions:

- delete a switch from an existing group
- move a switch to another group
- modify the IP address, port name, or DLCI, for a Frame Relay connection

The passport.frconfig script requires the following information as inputs:

- the group name to which the switch belongs
- the host name of the node
- the IP address of the node
- the name of the port to which the Frame Relay link is connected
- the data link connection identifier (DLCI) for the Frame Relay link

The passport.frconfig script adds the group, host name, and IP address to the /opt/MagellanNMS/cfg/HGDS.cfg file and the port and DLCI information to the /etc/opt/SUNWconn/fr/fr.cf file.

There are two ways to run the passport.frconfig script: in prompt mode and in no-prompt mode.

In prompt mode, the script prompts for the parameters that define a switch as a member of a group, and for the parameters to define a Frame Relay connection to the switch. It then prompts you for permission to run the passport.kick script. The passport.kick script is used to update the HGDS, FDTM, and FMDR servers with information about the new switch without the need to restart the servers with the Server Administration tool.

In no-prompt mode, the passport.frconfig script lets you enter all of the parameters on one line, but only reminds you to run the passport.kick script after you have finished running the passport.frconfig script. It does not provide you with the ability to start the passport.kick script.

This section contains the following procedures:

Example: Adding switches to a group using passport.frconfig in no-prompt mode

Use this procedure to add Passport (Passport) switches to a new group or to an existing group using the passport.frconfig script in no-prompt mode.

1 Log on as root.

Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in “Setting up the root account to run MDM software” (page 62).

2 Run the passport.frconfig script in no-prompt mode:

```
/opt/MagellanNMS/bin/passport.frconfig <group name>\
<host name> [<IP address> <port> <DLCI>]
```

where:

`group name` is the name of the group to which the switch belongs consisting of an uppercase string of from 1 to 12 characters.If the group does not already exist, the script creates a new group for you.

The group name must be unique on the workstation. If the group name consists of more than one word, join the words by underscore characters; for example SURV_G1.

If you wish to gather alarms and surveillance information automatically from your network, you should create at least one special group called a surveillance group that is dedicated to gathering surveillance information.

Examples:

name of a group used for provisioning and troubleshooting: FMGROUP

name of a surveillance group: FG_1

Note: Do not use the name of a module as the name of a surveillance group. Doing so may cause confusion in identifying what you are logged in to when using the Command Console.

`host name` is the name of the switch. The host name is an uppercase character string consisting of from 1 to 12 characters, as stored in the service data of switch. Example: host1

`IP address` is the IP address of the switch. The IP address must be a valid address consisting of four numbers from 1 to 3 digits, separated by periods. Omit this parameter if you are adding an existing switch to an existing group or to a new group. Example: 10.0.0.3

`<port>` is name of the port to which the Frame Relay link is connected. For an HSI card this is one of ports hihp0, hihp1, hihp2, or hihp3. By convention, the port labelled 1 on the workstation is hihp0, the port labelled 2 is hihp1, and so on. Omit this parameter if you are adding an existing switch to an existing group or to a new group.

`<DLCI>` is the data link connection identifier (DLCI) that identifies the Frame Relay link and is provisioned in service data of the switch. Contact your Passport network Administrator for the DLCI. Omit this parameter if you are adding an existing switch to an existing group or to a new group.

The script displays responses indicating the group has been created and reminds you to run the passport.kick script.

3 Repeat step 2 once for each switch that you are adding to a new group or to an existing group.

4 Update the HGDS, FDTM, and FDTR servers with the new information by running the passport.kick script.

/opt/MagellanNMS/bin/passport.kick

The script displays messages indicating that the servers are being updated with the modified group information and information about the Frame Relay connection operating parameters.

5 Start (or update) the Frame Relay connection:

/etc/init.d/fr.control update

6 Use the PING command to determine if the connection to the switch is up.

ping <passport IP address>

Example: Adding switches to a group using passport.frconfig in no-prompt mode

The following example shows the use of the passport.frconfig script in no-prompt mode to add a Passport (Passport) switch called WEST3 to group PPGRP and to start the Frame Relay connection. The IP address of the workstation is 47.28.2.19, the Frame Relay link connects to port hihp0 on the workstation, and the Frame Relay link has a DLCI of 16.

1 Enter the following command to add the switch to the group:

/opt/MagellanNMS/bin/passport.frconfig PPGRP WEST3\ 47.28.2.19 hihp0 16

The script responds with the following:

```
Configuring Passport host "West3" in group "PPGRP" with
IP Address "47.28.2.19" and DLCI "16" on port "hihp0"

The Host Group Server configuration file has been
modified, Please signal the related servers with the
passport.kick script or restart them from the Server
Administration tool.

The Frame Relay configuration file
(/etc/opt/SUNWconn/fr/fr.cf)
has been modified.
```

```
The Frame Relay connection will use the following
parameters:
   Port:       hihp0
   IP Address: 47.28.2.19
   DLCI:       16
   Interface:  fr0

If these parameters are not correct, please fix them
in the
Frame Relay configuration file.

All appropriate files have been modified.
```

2 Start the Frame Relay connection manually:

`/etc/init.d/fr.control update`

The connection information updates.

3 Update the HGDS, FDTM, and FMDR servers with the new information by running the passport.kick script:

`/opt/MagellanNMS/bin/passport.kick`

The script displays messages indicating that the servers are being updated with the modified group information and indicating that the frame relay connection information is being updated.

4 To ensure that the connection is up, enter the following command in a UNIX window:

`ping 47.28.2.19`

The following response indicates that the switch is reachable:

```
47.28.2.19 is alive
```

Adding switches to a group using passport.frconfig script in prompt mode

Use this procedure and the accompanying example to add a Passport (Passport) switch to a new group or to an existing group using the passport.frconfig script in prompt mode.

1 Log on as root.

The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in “Setting up the root account to run MDM software” (page 62).

2 Run the passport.frconfig script in no-prompt mode:

/opt/MagellanNMS/bin/passport.frconfig

The passport.frconfig script displays the following prompt:

```
Please specify a group name for the new host:
```

3 Enter the group name. The group name is the name of the group to which the switch belongs.

```
Please specify a name for the new host:
```

4 Enter the host name for the switch.

```
Please specify an IP address for the new host
(or just return for none):
```

5 Do one of the following:

- If you are adding a new switch to a new group or to an existing group, enter the IP address. The system responds with Please specify a Frame Relay port name for the new host (e.g. hihp0)

Go to step 6.

- If you are adding an existing switch to a new group or to an existing group press the Return key to omit the IP address. The system responds with:.Please specify a Frame Relay port name for the new host (e.g. hihp0):

Go to step 9.

6 Enter the name of the port to which the Frame Relay link is connected. For an HSI card this is one of ports hihp0, hihp1, hihp2, or hihp3. By convention, the port labelled 1 on the workstation is hihp0, the port labelled 2 is hihp1, and so on

```
Please specify a Frame Relay DLCI number for the new
host:
```

7 Enter the data link connection identifier (DLCI) that identifies the Frame Relay link and is provisioned in service data of the switch. Contact your Passport network Administrator for the DLCI.

The script displays a response indicating that the group has been created, displays a reminder to update or restart the HGDS, FDTM, and FMDR servers, then displays information about the port, the IP address, the DLCI, and the interface name for the Frame Relay connection. It then displays the following prompt:

```
Do you want to start the Frame Relay connection now
(y/n)?
```

8 Enter **y** to start the Frame Relay connection.

The script displays information indicating that the connection is started, then displays the following prompt:

```
Do you want to run passport.kick and signal the
related MDM servers to reload the HGDS configuration
now (y/n)?
```

9 If you have finished adding all switches to the group, enter Y. If not, enter **N**.

- If you enter Y, the script displays responses indicating that the HGDS, FDTM, and FMDR servers are being updated, followed by the responses:

```
Done
All appropriate files have been modified.
```

Go to step 10.

- If you enter N, the script exits. Go back to step 2 to add the next to the group.

10 Use the PING command to determine if the connection to the switch is up

`ping <passport IP address>`

Example: Adding switches to a group using passport.frconfig in prompt mode

The following example shows the use of the passport.frconfig script in prompt mode to add a Passport (Passport) switch called WEST4 to group PPGRP1 and to start the Frame Relay connection. The IP address of the workstation is 47.28.2.19, the Frame Relay link connects to port hihp0 on the workstation, and the Frame Relay link has a DLCI of 16.

1 Enter the following command to run the passport.frconfig script in prompt mode:

`/opt/MagellanNMS/bin/passport.frconfig`

The script responds with:

```
Please specify a group name for the new host: PPGRP1

Please specify a name for the new host: WEST4
```

```
Please specify an IP address for the new host:
(or just return for none): 47.28.2.19

Please specify a Frame Relay port name for the new host
(e.g. hihp0): hihp0

Please specify a Frame Relay DLCI number for the new
host: 16

Configuring Passport host "WEST4" in group "PPGRP1"
with IP Address "47.28.2.19 and DLCI "16"
on port "hihp0"

The Host Group Server configuration file has been
modified. Please signal the related servers with the
passport.kick script or restart them from the Server
Administration tool.

The Frame Relay configuration file
(/etc/opt/SUNWconn/fr/fr.cf)
has been modified.

The Frame Relay connection will use the following
parameters:
   Port:       hihp0
   IP Address: 47.28.2.19
   DLCI:       16
   Interface:  fr0

If these parameters are not correct, please fix them
in the Frame Relay configuration file.

Do you want to start the Frame Relay connection now
(y/n):?
```

2 Enter **Y** to start the Frame Relay connection.

The script responds as follows:

```
Running /etc/init.d/fr.control start...
Starting Frame Relay

Run /opt/SUNWconn/bin/frmon - 1hihp0
to monitor all of the current connections on this port.

Do you want to run passport.kick and signal the related
MDM servers to reload the HGDS configuration now
(y/n)?:
```

3 Because no further switches are being added, enter **Y**.

The script displays responses indicating that the HGDS, FDTM, and FMDR servers are being updated, followed by the responses:

```
Done
All appropriate files have been modified.
```

4 To ensure that the connection is up, enter the following command in a terminal window:

```
ping 47.28.2.19
```

```
47.28.2.19 is alive
```

The following response indicates that the switch is reachable:

Defining hosts and groups with the passport.atmconfig script

Use the examples in this section to learn how configure Passport (Passport) hosts and groups and start the ATM connection in networks that

- only contain Passport switches
- use IP running on an ATM link to connect the Preside Multiservice Data Manager (MDM) workstation to switches in the network. The ATM link connects to a network interface card (NIC) installed in the MDM workstation and to an ATM port on a gateway switch that provides access to remote switches in the network.

You must be logged in as root to run the passport.atmconfig script.

You can use the passport.atmconfig script to do the following:

- add a new gateway switch to an existing group or to a new group
- add a remote switch to an existing group or to a new group
- set up IP routing on the MDM workstation and start the ATM connection to the network

You cannot use the passport.atmconfig script to do the following:

- delete a switch from an existing group
- move a switch to another group

- add the IP addresses and host names of the following items to the etc/hosts file; you must add these by editing the /etc/hosts file before running the script:
  - — the MDM workstation
  - — the ATM network interface card (NIC) installed in the MDM workstation
  - — the switches to be managed with MDM
- install or configure the ATM network interface card (NIC) driver software. You must obtain the driver software from SunLink and use the documentation supplied with the card to install the driver and configure it before you run the passport.atmconfig script.

The passport.atmconfig script requires the following information as inputs:

- the identifier of the NIC interface card (usually ba0)
- the common name (host name) you wish to assign to the ATM interface on the NIC, for example PPNIC1
- the name(s) of the group(s) that the gateway switch and remote switches belong to, for example PPGRP1
- the host names or the IP addresses of the gateway switch and remote switches
- the virtual channel identifier (VCI) of the permanent virtual circuit (PVC) to the gateway switch

The passport.atmconfig script

- adds the group, host name, and IP address of the switch to the /opt/MagellanNMS/cfg/HGDS.cfg file
- adds information about the ATM interface to files
  /etc/opt/SUNWconn.atm/aarconfig
  /etc/opt/SUNWconn.atm/atmconfig
- creates or updates /etc/opt/SUNWconn.atm/atm.cf with ATM routing information

The passport.atmconfg script provides a prompt mode. It does not provide a no-prompt mode.

Adding a gateway and a remote switch with the passport.atmconfig script

This example shows use of the passport.atmconfig script to:

- add a new gateway Passport (Passport) switch with host name WEST1 and IP address 47.28.2.19 to a new group called PPGRP1
- add a new remote switch with host name WEST2 and IP address 47.28.2.20 to the same group (PPGRP1)
- set up and start an ATM connection to the gateway switch using a permanent virtual circuit (VCI) on VCI 34 running on a network interface card (NIC) called PPNIC1. The NIC has an IP address of 47.28.2.18 and an ATM device interface identifier of ba0.

At the beginning of this example

- the /etc/hosts file only contains the IP address and host name of the Preside Multiservice Data Manager (MDM) workstation
- the /opt/MagellanNMS/cfg/HGDS.cfg file contains only one other group called PPGRPALL which has only one member called EAST1

The user does the following while logged in as root:

1 The user opens the /etc/hosts file with a UNIX editor and finds that it only contains the IP address and host name of the MDM workstation:

```
47.28.2.17 localhost #the MDM workstation
```

2 The user adds the following records to the file, saves the file and closes the file:

```
47.28.2.18 PPNIC1 #network interface ba0 to passports
47.28.2.19 WEST1  #gateway Passport in group PPGRP1
47.28.2.20 WEST2  #a remote Passport in group PPGRP1
```

3 The user starts the passport.atmconfig program:

/opt/MagellanNMS/bin/passport.atmconfig

4 The script produces the following sequence of prompts and messages. The user's responses to prompts appear in boldface type.

```
Do you wish to provision the ATM interface and the
gateway Passport? [n]: y

The ATM interfaces available on the workstation are:
ba0

Please specify the ATM interface you wish to provision:
ba0

Please specify the host name of the ATM workstation
interface or hit return to be prompted for an IP
address: PPNIC1

The switches already defined in the
/opt/MagellanNMS/cfg/HGDS.cfg file are:
EAST1

Please specify a name for the gateway passport: WEST1

The gateway passport is not in a group. In order to do
surveillance or provisioning of this passport it must
belong to a group.

The Groups already defined in the
/opt/MagellanNMS/cfg/HGDS.cfg are:
PPGRPALL

Please specify the group name for gateway passport:
PPGRP1

Member "WEST1" added to group "PPGRP1" in the
/opt/MagellanNMS/cfg/HGDS.cfg file.

Please specify a permanent virtual circuit number for
connecting to the Passport: 34

Do you wish to add a remotely connected Passport
switch? [n]: y

The following gateway passports have been provisioned:
WEST1

Enter the gateway for which the new passport can be
reached: WEST1

The switches already defined in the
/opt/MagellanNMS/cfg/HGDS.cfg file are:
EAST1
```

```
Please specify a name for the remotely connected
Passport: WEST2

The remote passport is not in a group. In order to do
surveillance or provisioning of this passport it must
belong to a group.

The groups already defined in
/opt/MagellanNMS/cfg/HGDS.cfg are:
PPGRPALL

Please specify the group name for passport: PPGRP1

Member "WEST2" added to group "PPGRP1" in the
/opt/MagellanNMS/cfg/HGDS.cfg file.

Do you wish to add another remotely connected passport
switch? [n]: n

The Host Group Server configuration file has been
modified.
Please signal the related servers with the
passport.kick script or restart them with the SVM
Administration Tool

Do you want to run passport.kick and restart the
required servers for your change to take effect? [n]:y

Signaled the Host Group Directory Service (HGDS.
Waiting a bit to let it load the configuration."

Signaled the Passport Communications Manager (FDTM)
Waiting a bit to let it and its subservers load the
configuration.

Signaled the running Passport Surveillance Server(s)
(FMDR)
Please consult the NMS Log Display and the Server
Manager Administration tool to ensure the servers
health.

Done.

The ATM configuration file
(/etc/opt/SUNWconn/atm/atmconfig) will be modified.
```

```
The ATM connection will use the following parameters:
ba0  4.0  -  -  -
ba0  -  PPNIC1  -  -
ba0  SONET  -  -  -

If these parameters are not correct, please fix it
in the ATM configuration file.

The ATM Address Resolution file
(/etc/opt/SUNWconn/atm/aarconfig) will be modified.

The ATM connection will use the following parameters:
ba0  -  -  -  l
ba0  WEST1  -  34  t
ba0  -  -  -  m

If these parameters are not correct, please fix them
in the ATM Address Resolution file.

Do you want to start the ATM connection now (y/n)? [n]:
y

Running /etc/init.d/sunatm stop...

Running /etc/init.d/sunatm start...
Configuring ATM interfaces: ba0

Configuring ATM LAN Emulation interfaces:

Run /etc/opt/SUNWconn/atm/bin/atmstat <interface>
to monitor all the current connections on the
interface.

The atm.cf configuration file
(/etc/opt/SUNWconn/atm/atm.cf) will be modified.

The current interface entries are:

The current routing entries are:
route add WEST2 WEST1

If these routes are not correct, please fix them in the
/etc/opt/SUNWconn/atm/atm.cf file.

Do you want to apply the ATM routing now? [n]:y

Running /etc/init.d/atm.control stop...
Deconfiguring ATM routing

ATM Interface is configured.
```

```
Running /etc/init.d/atm.control start...
Configuring ATM routing

ATM Interface is configured.

Changing interface to be point to point

Adding the route into the routing table
add host WEST2: gateway WEST1

Run /usr/sbin/route -v get <remote passport>
to display the routing to this passport.

All appropriate files have been modified.
passport.atmconfig successful execution
```

Adding a remote switch with the passport.atmconfig script

This example shows the use of the passport.atmconfig script to:

- add a remote Passport (Passport) switch with host name WEST3 and IP address 47.28.2.22 to existing group PPGRP1
- update the ATM connection to an existing gateway switch called WEST1 with new routing information for the remote switch, WEST3

At the beginning of this procedure a gateway switch WEST1 has already been provisioned, it is a member of group PPGRP1, and the ATM connection to the gateway is already running.

To provision the remote switch, the user does the following while logged in as root:

1. The user opens the /etc/hosts file with a UNIX editor and finds that the file contains the IP addresses and host names of the Preside Multiservice Data Manager (MDM) workstation, the NIC card, and the gateway switch WEST1, but does not contain the IP address and host name of the remote switch.
2. The user adds the following record to the file, saves the file and closes the file:

   ```
   47.28.2.22 WEST3
   ```

3. The user starts the passport.atmconfig program:

   /opt/MagellanNMS/bin/passport.atmconfig

4 The script produces the following sequence of prompts and messages. The user's responses to prompts appear in boldface type.

```
Do you wish to provision the atm interface and the
gateway Passport? [n] n

Do you wish to enter a remotely connected passport
switch? [n]: y

Enter the gateway for which the new passport can be
reached: WEST1

The switches already defined in the
/opt/MagellanNMS/cfg/HGDS.cfg file are
EAST1
WEST1
WEST2

Please specify a name for the remotely connected
Passport: WEST3

The Groups already defined in the
/opt/MagellanNMS/cfg/HGDS.cf are:
PPGRPALL
PPGRP1

Please specify the group name for passport: PPGRP1
Member "WEST3" added to group "PPGRP1" in the
/opt/MagellanNMS/cfg/HGDS.cfg file

Do you wish to enter another remotely connected
passport switch: n

The Host Group Server configuration file has been
modified.
Please signal the related servers with the
passport.kick program

Please signal the related servers with the
passport.kick script or restart them with the SVM
Administration Tool

Do you want to run passport.kick and restart the
required servers for your change to take effect? [n]:y

Signaled the Host Group Directory Service (HGDS.
Waiting a bit to let it load the configuration."
```

```
Signaled the Passport Communications Manager (FDTM)
Waiting a bit to let it and its subservers load the
configuration.

Signaled the running Passport Surveillance Server(s)
(FMDR)
Please consult the NMS Log Display and the Server
Manager Administration tool to ensure the servers
health.

Done.

The atm.cf configuration file
(/etc/opt/SUNWconn/atm/atm.cf) will be modified.

The current interface entries are:
ifconfig ba0 PPNIC1 WESt1

The new routing entries are:
route add WEST2 WEST1
route add WEST3 WEST1

If these routes are not correct, please fix it in the
/etc/opt/SUNWconn/atm/atm.cf file.

Do you want to apply the ATM routing now (y/n)? [n]: y
Running /etc/init.d/atm.control.stop...

ATM Interface is configured.

Changing interface to be point to point

Adding the route into the routing table
add host WEST2: gateway WEST1
add host WEST3: gateway WEST1

Run /usr/sbin/route -v get <remote passport>
to display the routing to this passport.

All appropriate files have been modified
passport.atmconfig successful execution
```

Deleting a switch

Use this procedure to remove Passport (Passport) switch from Preside Multiservice Data Manager(MDM) if this MDM uses Frame Relay or ATM to connect to the switch.

1 Edit file /opt/MagellanNMS/cfg/HGDS.cfg and remove the entry that defines the switch as a member of the group from which it is to be removed.

2 If the switch is connected to the MDM workstation by means of

- a Frame Relay connection, edit file /etc/opt/SUNWconn/fr/fr.cf and remove information about the obsolete Frame Relay connection, then update the Frame Relay connection information by entering:

  /etc/init.d/fr.control update

- an ATM connection, edit file /etc/opt/SUNWconn/atm/atm.cf and remove information about the obsolete ATM route, then update the ATM connection information by entering

  route delete <remote passport name><gateway passport name>

3 Use the Server Administration tool to restart the following servers and allow the MDM workstation to use the updated host and group information:

- the Host Group Directory Server (HGDS)
- the Passport Communications Manager (FDTM)
- the FMIP Management Data Router (FMDR) servers for any groups that have had switches added to them or removed from them.

4 From the MDM window, select **System** -> **Administration** -> **GMDR Administration**.

5 From the **Security** menu, select **Login as admin**.

6 In the **Password** field, type in your password.

7 Click **OK**.

8 In the **GMDR Subserver** section, select the group name that switches were added to.

9 Click **Show Components**.

The **GMDR Components** window opens.

10 In the Components section, select the component.

The subcomponents appear in the **Subcomponents for** <component name> area.

11 Select the subcomponent name in the Subcomponents for <component name> area.

12 Click **Delete**.

The switch is removed from the subcomponent list in GMDR Admin.

13 Click **Close**.

14 From the **File** menu, Select **Save**.

15 From the **File** menu, select **Exit**.

16 From the MDM window, select **Fault** -> **Network Viewer.**

17 From the **Network Model Edit** menu, select **Enable Network Model Editing**.

18 Select the network element icon you wish to delete.

19 From the **Network Model Edit** menu, select **Delete Selected Components**.

20 Delete the network element.

21 From the Network Model Edit menu, select Leave Network Model Editing.

Chapter 9
Configuring MDM servers for MPE switches

This section contains the instructions to configure the Preside Multiservice Data Manager (MDM) servers to support the three following basic functions for networks that contain Nortel Networks Multiservice Provider Edge (MPE) switches:

- network access: allows users to log on to MPE switches and enter commands to perform operations such as troubleshooting
- surveillance access: allows the MDM software to gather surveillance information from MPE switches
- provisioning access: allows users to configure MPE switches

For information about servers other than those that support these basic functions, and for references to the instructions for configuring them, see "Roadmap to the MDM servers" (page 81).

Navigation

MPE server configuration procedures

Configuration procedures allow the administrator to set up and manage network, surveillance, and provisioning access to the MPE from the MDM.

Navigation

- "Configuring servers for network, surveillance, and provisioning access to MPEs" (page 169)
- "Defining the groups and hosts" (page 173)
- "Defining MPE 9500 hosts and groups with the mpe.config script" (page 184)
- "Deleting a MPE 9500 switch" (page 191)

Prequisites

- Read and understand "MPE server fundamentals" (page 198)

Configuring servers for network, surveillance, and provisioning access to MPEs

Configure servers for network, surveillance and provisiong access to an MPE from an MDM using this general procedure.

Prerequisites

- Root access and administrator privileges.
- Read and understand "Servers required to support MPE network access, surveillance, and provisioning access" (page 198)
- Read and understand "Reasons for MPE groups and guidelines for setting them up" (page 199)
- Read and understand "Groups of MPEs for network access" (page 201)
- Read and understand "Guidelines for grouping MPE switches for surveillance access" (page 202)
- Read and understand "NMDR server redundancy for surveillance access" (page 205)

Procedure steps

1. Ensure that you have IP Access to the MPE switches.

   For the procedures, see 241-6001-100 *Preside MDM Installation*.

2. Plan your MPE 9500 groups, userids and passwords. See "Reasons for MPE groups and guidelines for setting them up" (page 199).

3. Assign the userids and passwords on the MPE switches. Refer to the chapter on security in NN10700-011 *Nortel Networks Multiservice Provider Edge 9500 Administration and Security* for the instructions to assign userids and passwords on MPE switches.

4. Log on as root.

   Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in "Setting up the root account to run MDM software" (page 62).

5. Use the Server Administration tool to create an NDTM server that starts automatically when the workstation reboots, then start the server. For the instructions to do this, see "Adding a new server" (page 367).

The basic startup command follows. For all possible parameters that can be used in the startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

```
/opt/MagellanNMS/bin/ndtm
```

6 Using the Server Administration tool, create an HGDS server that starts automatically when the workstation reboots, then start the server.

The basic startup command is as follows. For all possible parameters that can be used with the startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

```
/opt/MagellanNMS/bin/hgds
```

7 Create and start one NMDR server for each MPE 9500 surveillance group. When creating these servers, ensure that you set them to start automatically when the workstation reboots.

Note: Some groups are created for command access or provisioning access, do not need an NMDR created for them.

CAUTION

Inability to connect to MPE 9500 switches

Do not define groups for surveillance that contain more than 60 MPE 9500 switches. Doing so may cause difficulty in connecting to all of the switches in the group to obtain surveillance information. You can create larger groups for other purposes such as network access.

For each NMDR server, you must include the following parameters in its startup command:

```
-g <group name> -u <userid> -p <password>
```

where:

`<group name>` is the name of the surveillance group that the NMDR server monitors

`<userid>` and `<password>` are the userid and password for the common account that the NMDR server uses to obtain surveillance information from the MPE 9500s in the surveillance group.

The password can also be the full path name of the file that contains the encrypted password. Password files are stored in the directory:`/opt/MagellanNMS/cfg/private`. See "Generating

secure passwords for Preside MDM Servers" in NN10600-605 *Passport - MDM Network Security: Operations*.

8 Run the mpe.config script or use the HGDS Admin Tool to a add a new or existing MPE 9500 to a new or an existing MPE 9500 group, to the Host Group Directory file (/opt/MagellanNMS/cfg/HGDS.cfg). See “Defining MPE 9500 hosts and groups with the mpe.config script” (page 184).

9 Use the Server Administration tool to create a GMDR server that starts automatically whenever the workstation reboots, then start the server. For instructions to do this, see “Adding a new server” (page 367).

The basic startup command is as follows. For all possible parameters that can be used in the startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

```
/opt/MagellanNMS/bin/gmdr
```

10 Use the Server Administration tool to create an OAMC server that starts automatically when the workstation reboots, then start the server. For instructions to do this, see “Adding a new server” (page 367).

The basic startup command is as follows. For all possible parameters that can be used in the startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

```
/opt/MagellanNMS/bin/OAMC
```

11 Use the GMDR Administration tool to configure the GMDR server to access the servers that you created to gather surveillance data.

For each NMDR server you must provide:

- `Server Name` is the name of the surveillance data (NMDR) server in the form NMDR_<group_name>
- `Host Name` is the host name or IP address of the workstation on which the NMDR server is running
- `User/CapabilityID and Password` is the userid and password to be used for authentication on connection

For each OAMC server you must provide:

- `Server Name` is the name of the OAMC server in the form OAMC or OAMC <service name>.
- `Host Name` is the host name or the IP address of the workstation on which the OAMC server is running
- `User/CapabilityID and Password` are not required.

12 See “Configuring GMDR to access the surveillance servers” (page 450) for the instructions to complete this task.

Defining the groups and hosts

This section describes how to define the network configuration on a Preside Multiservice Data Manager (MDM) host using the Host Group Administration tool.

Navigation

Launching the Host Group Administration tool

Launch the Host Group Administration tool to define host groups for supported devices. There are two methods.

Note: The Host Group Administration tool does not allow simultaneous administration sessions.

Procedure steps

1 Select a method.

Access from the MDM window	Access from the command line
step 2	step 3

2 From the Preside Multiservice Data Manager (MDM) main window, select **System -> Administration -> Host Group Administration**.

Note: If the user ID used to launch MDM is not the user ID root, this menu item is not available for selection.

The Host Group Administration window opens.

If the file /opt/MagellanNMS/cfg/HGDS.cfg exists, the contents are displayed.

3 From a UNIX xterm, as the userID root, type

```
/opt/MagellanNMS/bin/hgadmin &
```

The Host Group Administration window opens.

If the file /opt/MagellanNMS/cfg/HGDS.cfg exists, the contents are displayed.

Loading and merging a remote HGDS file

Use this procedure to load and merge a remote HGDS file.

Procedure steps

1. Select the **MPE** tab.
2. Select File -> Load and Merge Remote Host Group File.

   The **Load and Merge Remote Host Group File** dialog opens.
3. Type the name of the remote Preside Multiservice Data Manager (MDM) host in the data entry box **Remote Workstation**.
4. Type a user ID to access the remote MDM host in the data entry box **User ID**.
5. Type a password for the User ID in the data entry box .
6. Click **OK**.

   The Load and Merge Remote Host Group File dialog closes.

   The remote HGDS file information is displayed.

   If a local HGDS file is currently displayed, the Host Group Administration tool merges the HGDS information from the remote host with the HGDS information on the local host. Merge conflicts (for example, the same MPE Names with different IP addresses) are identified. You are provided the option of accepting the new information or retaining the current window contents.

Clearing the window data

Use this procedure to clear all previous data.

Procedure steps

1. Select the **SRS** tab.
2. Select **File -> Clear All Data**.

   The **Clear All Data** dialog opens.
3. Click **OK**.

   The Clear All Data dialog closes.

   All of the Host Group Administration window panels are cleared of data.

Adding a MPE node

Use this procedure to add a new node.

Procedure steps

1. Select the **SRS** tab.
2. Click **Add** below the panel **MPE Table**
   (or select Options -> MPE Table Options -> Add MPE).

   The **Add New MPE** dialog opens.
3. Type the node name in the data entry box **MPE Name**.
4. Type the MPE IP address in the data entry box **IP Address**.
5. Click **OK**.

   The Add New MPE dialog closes and the new node is added to the MPE Table in order according to it's IP Address.

Changing a node definition

Use this procedure to change the name or IP address of a node that already exists.

Procedure steps

1. Select the **SRS** tab.
2. Select the node in the **MPE Table**.
3. Click **Edit** below the panel MPE Table
   (or select Options -> MPE Table Options -> Edit MPE).

   The **Edit MPE** dialog opens.
4. Type the node name in the data entry box **MPE Name**.
5. Type the MPE IP address in the data entry box **IP Address**.
6. Click **OK**.

   The Edit MPE dialog closes.

   The updated node information is replaced in the MPE Table, and in all of the groups of which it is a member.

Removing a node

Use this procedure to delete an node.

Procedure steps

1. Select the **SRS** tab.
2. Select the node in the **MPE Table**.
3. Click **Delete** below the panel MPE Table
   (or select Options -> MPE Table Options -> Delete MPE).

   The **Delete MPE** dialog opens.
4. Click **OK**.

   The Delete MPE dialog closes.

   Note: The node is removed from the MPE Table and from all of the groups of which it is a member.

Displaying node attributes

Use this procedure to display node attributes such as the node name, the IP address and the groups the node belongs to.

Procedure steps

1. Select the **SRS** tab.
2. Select the node in the **MPE Table**.

   The following node attributes are displayed in the **MPE Attributes** panel:

   - nodename
   - IP address
   - groups that include this node as a member

   Note: You can reorder the list of nodes, according to the above attributes, by double-clicking on the table headers. For example, you can list the nodes in alphabetical order according to node name by double-clicking on the node name header. If you double-click on the node name header a second time, the nodes are reordered in reverse alphabetical order. If you double-click on the IP address, the nodes are reordered according to their IP address.

Adding a MPE group

Use this procedure to add a new MPE group.

Procedure steps

1. Select the **SRS** tab.
2. Click **Add** below the panel **MPE Groups** panel
   (or select Options -> MPE Group Options -> Add MPE group).

   The **Add New MPE Group** dialog opens.
3. Type the group name in the data entry box **MPE Group Name**.
4. Click **OK**.

   The Add New MPE Group dialog closes.

   The new group is added to the MPE Groups panel.

Adding a node to a group

Use this procedure to add an MPE node to a group.

Procedure steps

1. Select the **SRS** tab.
2. Select the node in the **MPE Table**.
3. Select the group in the **MPE Groups** panel.

   The button **Add MPE <nodename>** to **group <group_name>** below the **MPE Attributes** panel is activated.
4. Click **Add MPE <nodename> to group <group_name>** (or select Options -> MPE Table Options -> Add MPE to Group).

   The node is added to the group and is displayed in the **MPE Group Members** panel.

   There is no restrictions on the number of nodes in a group.

Removing a node from a group

Use this procedure to remove an MPE node from a group.

Procedure steps

1. Select the **SRS** tab.
2. Select the group in the **MPE Groups** panel.

   The nodes that belong to the selected group are displayed in the **MPE Group Members** panel.
3. Select the node in the **MPE Group Members** panel.

   The button **Remove MPE <nodename> from group <group_name>** below the **MPE Group Members** panel is activated.
4. Click **Remove MPE <nodename> from group <group_name>** (or select Options -> MPE Group Options -> Remove MPE from Group).

   The **Remove MPE from group** dialog opens.
5. Click **OK**.

   The Remove MPE from group dialog closes.

   The node is removed from the group and is no longer displayed in the **MPE Group Members** panel.

Note: Removing a node from a group does not remove the node from other groups and does not remove the node from the MPE Table.

Removing a group

Use this procedure to delete an MPE group.

Procedure steps

1. Select the **MPE** tab.
2. Select the MPE group in the **MPE Groups** panel.

   The nodes that belong to the selected group are displayed in the **MPE Group Members** panel.
3. Click **Delete** below the panel MPE Groups panel
   (or select Options -> MPE Group Options -> Delete Group).

   The **Delete MPE Group** dialog opens.
4. Click **OK**.

   The Delete MPE Group dialog closes.

   The group is no longer displayed in the **MPE Groups** panel.

   Note: Removing a group does not remove the group members from other groups and does not remove the group members from the MPE Table.

Saving the HGDS file

Use this procedure to after to have made changes to the HGDS file to save the new contents.

Procedure steps

1 Select the **SRS** tab.

2 Select File -> Save.

The **Save Host Group File** dialog opens.

3 Click **OK**.

The Save Host Group File dialog closes.

The current version of the file /opt/MagellanNMS/cfg/HGDS.cfg is saved with a time-stamped suffix.

The contents of the Host Group Administration window are written to the file /opt/MagellanNMS/cfg/HGDS.cfg on the local Preside Multiservice Data Manager (MDM) host and the file is saved.

The HGDS.cfg data is loaded with the HGDS the next time the HGDS is started.

Note: The Host Group Administration tool will not allow the file HGDS.cfg to be updated if mandatory data is missing or is incorrect.

4 If the HGDS is currently running, the **Reload HGDS Configuration** dialog opens with the prompt

```
Do you want to signal the related MDM servers to reload
the HGDS configuration now?
```

Click **Yes** to restart the servers.

Click **No** to restart the servers at another time using the MDM Server Administration (SVMADM) tool.

Closing the Host Group Administration tool

Use this procedure to close the Host Group Administration tool.

Procedure steps

1 Select the **SRS** tab.

2 Select **File -> Exit**.

If no updates have been made to the Host Group Administration window contents, the **Host Group Administration** window closes**.**

If updates have been made to the Host Group Administration window contents, the **Save Host Group File** dialog opens (see “Saving the HGDS file” (page 182)).

Defining MPE 9500 hosts and groups with the mpe.config script

Use the procedures in this section to configure MPE 9500 hosts and groups in networks that only contain MPE 9500 switches.

- You can use the mpe.config script to do the following:
  - add a new MPE 9500 switch to an existing MPE 9500 group or to a new MPE 9500 group
  - add an existing MPE 9500 switch to an existing MPE 9500 group or to a new MPE 9500 group
- You cannot use the mpe.config script to perform the following functions:
  - delete a MPE 9500 switch from an existing group
  - move a MPE 9500 switch to another group

The mpe.config script adds the group, host name, and IP address to the /opt/MagellanNMS/cfg/HGDS.cfg file.

There are two ways to run the mpe.config script: in no-prompt mode and in prompt mode.

In no-prompt mode, the mpe.config script lets you enter all of the parameters on one line, but only reminds you to run the hdgs.kick script after you have finished running the mpe.config script. It does not provide you with the ability to start the hgds.kick script.

In prompt mode, the script prompts for the parameters that define a MPE 9500 switch as a member of a MPE 9500 group, and for permission to run the hdgs.kick script. The hdgs.kick script is used to update the HGDS, NDTM, and NMDR servers with information about the new switch without the need to restart the servers with the Server Administration tool.

Prerequisites

- Root access and administrator privileges.
- Read and understand “Reasons for MPE groups and guidelines for setting them up” (page 199)

- Read and understand "Groups of MPEs for network access" (page 201)
- The mpe.config script requires the following information as inputs:
  - the group name to which the MPE 9500 switch belongs
  - the host name of the MPE 9500 node
  - the IP address of the MPE 9500 node

Navigation

This section contains the following procedures:

- "Procedure steps in no-prompt mode" (page 185)
- "Procedure steps in prompt mode" (page 187)

Procedure steps in no-prompt mode

Use this procedure to add MPE 9500 switches to a new MPE 9500 group or to an existing MPE 9500 group using the mpe.config script in no-prompt mode.

1 Log on as root.

Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in "Setting up the root account to run MDM software" (page 62).

2 Run the mpe.config script in no-prompt mode:

/opt/MagellanNMS/bin/mpe.config <group name>\ <host name> [<IP address>]

where:

`group name` is the name of the MPE 9500 group to which the MPE 9500 switch belongs consisting of an uppercase string of from 1 to 12 characters.If the group does not already exist, the script creates a new group for you.

The group name must be unique on the workstation. If the group name consists of more than one word, join the words by underscore characters; for example SURV_G1.

If you wish to gather alarms and surveillance information automatically from your network, you should create at least one special group called a surveillance group that is dedicated to gathering surveillance information.

Note: Do not use the name of a MPE 9500 module as the name of a surveillance group. Doing so may cause confusion in identifying what you are logged in.

`host name` is the name of the MPE 9500 switch. The host name is an uppercase character string consisting of from 1 to 40 characters, as stored in the service data of MPE 9500 switch.

`IP address` is the IP address of the MPE 9500 switch. The IP address must be a valid MPE 9500 address consisting of four numbers from 1 to 3 digits, separated by periods. Omit this parameter if you are adding an existing MPE 9500 switch to an existing group or to a new group.

The script displays responses indicating the group has been created and reminds you to run the hgds.kick script.

3 Repeat step 2 once for each MPE 9500 switch that you are adding to a new group or to an existing group.

4 Update the HGDS, NDTM, and NDTR servers with the new information by running the hdgs.kick script.

```
/opt/MagellanNMS/bin/hgds.kick
```

The script displays messages indicating that the servers are being updated with the modified group information and information.

Job aid (example)

The following example shows the use of the mpe.config script in no-prompt mode to add a MPE 9500 switch called WEST3 to MPE 9500 group MPEGRP and to start the Frame Relay connection. The IP address of the workstation is 47.28.2.19, the Frame Relay link connects to port hihp0 on the workstation, and the Frame Relay link has a DLCI of 16.

1 Enter the following command to add the MPE 9500 switch to the group:

```
/opt/MagellanNMS/bin/mpe.config MPEGRP WEST3\
47.28.2.19
```

The script responds with the following:

```
Configuring MPE 9500 host "West3" in group "MPEGRP"
with IP Address "47.28.2.19"

The Host Group Server configuration file has been
modified, Please signal the related servers with the
hdgs.kick script or restart them from the Server
Administration tool.
```

```
All appropriate files have been modified.
```

2 Update the HGDS, NDTM, and NMDR servers with the new information by running the hdgs.kick script:

/opt/MagellanNMS/bin/hdgs.kick

The script displays messages indicating that the servers are being updated with the modified group information and indicating that the frame relay connection information is being updated.

3 To ensure that the connection is up, enter the following command in a UNIX window:

ping 47.28.2.19

The following response indicates that the MPE 9500 is reachable:

```
47.28.2.19 is alive
```

Procedure steps in prompt mode

Use this procedure and the accompanying example to add a MPE 9500 switch to a new MPE 9500 group or to an existing MPE 9500 group using the mpe.config script in prompt mode.

1 Log on as root.

Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in"Setting up the root account to run MDM software" (page 62).

2 Run the mpe.config script in prompt mode:

/opt/MagellanNMS/bin/mpe.config

The script responds with:

```
Please specify a group name for the new host: MPEGRP1
```

3 Enter the group name.

The group name is the name of the MPE 9500 group to which the MPE 9500 switch belongs consisting of an uppercase string of from 1 to 12 characters.If the group does not already exist, the script creates a new group.

The group name must be unique on the workstation. If the group name consists of more than one word, join the words by underscore characters; for example SURV_G1.

If you wish to gather alarms and surveillance information automatically from your network, you should create at least one special group called a surveillance group that is dedicated to gathering surveillance information.

Note: Do not use the name of a MPE 9500 module as the name of a surveillance group. Doing so may cause confusion in identifying what you are logged in.

The script responds with:

```
Please specify a name for the new host:
```

4 Enter the host name for MPE switch. The host name is an uppercase character string consisting of from 1 to 40 characters, as stored in the service data of MPE switch.

The script responds with:

```
Please specify an IP address for the new host (or just
return for none):
```

5 Select one:

If you are adding....	Action
a new switch to a new group or to an existing group	Enter the IP address.
adding an existing MPE 9500 to a new group or to an existing group	Press the carriage return key to omit the IP address.

If you enter the IP address for MPE switch. The IP address must be a valid MPE 9500 address consisting of four numbers from 1 to 3 digits, separated by periods.

The script responds with:

```
Do you want to run MPE.kick and signal the related MDM
servers to reload the HGDS configuration now (y/n)?
```

6 Enter Y for yes or N for no. Use the table as a guide.

If you are adding....	Action
more MPE 9500 switches must be added to the group	Enter **N** and return to step 2.
all MPE 9500 switches have been added to the group	Enter **Y**

When you select **Y** the script displays messages indicating that the servers are being updated with the modified group information and information, followed by the following message:

```
Done

All appropriate files have been modified.
```

Job aid (example)

The following example shows the use of the mpe.config script in prompt mode to add a MPE 9500 switch called WEST4 to MPE 9500 group MPEGRP1 and to start the Frame Relay connection. The IP address of the workstation is 47.28.2.19, the Frame Relay link connects to port hihp0 on the workstation, and the Frame Relay link has a DLCI of 16.

1 Enter the following command to run the mpe.config script in prompt mode:

```
/opt/MagellanNMS/bin/mpe.config
```

The script responds with:

```
Please specify a group name for the new host: MPEGRP1

Please specify a name for the new host: WEST4

Please specify an IP address for the new host:
(or just return for none): 47.28.2.19

Configuring MPE 9500 host "WEST4" in group "MPEGRP1"
with IP Address "47.28.2.19

The Host Group Server configuration file has been
modified. Please signal the related servers with the
hdgs.kick script or restart them from the Server
Administration tool.

Do you want to run MPE.kick and signal the related MDM
servers to reload the HGDS configuration now (y/n)?
```

2 Because no further MPE 9500s are being added, enter **Y**.

The script displays responses indicating that the HGDS, NDTM, and NMDR servers are being updated, followed by the responses:

```
Done
All appropriate files have been modified.
```

Deleting a MPE 9500 switch

Use this procedure to remove MPE 9500 nodes from Preside Multiservice Data Manager (MDM) if this MDM uses frame relay or ATM to connect to the MPE 9500s.

1. Edit file /opt/MagellanNMS/cfg/HGDS.cfg and remove the entry that defines the MPE 9500 switch as a member of the group from which it is to be removed.
2. Use the Server Administration tool to restart the following servers and allow the MDM workstation to use the updated host and group information:
   - the Host Group Directory Server (HGDS)
   - the MPE 9500 Management Data Router Server (NDTM)
   - the FMIP Management Data Router (NMDR) servers for any MPE 9500 groups that have had MPE 9500 switches removed from them.
3. From the Preside MDM window, select **System** -> **Administration** -> **GMDR Administration**.
4. From the **Security** menu, select **Login as admin**.
5. In the **Password** field, type in your password.
6. Click **OK**.
7. In the **GMDR Subserver** section, select the group name that MPE 9500 switches were added to.
8. Click **Show Components**.

   The **GMDR Components** window opens.
9. In the Components section, select the component.

   The subcomponents appear in the **Subcomponents for** <component name> area.
10. Select the subcomponent name in the Subcomponents for <component name> area.
11. Click **Delete**.

    The MPE 9500 device is removed from the subcomponent list in GMDR Admin.
12. Click **Close**.

13. From the **File** menu, Select **Save**.
14. From the **File** menu, select **Exit**.
15. From the Preside MDM window, select **Fault** -> **Network Viewer.**
16. From the **Network Model Edit** menu, select **Enable Network Model Editing**.
17. Select the network element icon you wish to delete.
18. From the **Network Model Edit** menu, select **Delete Selected Components**.
19. Delete the network element.
20. From the Network Model Edit menu, select Leave Network Model Editing.

SNMP proxy agent (SPA) configuration

Navigation

Configuring the SNMP proxy agent (SPA)

Use this procedure to configure the SNMP proxy agent to enable a foreign SNMP management system to access MPE 9500 devices.

Perquisites

- Read and understand "MPE server fundamentals" (page 198)
- Read and understand "SNMP Proxy Agent (SPA) fundamentals" (page 207)
- Determine which UDP port this SPA instance uses to receive requests
- The SNMP agent of each Neptune device must be configured to send SNMPv1 traps to the SPA workstation
- If it is required that this SPA instance uses the UDP port 161 to receive SNMP requests from SNMP managers, any process currently bound to this port must be stopped before SPA is started by SVM. On an MDM workstation, this port is normally used by the workstation SNMP manager. To stop this process:
  - As SuperUser, execute "/etc/init.d/startsnmp stop" from an XTERM window; this will stop the workstation SNMP agent
  - As SuperUser, rename the file /etc/rc2.d/S898snmp to /etc/rc2.d/_S898snmp to prevent the workstation SNMP agent from being restarted when the workstation is rebooted.

  As a consequence of using the workstation SNMP agent port for SPA, the workstation will no longer reply to SNMP management processes monitoring workstations in the network. The requests sent by these processes will be received by SPA which will discard them because it

will not be able to match them with a managed Neptune device. However, these discarded requests will be counted in SPA discarded request statistics.

Procedure steps

1. Copy the file /opt/MagellanNMS/lib/cfg/spa.cfg to /opt/MagellanNMS/cfg/spa_<port number>.cfg to create the runtime parameters configuration file.
2. If required, change the new file permissions to allow the operator to modify it and the SPA to read it.
3. Modify any parameter in the new file as needed. The file already contains comments explaining the function of each parameter and its possible values.
4. Copy the file /opt/MagellanNMS/lib/cfg/spa.mgr to /opt/MagellanNMS/cfg/spa_<port number>.mgr to create the SNMP managers configuration file.
5. If required, change the new file permissions to allow the operator to modify it and the SPA to read it.
6. In the new file below the line containing “SNMP v1”, insert a new line for each SNMP manager requiring SNMPv1 traps. The format of those lines is:

   Manager: <manager IP address> [<manager UDP port number>
7. In the new file below the line containing “SNMP v2c”, insert a new line of the same format for each SNMP manager requiring SNMPv2c traps.
8. Configure the workstation as an SNMP v1 trap destination to send SNMPv1 traps to the SPA workstation.
9. Start the SNMP proxy agent instance using SVADM. The command line is:

   /opt/MagellanNMS/bin/spa [-p <port number>] [-m <max requests>

Reloading the configuration files using SPA

Use this procedure to reload the configuration files. This procedure can also be used to dynamically add or delete SNMP managers or modify some runtime parameters such as the list of HGDS groups. By sending a HUP signal, SPA reloads its configuration file without being stopped.

Procedure steps

1 From the command line of a UNIX window, determine the SPA instance process id by typing the following command:

```
/opt/MagellanNMS/bin/ipcmon -s | grep spa_<port number> | grep Alive
```

2 Type the following command to reload the configuration files:

```
kill -HUP <process_id>
```

A HUP signal is sent to this SPA instance which will reload its configuration files.

Redefining the selected log levels using SPA

Use this procedure to redefine the selected log levels. SPA can be triggered to toggle between issuing the logs from all possible levels to its server log file and coming back to the list of levels selected by its runtime parameters configuration file by sending it a USR1 signal:

Procedure steps

1 From the command line of a UNIX window, determine the SPA instance process id by typing the following command:

```
/opt/MagellanNMS/bin/ipcmon -s | grep spa_<port number> | grep Alive
```

2 Type the following command to redefine the log file:

```
kill -USR1 <process_id>
```

If the list of log levels currently used is the list selected in the configuration file, all possible log levels are selected. If all possible log levels are currently selected, SPA returns to the log levels list selected by the configuration file.

Note: if it is required to select a different list of log levels than the 2 selections available through the USR1 signal, the list can be modified as required in the configuration file and the HUP signal used to reload this file.

Generating statistical logs using SPA

Use this procedure to generate statistical logs through the USR2 signal.

Procedure steps

1 From the command line of a UNIX window, determine the SPA instance process id by typing the following command:

```
/opt/MagellanNMS/bin/ipcmon -s | grep spa_<port number> | grep Alive
```

2 Type the following command to redefine the log file:

```
kill -USR2 <process_id>
```

SPA will terminate the current statistical interval, compute the required statistical values, zero the statistical counters, and restart a new statistical interval.

MPE server fundamentals

Read the MPE server fundamentals to understand how servers work together to support provisioning, surveillance, and network access. See the following sections for information about the specific server topics:

- "Servers required to support MPE network access, surveillance, and provisioning access" (page 198)
- "Groups of MPEs for network access" (page 201)
- "Reasons for MPE groups and guidelines for setting them up" (page 199)
- "Groups of MPEs for network access" (page 201)
- "Guidelines for grouping MPE switches for surveillance access" (page 202)
- "NMDR server redundancy for surveillance access" (page 205)
- "SNMP Proxy Agent (SPA) fundamentals" (page 207)

Servers required to support MPE network access, surveillance, and provisioning access

The figure "Interdependencies of servers that support basic functions, networks containing MPE switches" (page 200) shows the servers that need to be configured to support the basic functions of a MPE network access, MPE surveillance access, and MPE provisioning access, and it illustrates the dependencies between these servers.

The servers that need to be configured to support these functions are:

- MPE Communication Manager (NDTM)
- Host Group Directory Server (HGDS)
- MPE Management Data Router (NMDR)
- General Management Data Router (GMDR)
- MDM Log Collector (OAMC)

For detailed descriptions of these servers, see 241-6001-310 *Preside MDM Server Reference Guide*.

Reasons for MPE groups and guidelines for setting them up

A MPE group is a set of MPE switches that shares a least one common userid and password for performing a common management role such as network access, surveillance, or provisioning, and which is defined as a group in the configuration files of the Preside Multiservice Data Manager (MDM) software.

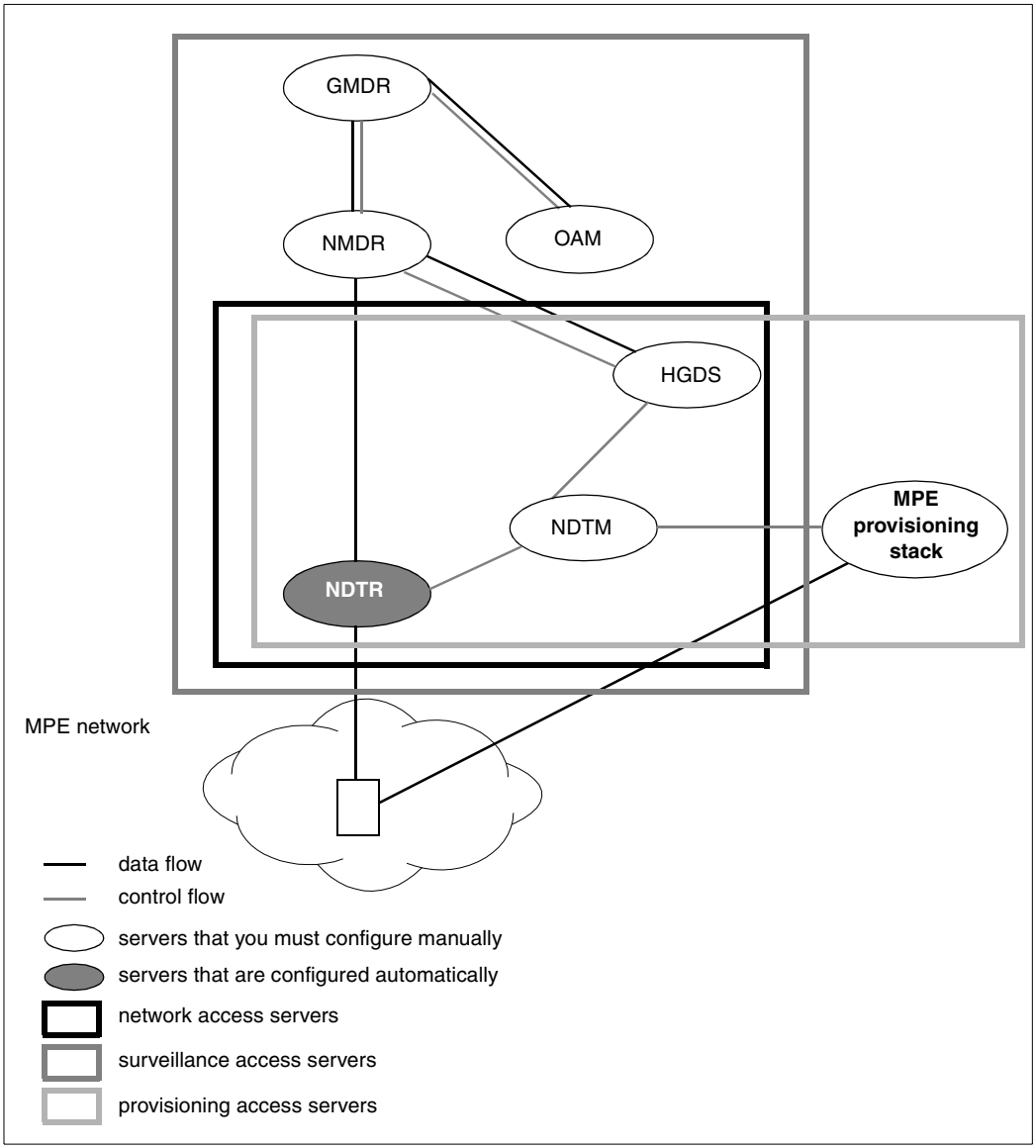
Because the userid defines the administrative capability (scope and impact) of a user, you can use MPE groups to control access to the administrative functions on a switch. When a user logs on with a userid, the user has access to all of the switches defined in the group and can perform any administrative functions allowed by the administrative capability of the userid.

MPE groups are therefore used to control access to the network. Access is required for two main reasons:

- network access: to allow an operator or administrator to log onto a MPE switch with the command access or to perform provisioning operations
- surveillance access: to allow the MPE Management Data Router (NMDR) server to log on to a group of MPE switches and obtain surveillance information

A MPE switch can belong to several groups, so that it can be accessed by different userids for different tasks. For example, a switch can be accessed by an operator for surveillance, and by a network administrator for provisioning.

Figure 13
Interdependencies of servers that support basic functions, networks containing MPE switches



Groups of MPEs for network access

You can define groups that allow users, such as operators or administrators, to access all of the MPE switches in a group of MPE switches and perform operations such as provisioning or troubleshooting. When a user logs on to a group with a userid defined on all MPE switches in the group, the user has access to all of the MPE switches in the group and can perform any of the functions that the userid allows the user to perform.

Guidelines for grouping MPE switches to provide network access are as follows:

- At least one common userid and password must be defined on all MPE switches in a group for performing network access functions. This common userid and password must authenticate in the same way on all MPE switches in the group. That is, the userid and password must be defined with the same login class permissions.
- You are not limited to defining just one common userid and password. You can define several common userids and passwords on the MPE switches in a group and dedicate each to a different function. For example, one userid could have access privileges for provisioning, while another could have access privileges for performing maintenance functions. However, any common userid and password must authenticate in the same way on all MPE switches in the group.
- The same MPE switch can be used in more than one group.

  Note: For an example of grouping MPE switches, see “MPE groups” (page 204).

- A MPE group can not contain Passport members, and a Passport group can not contain MPE members.
- Group names must be unique.

Grouping MPEs for surveillance access

To use the guidelines in this section to group MPE switches for surveillance access you first require an understanding of how surveillance information is obtained from the network. This section is divided into two parts:

- “At startup time” (page 202)
- “At run time” (page 202)

At startup time

To obtain surveillance information the following sequence occurs. See the figure "NMDR server redundancy" (page 206) for an illustration of this sequence.

1 The NMDR server on a Preside Multiservice Data Manager (MDM) workstation logs in to all of the MPEs in a surveillance group with a common userid and password that it obtains from arguments in its startup command.

2 Each MPE switch authenticates the user id and password, and returns a customer network identifier (CNMID).

   To perform its filtering function, an NMDR server needs to receive surveillance information from all of the devices on all of the MPEs in the surveillance group. For an NMDR server to receive the information, the common userid and password must be defined on all MPE switches.

3 To obtain surveillance information from an NMDR server, a client application, such as the GMDR server, registers with the NMDR server. This registration request also includes a userid and password, which can set up by means of the GMDR Administration tool.

4 The NMDR server passes the userid and password contained in the registration request to one of the MPEs in the surveillance group for authentication.

5 The MPE switch authenticates the userid and password.

6 The NMDR initiates a state walk-through to obtain the list of all components that it surveils.

   The setup is now complete.

At run time

When setup is complete, the a MPE switch forwards surveillance information to the MDM workstation.

Guidelines for grouping MPE switches for surveillance access

Guidelines for grouping MPE switches for surveillance access are as follows:

Userids and passwords

- All MPE switches in a surveillance group must support at least one common userid and password for surveillance purposes. This common userid and password must authenticate in the same way on all MPE switches.
- For security reasons, a common userid and password for surveillance purposes must have the minimum login class with a permission of "view".

NMDR servers and groups:

- For surveillance, you must define at least one surveillance group.
- The same MPE switch can be used in more than one group.
- There must be one NMDR server for each surveillance group.
- The names of surveillance groups must be unique on a given workstation. For example, you cannot have two groups called TOTO on the same workstation. You can, however, duplicate the names of surveillance groups on different workstations.

Do not create groups containing more than 60 MPE switches for surveillance access.

CAUTION

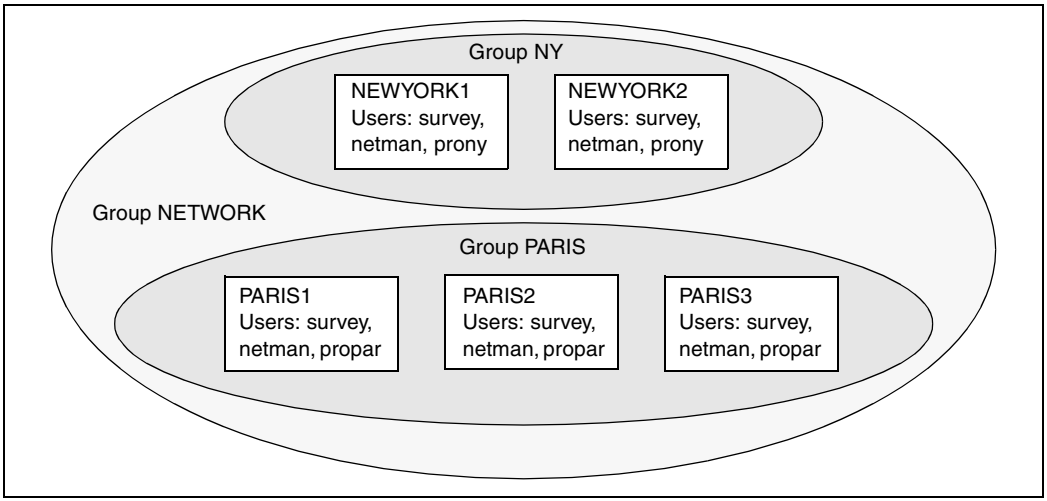
Risk of difficulty in obtaining surveillance information

Defining groups with more than 60 members for surveillance access may cause difficulty in connecting to all of the switches in the group to obtain surveillance information.

Grouping MPEs, a simple example

The figure “MPE groups” (page 204) contains a simple example of grouping in a network that contains five MPE switches. Two of the switches (NEWYORK1 and NEWYORK2) are located in New York, and the other three are located in Paris (PARIS1, PARIS2, and PARIS3).

Figure 14
MPE groups



Network administrative requirements

The network has the following administrative requirements:

- User survey needs to access all switches in the network for surveillance.
- User prony needs to perform provisioning on all of the switches in New York and user propar needs to perform provisioning on all of the switches in Paris; node provisioning is performed locally.
- User netman needs to access all switches in the network for network management purposes.

Group setup

Administering this network requires three groups:

- a group that contains all of the MPE switches (NETWORK) that can be accessed by users survey and netman
- a group that contains only the New York-based switches (NY) that can be accessed by user prony
- a group that contains all of the Paris-based switches (PARIS) that can be accessed by user propar

For a detailed description of how you can share servers among Preside Multiservice Data Manager (MDM) workstations that are connected to an Ethernet LAN, see “Using the Service Selection tool” (page 467).

NMDR server redundancy for surveillance access

If you have two or more workstations that are connected by a LAN, one of the ways to add redundancy for surveillance gathering is to take advantage of the ability of a GMDR server to discard duplicate surveillance information that it receives from NMDR servers.

To achieve redundancy, you can create duplicate surveillance groups on each of the workstations and run a separate NMDR server on each workstation, as shown in the figure “NMDR server redundancy” (page 206). Then, using the GMDR Administration tool, as described in “GMDR Administration tool” (page 423), you can set up the GMDR server on each workstation to gather surveillance information from the NMDR servers on both workstations.

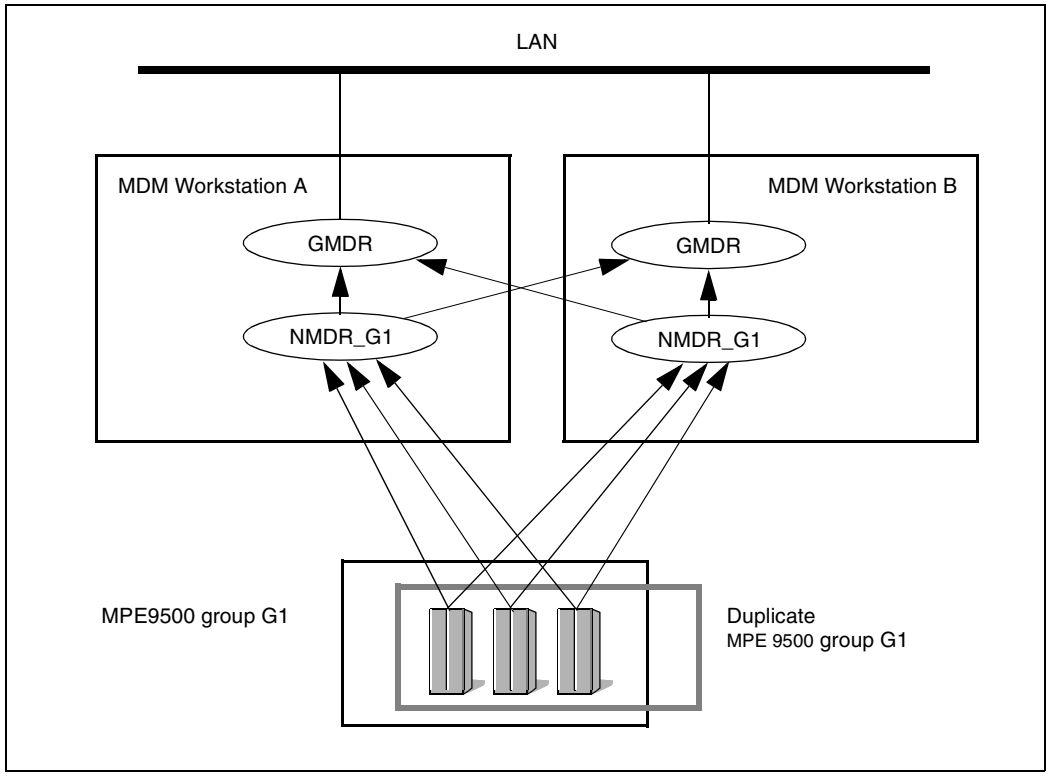
The GMDR server receives alarms from the NMDR servers on both workstations but only displays the alarms once, because the GMDR server discards duplicate alarm notifications. Therefore, should one of the NMDR servers fail, the GMDR server continues to receive surveillance data from its redundant NMDR server without producing an impact on the Fault tools that rely on this information.

The figure “NMDR server redundancy” (page 206) shows a network containing three MPE switches that are monitored by two standalone workstations connected by a LAN. Identical groups called G1 are defined on both workstations. Separate NMDR servers are started to retrieve surveillance data from the groups.

Using the GMDR Administration tool, each GMDR server is configured to receive surveillance data from the NMDR server on its own workstation and from the NMDR server on the redundant workstation through the LAN connection.

The GMDR server on workstation A discards duplicate data from the NMDR servers. Should server NMDR_G1 fail on workstation A, the GMDR server on workstation A still gets the same surveillance information from the redundant NMDR through its LAN connection to workstation B.

Figure 15
NMDR server redundancy



Distribution of servers among workstations on a LAN

For small networks, all of the servers that support MPE network access, MPE surveillance access, and MPE provisioning access can run on the same workstation.

For medium and large networks, servers can be deployed among workstations connected by the same Ethernet LAN or by a WAN IP connection. This is can be done for a number of reasons including the following:

- to distribute the workload over a number of workstations to improve performance
- to permit effective use of older less powerful workstations along with new more powerful workstations

- to add redundancy and resiliency for fault management

The following guidelines apply to deploying the servers for MPE network access, MPE surveillance, and MPE provisioning access over multiple workstations:

- The following servers must run on a workstation that provides network access : HGDS, NMDR, NDTM, and NDTR.
- If you intend to use LAN Service Selection in a mixed MPE and Passport network, the MPE and Passport access servers must be running on the same workstation.
- The GMDR server can run on any workstation on the LAN, provided the workstation can handle traffic to the server. To ensure that the GMDR server receives surveillance information, you must use the GMDR Administration tool to specify the NMDR server (or servers) from which the GMDR server is to obtain the surveillance information for MPE switches.

SNMP Proxy Agent (SPA) fundamentals

The SNMP Proxy Agent (SPA) is available on MPE 9500 devices. SPA provides a single point of SNMP access to several MPE 9500 devices through an MDM server. SPA receives SNMP requests from SNMP management processes and then performs the following functions:

- forwards SNMP requests received from SNMP management processes to the appropriate MPE 9500 devices,
- forwards SNMP replies received from MPE 9500 devices to the requesting SNMP Manager,
- forwards SNMP traps received from MPE 9500 devices to registered SNMP Managers,
- supports versions V1 and V2C of the SNMP protocol,
- supports multiple community strings per MPE 9500 device.

SPA only runs on MDM workstations. Each SPA instance is created and monitored by the MDM Server manager (SVM). It obtains the list of MPE 9500 devices it provides access to from the Host Group Directory Server (HGDS) and receives traps issued by the Neptune devices through the MDM Trap Server (TSVR).

SPA issues logs to notify operators of important server events and problems. These logs are collected and displayed by the MDM OAM log collector. SPA can also record a trace of its execution by storing logs in a server log file. The level of detail logged depends on which log levels are selected as part of the SPA configuration.

Defining address filters

If several SPA instances run on the same workstation and are intended to manage different regions of the MPE 9500 network, the quantity of traps forwarded by TSVR to each SPA instance can be optimized by defining a set of IP address filters for each SPA instance.

The examples described here assume that MPE 9500 devices are grouped within HGDS MPE 9500 groups based on the IP address subnetwork to which they belong. Then, after identifying the address filter corresponding to each subnetwork, the corresponding addressFilter declarations are added to the runtime parameters configuration file and the SPA instance is stopped and restarted.

Since SPA supports dynamic reconfiguration, SPA can de-register and then re-register to TSVR during a reload configuration procedure. For example, if address filters change, you need to reload the configuration files using the “Reloading the configuration files using SPA” (page 195) procedure.

Classless subnet addressing

If the network address plan is based on classless addressing, the format used for the addressFilter declarations is: a.b.c.d/n

a.b.c.d	any valid IP address
n	number of bits in the specified address that must be matched for the filter to succeed

For example, an IP address will match the address filter, 47.128.154.215/12 if its first twelve bits match the first twelve bits of the address 47.128.154.215.

Classful subnet addressing

If the network address plan is based on classful addressing, the format used for the addressFilter declarations is:
<IPelement>[.<IPelement>[.<IPelement>[.<IPelement>]]]

IPelement represents one of the four positions of an IP address and can be in one of the following formats:

*	accepts all values between 0 and 255
<integer>	accepts only this value, which must be between 0 and 255
<integer>-<integer>	accepts only values in this range, each <integer> must be between 0 and 255

If there are less than 4 IPelements, the missing ones default to "*".

For example, an address filter of 55.123.10-40.* accepts any address that has all of the following characteristics:

- the first two elements are 55.123
- the third element is a value between 10 and 40
- the fourth element is a value between 0 and 255

Chapter 10
Configuring network access data mediation

This section contains the instructions to allow advanced users of Preside Multiservice Data Manager (MDM) to configure the Network Data Access Mediation server (NDAM) for the following purposes:

- to provide clients such as HP OpenView NNM desktop with access to the MDM surveillance information
- to perform filtering according to component type or geographic region for the HP OpenView NNM desktop and Fault tools

The NDAM server is mandatory for the deploying HP OpenView NNM desktop. For Fault clients, the NDAM server provides an optional capability that is described in this chapter.

See the following sections for information about configuring network data access mediation:

Purpose of network data access mediation

The Fault servers collect, interpret, and concentrate the management data from the network. If you are not familiar with the Fault servers, and how to configure them, see the following sections:

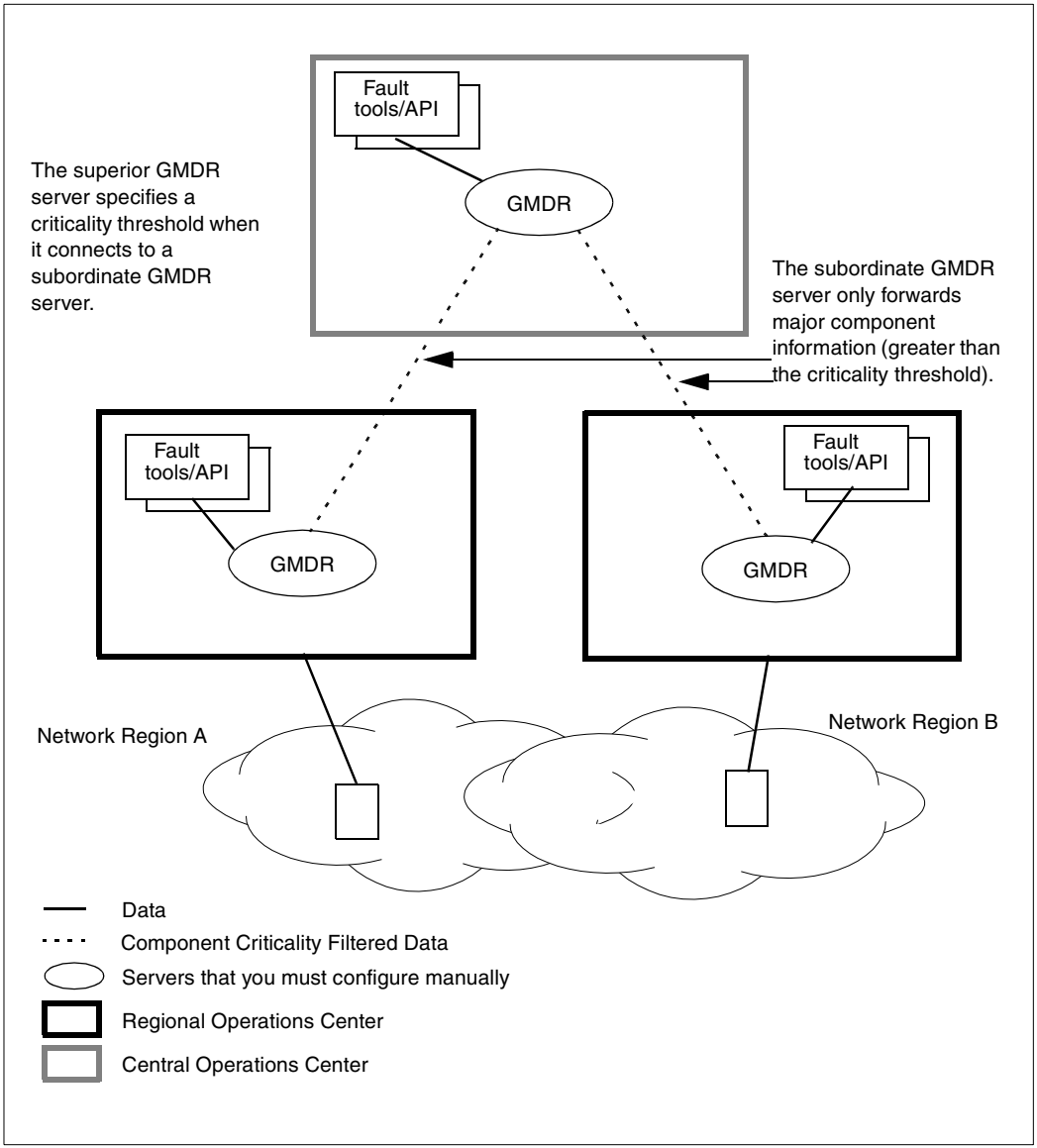
- For networks that contain DPN equipment, see “Configuring servers for DPN switches” (page 93).
- For networks that contain Passport equipment, see “Configuring MDM servers for Passport switches” (page 123).

The Fault clients (Alarm Display, Component Information Viewer) can access the information collected by the Preside Multiservice Data Manager (MDM) data collection servers from the Global Management Data Router (GMDR) server and the Network Model (NMSERVER) server. This information can be forwarded to the clients such as HP OpenView NNM desktop.

If all of the information were made available to a client, users would be subjected to huge amounts of information and not all of it would be useful to perform their jobs. A way of limiting the amount of data forwarded to these clients is required. Fault supports a number of ways to reduce the information forwarded to clients (or to hierarchical GMDR servers):

- through Component Criticality Thresholds. These thresholds can be configured:
  - — by specifying thresholds when setting up hierarchical GMDR servers
  - — by supplying parameters in the startup command for the SURNUP server
  - — See 241-6001-310 *Preside MDM Server Reference Guide* and “GMDR Add Server and GMDR Edit Server dialogs” (page 430) for more information.
- through component type and regional filtering performed by an NDAM server

Figure 16
Use of component criticality-based filtering for regional-central network management



Component criticality thresholds

A subordinate GMDR server assigns a criticality value to all components it manages. When a superior GMDR server connects to a subordinate GMDR server, it can supply a component criticality threshold value. The subordinate GMDR only provides management data for components whose faults pass a threshold test. With thresholding, it is possible to deploy regional management centers that have full view of their managed devices and central management centers (fed from the regional GMDRs) that can see all devices in the network, but only get information for the most important sub-components as controlled by the criticality threshold. See the figure "Use of component criticality-based filtering for regional-central network management" (page 213). You can customize the component criticality assignments by modifying the GMDR criticality schema and by adding exceptional mappings to its criticality overrides configuration file (/opt/MagellanNMS/cfg/GMDRCritOverrides.cfg).

Component type and regional filtering

Component Type filtering lets you specify the type of module, subcomponent, and link types for which a client can receive management data. Regional filtering lets you subdivide the network into different regions and only supply a client with information from the devices in a region. The network data access mediation capabilities of the NDAM server provides these two forms of filtering. You can set up filtering in two ways:

- for HP OpenView NNM desktop, by specifying a list of type and device filtersets and individual overrides at connection time
- for Preside Multiservice Data Manager (MDM) Fault clients, by forced authentication and filtering

The NDAM server can be deployed as a superior GMDR server, a subordinate GMDR server, or as a proxy GMDR server (in place of a GMDR server).

For HP OpenView NNM desktop clients, the NDAM server provides combined access to the GMDR database and Network Model information. For MDM Fault clients, the NDAM server provides access to the GMDR server's information only.

NDAM therefore supports all the capabilities of GMDR plus the filtering described previously. NDAM is therefore always associated with a single GMDR server and its clients. Unlike GMDR, NDAM does not store information in a memory database. It passes through all queries to its assigned GMDR and Network Model servers, and filters the replies according to the filtersets associated with the client connections.

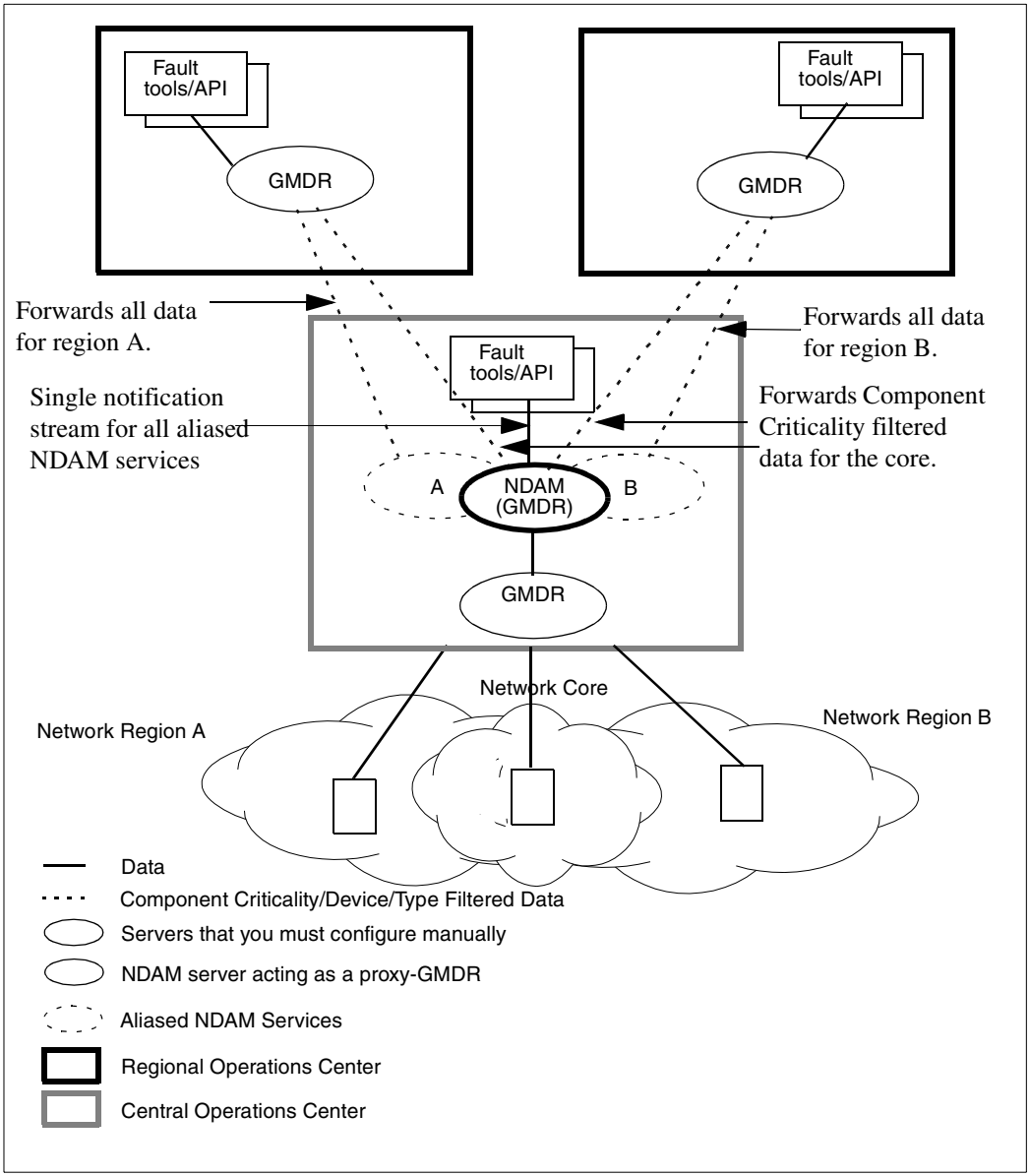
NDAM also uses a single notification stream from the GMDR and Network Model servers, filters it and multiplexes it for NDAM clients. For example, the NDAM server receives an alarm only once from GMDR but can forward the alarm to many clients. An important fact is that NDAM supports Component Criticality Filtering just like GMDR so it is possible to combine both forms of filtering. This lets you do such things as divide the network into a number of regions, one of which represents the network backbone. You can then access data for each region with different Criticality Thresholds as follows:

- connectivity information from the backbone
- full regional information for the regional centers
- hardware and connectivity information from the regions
- full backbone information for the central operations center

For an example, see the figure “Example of component criticality-based filtering for regional-central network management” (page 216).

NDAM also supports service name aliasing to allow a single NDAM server to act as multiple subordinates to the same GMDR server, each connection with a different filterset and criticality threshold mapping.

Figure 17
Example of component criticality-based filtering for regional-central network management



NDAM deployment and configuration strategies

To deploy NDAM for HP OpenView NNM desktop clients, you need to start the NDAM server with the GMDR server option (-g) and the Network Model option (-m). If multiple NDAM servers need to run on the same workstation, you can configure multiple NDAM servers, but you must assign each one a separate service name by means of the -n option.

> ***Note:*** NDAM does not automatically prefix the provided alternate name as GMDR does. This allows NDAM to act as a proxy for GMDR. If you want the service name to include an NDAM_ prefix, you must include it in the value for the -n option. In this deployment it is atypical to start NDAM with the forced authentication (no -s) option.

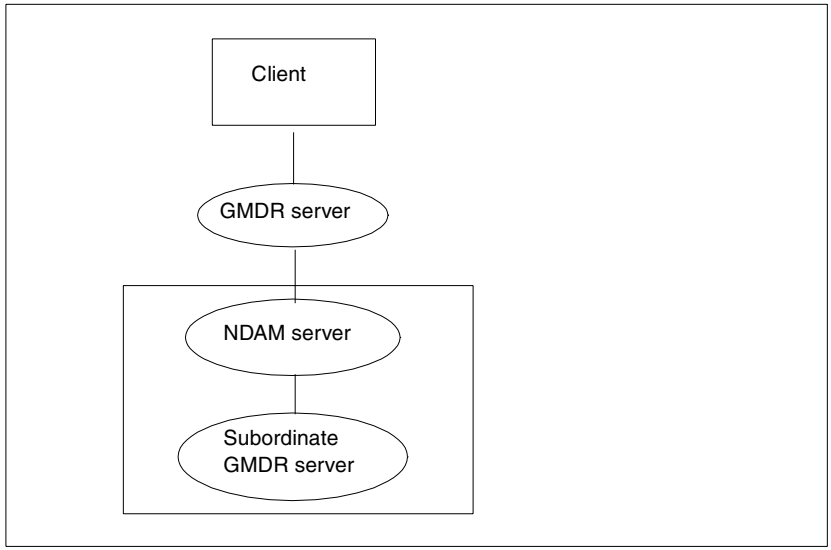
For Fault deployment, NDAM can be configured in two ways:

- as a subordinate GMDR server
- as a proxy server for GMDR

Subordinate GMDR server

When used with a subordinate GMDR server, the NDAM server acts as the intermediary for two hierarchical GMDRs. See the figure "Deployment of NDAM between GMDR servers" (page 218). A superior GMDR server obtains information from a subordinate GMDR possibly on a remote workstation, and the subordinate GMDR server is capped by an NDAM server which is configured as a sub-server to the superior GMDR server.

Figure 18
Deployment of NDAM between GMDR servers



This allows the superior GMDR server to gather information that is filtered according to region or according to component type from subordinate GMDRs and provide it to its clients (Fault tools, SURNUP servers, API and EPI clients and GMDR Administration tool).

In this configuration, you need start the NDAM server with the following options:

- GMDR option (-g)
- -m option with a value of “~”. The quotation marks are mandatory. The -m”~” value specifies that no network model information is involved.
- -s option to set up forced authentication

You cannot configure the NDAM authentication information on the superior GMDR to specify the Filtersets explicitly. You must assign them implicitly through the authentication mechanism.

If the NDAM server needs to be configured as a subordinate to the same superior, GMDR server with the goal of extracting different Filterset/ Criticality Threshold filtering combinations from the same GMDR server, you must specify multiple service name aliases with the -a option and each alias must include a prefix of GMDR_.

To use NDAM as a GMDR replacement, a similar configuration applies; You need to start the NDAM server with the following options:

- -g (GMDR) option
- -m "~" option to disable the Network Model.
- -s option to enable the forced authentication mode. The forced authentication configuration must include a password-less wildcard entry. This is necessary because the Fault tools all access the GMDR server named GMDR by default, and lack the means of specifying explicit authentication information when connecting to it.
- -n option to specify the service name of NDAM server as GMDR

In this mode, NDAM does not support the GMDR Administration Interface. The GMDR Administration tool must be connected directly to the real GMDR server used by NDAM. Similarly, NDAM used as a proxy-GMDR does not support the Inbound API capabilities of the Alarm and Status API. To inject alarms, you must connect directly to the underlying GMDR server. Finally, the Alarm and Status API repFilter, repInfo, repScope, repOClass, and repOid sieve attributes are not available because NDAM does not have an object model of its own to which these filters can be applied.

NDAM authentication configuration

NDAM can be used in either plain or forced-authentication mode (-s option).

In plain mode, NDAM requires a REGISTER message. This message is provided by superior GMDR servers, the Alarm and Status API REGISTER message, and implicitly by the various Preside Multiservice Data Manager Fault tools. However, NDAM actually ignores its contents (user name and password) just like GMDR. In forced-authentication mode though, NDAM checks the authentication information against a list of pre-configured authentications and only accepts matching entries. The authentication information also contains a list of device and type filtersets to be

automatically applied to the client connection. This therefore allows the server side of the Fault stack to control the filtering applied to specific client connections.

To support Fault tools directly without having to deploy an additional GMDR server superior to NDAM, NDAM also supports wildcard authentication. There are two forms of wildcards:

- Multiple service specific wildcards that are specified as %<NDAM SERVICE NAME> or an alias. For example, %EASTREGION) with no password. Any registration made through this service name that does not match a non-wildcard authentication will be accepted with the specified list of filtersets.
- A single global wildcard that is specified as “x” with no password. In this form the wildcard accepts any authentication that does not match a specific entry nor a service specific wildcard.

In addition, on any other type of authentication, it is possible to omit the password (actually specify an x or an empty string). The password is then optional for the corresponding REGISTER messages.

The list of allowed authentications is created using the /opt/MagellanNMS/bin/ndamuser utility with the following command line:

```
/opt/MagellanNMS/bin/ndamuser <user name> \
[<password> [<typeset(.typ) and deviceset(.dev)
names...>]]
```

where:

`<user name>` is x for a global wildcard, %<service name> for a service-specific wildcard (the service name must be in upper-case), or another string for the corresponding authentication.

`<password>` is a valid password or x to indicate that no password is necessary.

`<typesets>` and `<devicesets>` are the names of the filtersets associated with this authentication, they can be specified with or without the NDAM_ prefix (though the corresponding files must be found in /opt/MagellanNMS/

cfg/ for the devicesets and /opt/MagellanNMS/cfg or /opt/MagellanNMS/lib/cfg for the typesets). The names must also have a .typ or .dev suffix to distinguish them as typesets or devicesets files respectively.

> ***Note:*** If forced authentication is used in the context of HP OpenView NNM Desktop clients, you must supply a correct wildcard authentication for NDAM.

The ndamuser utility can be used to add or modify existing authentication entries. To remove authentications, use a UNIX text editor to remove the corresponding line from the /opt/MagellanNMS/cfg/private/NDAM.passwd file (do not add entries manually to this file because the password is encrypted).

NDAM filterset file configuration

There are two types of NDAM filtersets files: typeset files and deviceset files.Typeset files define the types of components that NDAM reports data on. Deviceset files contain lists of devices and can be used to divide the network elements (modules) into geographic regions. Device set files therefore list the modules that are part or are not of the region and support GLOB style pattern matching for more efficiency.

Typeset filers can be specified in one of two ways as controlled by the -F option to NDAM. Without -F (the default option), the filterset files are specified as in the Network Model API by their highest and lowest categories only. For example:

EM-FRAMER accepts data for all Passport FRAMER components (Unacked trunks, FrUni, ...). However, !PM and !PM-* reject all DPN-100 module and subcomponent information.

With the -F (full types) option, the filterset files must be specified with all intermediate types. For example:

EM-FRUNI-FRAMER accepts only FRUNI FRAMER information but no Unacknowledged Trunk Framer information.

GLOB style patterns are supported so that EM-*FRAMER is equivalent to EM-FRAMER without the -F option.

> ***Note:*** All the default typeset files provided with Preside Multiservice Data Manager (MDM) are specified with first-last types only and that it is not possible to mix both types of typeset files. If the -F option is used, all typeset files used must follow the full type specification.

Multiple filterset files can be specified by the client application, such as HP OpenView NNM desktop, or as forced authentication parameters. The files are examined in the specified order and matching data is either rejected as soon as a file is found that explicitly rejects it or accepted as soon as a file explicitly accepts it. If match is found for a component in any of the files, the data is rejected.

For more details about the structure of deviceset files and typeset files, see 241-6001-310 *Preside MDM Server Reference Guide*.

Chapter 11
Configuring Multi-nodal Naming Service domains

This section explains the purpose of a Multi-nodal Naming Service (MNS) domain and contains guidelines and instructions for configuring MNS domains.

You must use the procedures in this chapter to set up MNS domains before you can use the Service Selection tool. See "Using the Service Selection tool" (page 467) for a description of this tool and for the instructions to use it.

Skip this chapter if your Preside Multiservice Data Manager (MDM) workstations are not located on a LAN, if your network only contains standalone MDM workstations, or if you are not planning to use the Service Selection tool.

See the following sections for more information:

- "What MNS domains are used for" (page 223)
- "Guidelines for setting up level 2 MNSD domains" (page 227)
- "Configuring a level 2 MNSD domain" (page 228)

What MNS domains are used for

To manage medium and large networks, several workstations running Preside Multiservice Data Manager (MDM) software can be deployed on the same Ethernet LAN. In these networks, MDM software can be deployed in a server-client fashion among the workstations on the LAN.

The server workstations can be configured to run sets of MDM processes called MDM servers, which support the following main areas of service: surveillance, support of the Network Model, provisioning, and network access (access to the network elements). Workstations configured to run these servers are referred to as Server Set workstations.

The client workstations can be configured to run just the servers that support user sessions and provide access to the MDM tools. Workstations configured to run these servers are referred to as Client Set workstations.To perform their functions, the servers on the Client Set workstations rely on the services provided by the servers on the Server Set workstations.

To allow processes on the same workstation and on different workstations to share services, the processes must be able to locate one another. The Multi-nodal Naming Service (MNS) makes this possible by providing a place for processes to register and obtain the information needed to locate one another. MNS provides a two-level service as follows:

- It provides a level 1 service that allows processes on the same local workstation to locate one another. To allow processes on the same workstation to locate one another, a workstation must be running a level 1 MNSD process. Every workstation on the LAN must be running this process.
- It provides a level 2 service that allows processes on different workstations to locate one another. To allow processes on different workstations to locate one another, at least one of the workstations must be running a level 2 MNSD process. This process provides access to the process identifiers, hostnames, and IP addresses of all workstations that run processes which must be able to interact.

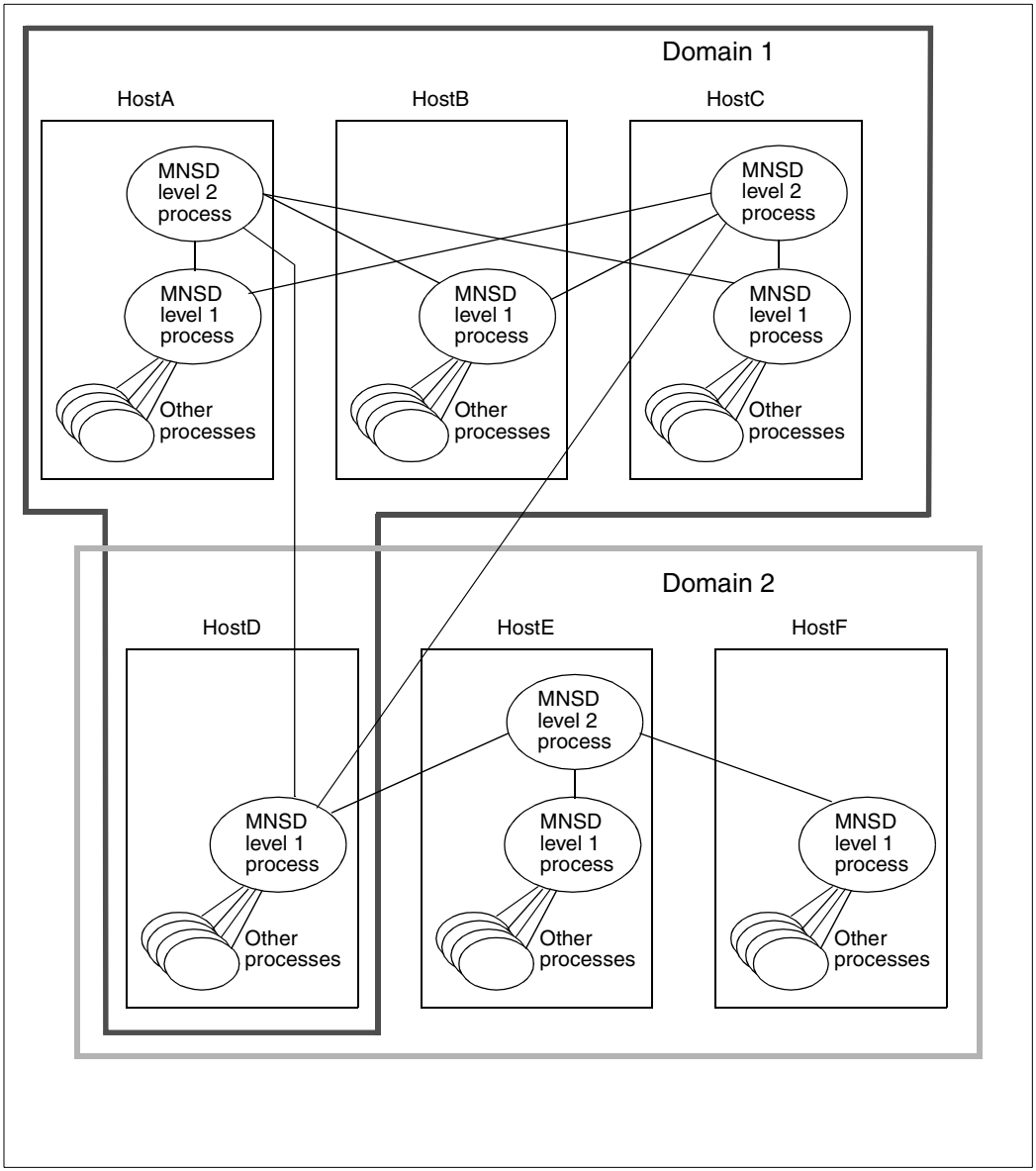
A group of Server Set and Client Set workstations that run processes that interact is referred to as a level 2 MNSD domain. You are not limited to just one level 2 MNSD domain on a LAN. For networks that are being managed by a number of workstations, you can define two or more level 2 MNSD domains, each with its own set of workstations running processes that interact. For a sample MNS configuration containing two level 2 MNSD domains see the figure “A sample MNS configuration of 2 MNS domains” (page 226).

To provide redundancy, you can configure more than one workstation in a level 2 MNSD domain to run the level 2 MNSD process, as shown in the figure “A sample MNS configuration of 2 MNS domains” (page 226). With more than one workstation running a level 2 MNSD process, the servers on a workstation have an alternate place to find the location of servers on other workstations in the domain, in case of failure. In the sample configuration shown in the figure “A sample MNS configuration of 2 MNS domains” (page 226), the servers running on workstations in Domain 1 can select the MNSD level 2 process on hosts A, B or C.

You can set up a workstation so it belongs to more than one level 2 MNSD domain. In the figure “A sample MNS configuration of 2 MNS domains” (page 226), workstation Host D belongs to two domains: Domain 1 and Domain 2.

No work is required to set up a level 1 MNSD process on a workstation. This process starts automatically at boot time. You must start a level 2 MNSD process manually from command, or with the Server Administration tool.

Figure 19
A sample MNS configuration of 2 MNS domains



Guidelines for setting up level 2 MNSD domains

Determining the number of level 2 MNSD domains to set up on a LAN depends the number of workstations on the LAN and how you wish to organize the workstations for managing your network.

Two main ways for organizing level 2 MNSD domains are possible. You can choose to set up level 2 MNSD domains to manage the network on a functional basis (specialization). For example, you can set up one domain that contains workstations dedicated to provisioning, and another that contains workstations dedicated to network access. Alternatively, you can choose to set up level 2 MNSD domains on a regional basis. For example, you can dedicate one domain that contains workstations for managing the eastern part of your network, and another that contains workstations for managing the western part.

Guidelines for setting up level 2 MNSD domains are as follows:

- If you have more than one workstation on a LAN, and the workstations are to share tools and servers (they are not standalone), you must configure are least one level 2 MNSD domain on the LAN.

  Note: You can configure more than one level 2 MNSD domain.

- For redundancy, consider running a level 2 MNSD process on more than one workstation in a level 2 MNSD domain. To provide the most redundancy possible, we recommend that you run a level 2 MNSD process on every Server Set workstation in a level 2 MNSD domain.
- You can configure a workstation to belong to more than one level 2 MNSD domain. This is useful if you wish to use workstation to manage different regions, or to use a service that is only available in a different level 2 MNSD domain.
- To minimize the impact on workstation performance, we recommend that you do not configure a workstation to belong to more than two level 2 MNSD domains.

Configuring a level 2 MNSD domain

Use the procedures in this section to configure a level 2 MNSD domain. The first procedure ensures that on every workstation in a domain, file /etc/hosts contains the host names of all Preside Multiservice Data Manager workstations on the LAN and the second ensures that at least one workstation in the domain runs the level 2 MNSD process.

Note: No work is required to configure a level 1 MNSD domain.

Ensuring that file /etc/hosts contains the host names of the workstations in a domain

Use the following procedure on every workstation in a domain to ensure that file /etc/hosts contains the host names and IP addresses of all other workstations in the domain.

Ensuring that all host names are listed in file /etc/hosts

1. Log on as root to any of the workstations in the domain.
2. Display the contents of file /etc/hosts:

   ```
   more /etc/hosts
   ```

3. File /etc/hosts should contain the hostnames and IP addresses of every workstation on the domain. If any are missing, do one of the following:
   - If the workstations in your network are using a Naming Information Service (NIS), use Sun's NIS Administration tool to ensure that file /etc/hosts contains the hostnames and IP addresses of all workstations in the level 2 MNSD domain.
   - If the workstations in your network are not using NIS, use an editor to add the host names and IP addresses of all workstations in the domain to file /etc/hosts.
4. Repeat the previous steps on every workstation in the level 2 MNSD domain.

Setting up a level 2 MNSD process

The following procedure sets up a level 2 MNSD process. You must perform this procedure on at least one workstation in each level 2 MNSD domain. For maximum redundancy, we recommend that you perform this procedure on every Server Set workstation in a domain.

Setting up a level 2 MNSD process

1 Log on as root at one of the workstations you have chosen to run the level 2 MNSD process.

2 Use the Preside Multiservice Data Manager Server Administration tool to add and start the level 2 MNSD process.

The Server Administration tool is described in “Using the Server Administration tool” (page 359). Read this section before proceeding.

You can use descriptive name for the level 2 MNSD process. This name must be unique among the list of servers running on that workstation (for example, Level 2 Name Server)

Specify the startup command for the level 2 MNSD process as follows:

```
/opt/MagellanNMS/bin/mnsd -2 localhost <hostname1
hostname2 ...>
```

where:
`<hostname1 hostname2 ...>`

are the names of all the workstations in the level 2 MNSD domain, other than local host (this workstation)

The default values for all other parameters for this server are acceptable.

Example

In the sample configuration shown in the figure “A sample MNS configuration of 2 MNS domains” (page 226), the Server Administration tool was used on workstation HostA to start a level 2 MNSD process. The following startup command was used to start the process:

```
/opt/MagellanNMS/bin/mnsd -2 localhost HostB HostC
HostD
```

Chapter 12
Configuring Multi-nodal Naming Service TCP/UDP port mappings

This section explains the purpose for configuring Multi-nodal Naming Service (MNS) TCP/UDP port mappings.

See the following topics for more information:

- "Mapping service names to TCP/UDP port numbers" (page 231)
- "Configuring TCP/UDP port numbers" (page 232)

Mapping service names to TCP/UDP port numbers

Preside Multiservice Data Manager (MDM) uses the MNSD server to store the mappings of service names to TCP/UDP port numbers. These port number mappings allow MDM processes to locate and talk to each other. Normally, the operating system selects the actual TCP/UDP port number allocated (bound) by an MDM server for a service. As a result, the TCP/UDP port number can change each time the server restarts (generally, the service name does not change).

Dynamic port assignment is desirable because MDM relies on a large number of dynamic processes to provide its services. Otherwise, it would be difficult to statically assign the TCP/UDP port numbers in advance in a fail-safe manner. Dynamic port assignment makes it impossible to deploy MDM servers and clients across a communication firewall.

Configuring TCP/UDP port numbers

To allow deployment across a communication firewall, Preside Multiservice Data Manager (MDM) provides the following two methods to predetermine the TCP/UDP port numbers for use by the MDM processes.

- configuring a range of TCP/UDP port numbers that MDM processes will be allowed to bind
- configuring the TCP/UDP port numbers that a specific MDM server will be allowed to bind

For procedures on configuring TCP/UDP port mappings, see 241-6001-310 *Preside MDM Server Reference Guide*.

Note: Services used specifically by Operator Client are documented in Appendix A of NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration*.

Chapter 13
Configuring DPN alarm clearing

This section contains instructions for setting up alarm clearing to allow operators to do the following:

- clear DPN alarms locally on the workstation
- clear DPN alarms globally throughout the DPN switches in a network

For a first time installation you can use the information in this section to set up alarm clearing, or you can use the Preside Multiservice Data Manager (MDM) Software Configuration tool, as described in 241-6001-100 *Preside MDM Installation*.

See the following sections for more information:

- "About alarm clearing" (page 233)
- "How an MDM operator uses alarm clearing" (page 235)
- "Setting up local alarm clearing" (page 236)
- "Setting up global alarm clearing for DPN" (page 236)
- "Troubleshooting global alarm clearing" (page 240)

About alarm clearing

This section describes the two types of alarm clearing and the way in which alarms are collected from the DPN network.

Types of alarm clearing

There are two types of alarm clearing: local alarm clearing and global alarm clearing.

Local alarm clearing lets an operator clear alarms locally from the GMDR database on a Preside Multiservice Data Manager (MDM) workstation.

Global alarm clearing lets an operator clear SET alarms from the MDM and from the active alarm lists (AALs) on all Operations Agents throughout Network Control System (NCS) of the DPN network. The main reason for removing SET alarms from the AALs is to clean up the lists so that only alarms of interest to the network operator remain. This makes monitoring easier.

Alarm clearing can be initiated in several ways:

- from the Alarm Display
- from the Component Information Viewer
- by entering commands at a VT-100 terminal or in the UI of the Command Console (CC)

For information about the Alarm Display and the Component Information Viewer, see 241-6001-011 *Preside MDM Fault Management User Guide*:

For information about the Command Console, see 241-6001-804 *Preside MDM Workstation Utilities User Guide*

How alarms from DPN are collected and stored

In the DPN network, alarms from devices and applications in the network control system (NCS) are routed up the OAs in the NCS hierarchy. SET alarms are stored in the NCS Active Alarm List (AAL) of each Operations Agent (OA) in the NCS. These alarms remain in the AAL until the corresponding alarm has been cleared, or until the alarm is manually deleted. In both cases the alarm is removed from the AAL.

Lists of active alarms are collected and maintained in the following places:

- locally on the workstation in a database associated with the DPN Management Data Router (DMDR) server and in the GMDR database

- in the AALs stored in the Processing Elements (PEs) in the NCS

When the DMDR server connects to an OA in the NCS, it requests a dump of the AAL and uses it to update the DMDR database with all the current SET alarms which are not in the DMDR database. Once the connection between the DMDR server and the OA is established, any SET alarms are automatically copied to the DMDR and GMDR databases.

Alarms stored in the DMDR and GMDR databases can be cleared with local alarm clearing [local to the Preside Multiservice Data Manager (MDM) workstation] or with global alarm clearing. However, alarms stored in the AALs in the NCS can only be cleared by means of global alarm clearing.

How an MDM operator uses alarm clearing

An operator using Preside Multiservice Data Manager (MDM) can delete alarms from the AAL with the Component Information Viewer (CIV) tool or the Alarm Display (AD) tool by selecting a specific alarm with the mouse and selecting local or global clearing from a popup menu.

Both local and global alarm clearing call the manclr process and pass it the component ID, fault code, the alarm ID, the local/global clear flag, and the display name associated with alarm to clear.

Local alarm clearing

When an operator selects local clear with CIV or AD tool, the Data Manager Agent (DMA) server sends a clear request to the DMDR and GMDR databases. The alarm is then cleared from the DMDR and GMDR databases on the workstation.

Global alarm clearing

When the operator selects global clear from the CIV or AD tool, the DMA server sends a clear request to the DMDR and GMDR databases to clear the alarm local on the workstation. The DMA server also logs on to the top level OA in the region managed through this workstation using the information contained in file /opt/MagellanNMS/cfg/DmaClrOA.cfg. It then takes the action required to clear the alarms through the NCS. For details on how the DMA server performs this function, see 241-6001-310 *Preside MDM Server Reference Guide*.

Clearing alarms from a VT100 or from the Command Console

Network operators using VT100 access or the Command Console tool can delete alarms using the NCS OA MANCLR command with appropriate parameters. The operator command must be directed to the OA which hosts the AAL for the node with the alarm.

Clearing alarms using the Global Clear tool

The Global Clear tool lets an operator clear SET alarms from the Preside Multiservice Data Manager servers and from the active alarm lists (AALs) on the switch. The Global Clear tool is initiated from the Alarm menu by selecting
Start Tool ->Fault ->Global Clear of Alarm.

Clearing alarms using Global Clear of Alarm from the Start Tool ->Fault menu allows only one alarm to be cleared at a time. Using this method, the user needs an up-front authentication with a node group before globally clearing an alarm.

Setting up local alarm clearing

For local alarm clearing to work, the GMDR server must be configured and running on the workstation. No additional configuration is required.

Setting up global alarm clearing for DPN

Use the following procedure to set up global alarm clearing for DPN. Setting up global alarm clearing involves the following main steps:

- adding an entry to file opt/MagellanNMS/cfg/DmaClrOA.cfg that provides the Preside Multiservice Data Manager software with the information required to log in to the top level OA in the region managed through this workstation

  The NCS Capability ID and password in the login information must have access privileges that are sufficient to permit global alarm clearing.

- using the Server Administration tool to start the DMA server with the -c option
- using the GMDR Administration tool to set up the GMDR server to access the DMA server as one of is subservers

Prerequisites

Before setting up global alarm clearing, first ensure that:

- The OA definition section of the HGDS server configuration file (HGDS.cfg) defines an OA Member for the top level OA in the region managed through this workstation.
- An NCS capability ID (log in ID) is set up on the top level OA in the managed region with a capability, level, and impact of at least:

NAMS	Network	Service
	OA/Device	None
	Application/Line	None
Switching	Network	None
	Device	None
	Line	None

- The Host Group Directory Server (HGDS) and the NCS Communications Manager (NCSMGR) server are running on the workstation.

Setting up global alarm clearing

1 Using a UNIX editor, open file /opt/MagellanNMS/cfg/DmaClrOA.cfg for editing.

2 Add a single statement to the file in the following format:

```
:DDDDDDDDDDDD:IIIIIIIIIII:PPPPPPPPPPPP:
```

where:

`D`

is the OA Destination mnemonic. The OA Destination mnemonic corresponds to the OA Member field for the top level OA in the managed region as defined in file /opt/MagellanNMS/cfg/HGDS.cfg. In file HGDS.cfg, the OA Member field contains the name of the Management Data Interface (MDI) on the OA. The Preside Multiservice Data Manager (MDM) workstation connects to this OA to send global alarm clearing

request messages to NCS. This mnemonic must match the OA Member for the top level OA entered in file /opt/MagellanNMS/cfg/HGDS.cfg.

Maximum 12 characters.

See the section on OA definitions in 241-6001-310 *Preside MDM Server Reference Guide*.

I

is the NCS capability id (NCS login ID). The id must have the following minimum capability, level, and impact:

NAMS	Network	Service
	OA/Device	None
	Application/Line	None
Switching	Network	None
	Device	None
	Line	None

Maximum 12 characters**.**

P

is a password that has the NCS capability ID. Maximum 12 characters.

The following is an example of a file entry. For this example, there should also be an OA Member called CORENCSIF in file /opt/MagellanNMS/cfg/HGDS.cfg.

```
:CORENCSIF:CORENCS:axylt:
```

3 Start the Server Administration tool from the application main window by selecting System -> Administration -> Server Administration.

Note: Your user account must be set up run the *NMSAdmin* toolset at login to be able to see the Server Administration tool in the menus.

4 Using the Server Administration tool, stop the DMA server, if it is running.

See “Logging out as administrator and accessing view mode” (page 379).

5 Log in as the Server Administrator tool administrator by selecting Enable Editing from the Security menu.

See “Logging out as administrator and accessing view mode” (page 379).

6 Edit the server information to ensure that the server starts automatically when the workstation reboots and that the startup command contains the -c option, as follows:

/opt/MagellanNMS/bin/dma -c [<filename>]

where:

-c [<filename>]

is the name of the file that contains the parameters to establish a virtual circuit to the top level OA in the region managed through this workstation. If you enter the -c option without a filename, the default file name of /opt/MagellanNMS/cfg/DmaClrOA.cfg is used.

See “Editing a server” (page 377).

7 Start the DMA server.

8 Start the GMDR Server Administration tool from the application main window by selecting System -> Administration ->GMDR Administration.

9 Log on to the GMDR Administration tool as the administrator by selecting Log in as admin from the Security menu.

See “Logging in as the administrator” (page 448).

10 Click Add.

The Add Server dialog opens.

11 Enter the following information into fields in the Add Server dialog:

- Server Name: DMASERVER
- Host Name: localhost or the IP address of the workstation on which the GMDR server is running
- User Id and Password: not required

12 Click OK to add the server.

The server appears in the GMDR Servers area of the main window.

13 Open a connection to the DMA server by clicking on DMASERVER in the GMDR Servers list then clicking Connect.

The server state changes to Connecting while GMDR attempts to connect to the server. GMDR attempts to reconnect to a server once every thirty seconds until it is successful, or until the user halts connection attempts

by clicking Disconnect. The state changes to Connected once the connection is established.

You are now ready to initiate global alarm clearing requests from the Component Information Viewer or the Alarm Display.

Troubleshooting global alarm clearing

If global alarm clearing does not work after configuring it, the most likely causes are configuration errors on the Preside Multiservice Data Manager (MDM) workstation or in NCS.

In MDM, the most likely causes are as follows:

- The DMA server is stopped or has not been started with the -c option.
- The GMDR server has not been configured with the GMDR Administration tool to set up the DMA server as one of its subservers. The server name used for the configuration must be DMASERVER and the server must be in the Connected state.
- The OA destination mnemonic entered in file /opt/MagellanNMS/cfg/DmaClrOA.cfg does not have a matching OA Member defined in file opt/MagellanNMS/cfg/HGDS.cfg.
- The DNA of the MDI assigned to the OA Member in MagellanNMS/cfg/HGDS.cfg does not match the DNA entered in NCS.

In the NCS the most likely cause is:

- The NCS capability ID associated with the password used to log into the top level OA in the managed region has insufficient capability, level, or impact. The minimum capability, level and impact should be:

NAMS	Network	Service
	OA/Device	None
	Application/Line	None
Switching	Network	None

Device	None
Line	None

Use the following procedure to troubleshoot global alarm clearing. The following procedure starts by looking at the MDM workstation, then at NCS.

Isolating a global alarm clearing problem

1. Start the Server Administration tool from the application main window by selecting System -> Administration -> Server Administration.

   Note: Your user account must be set up run the NMSAdmin toolset at login to be able to see the Server Administration tool in the menus.

2. Look for the DMA server in the servers list and double-click on it to view the server information.

   The server should be Running, should be set to start at reboot, and the startup command should include the -c option.

   - If the server information is correct and the server is running, go to step 7.
   - If the server information is correct but the server is not running, select the server, then go to step 5.
   - If the server is not defined or the server information is incorrect, go to step 3.

3. Using the Server Administration tool, stop the DMA server, if it is already running.

   See “Logging out as administrator and accessing view mode” (page 379).

4. Log in to the Server Administration tool as the administrator by selecting Enable Editing from the Security menu.

   See “Editing a server” (page 377).

5. Edit the server information to ensure that the server starts automatically when the workstation reboots and the startup command contains the -c option, as follows:

   ```
   /opt/MagellanNMS/bin/dma -c [<filename>]
   ```

   See “Editing a server” (page 377).

6. Start the DMA server.

7 Start the GMDR Server Administration tool by selecting System -> Administration ->GMDR Administration.

8 The DMA server should appear in the server list, be named DMASERVER, and have a status of Connected.

- If the DMA server appears, is named DMASERVER and is connected, go to step 15.
- If the DMA server appears, is named DMASERVER, but is not connected, go to step 13.
- If the DMA server does not appear, or is not named DMASERVER go to step 9.

9 Log in to the GMDR Administrator tool by selecting Log in as admin from the Security menu.

See “Logging in as the administrator” (page 448).

10 Click Add.

The Add Server dialog opens.

11 Enter the following information into fields in the Add Server dialog:

- Server Name: DMASERVER
- Host Name: localhost or the IP address of the workstation on which the GMDR server is running
- User Id and Password: not required

12 Click OK to add the server.

The server appears in the GMDR Servers area of the main window.

13 Click on DMASERVER in the servers list.

14 Click Connect.

15 In a UNIX access window, open file /opt/MagellanNMS/cfg/DmaClrOA.cfg and write down the OA Destination mnemonic, the NCS capability ID, and the password. You will need this information later.

Example:

OA destination mnemonic = CORENCSIF
NCS Capability ID = CORENCS
Password = axylt

16 In a UNIX access window, open file /opt/MagellanNMS/cfg/HGDS.cfg and look for an OA Member that matches the OA Destination mnemonic in file /opt/MagellanNMS/cfg/DmaClrOA.cfg.

Example: OA Member CORENCSIF

17 If there is no corresponding OA Member in file /opt/MagellanNMS/cfg/HGDS.cfg, define the top level OA in the managed region as a member of an OA group, then restart the HGDS server.

See “You are now ready to create OA groups. See “Defining the OA groups and OA members” (page 108).” (page 107).

18 Start the Command Console from the application main window by selecting System -> Utilities -> Command Console.

The Connection Manager Dialog opens.

19 Select Connection Management from the Security menu.

The Command Console Connection Management dialog opens.

20 Enter the OA Destination mnemonic, the NCS Capability ID, and the password from file /opt/MagellanNMS/cfg/DmaClrOA.cfg into the Destination, User Id, and Password fields.

21 Click Connect.

The information you entered is authenticated. When authentication is successful, the message Connected to <OA Destination mnemonic> is displayed.

Example:

```
Connected to CORENCS
```

22 If authentication is successful the NCS Capability. level, and impact may be insufficient for global alarm clearing. Go to step 23.

If authentication is not successful, one or more of the following may be the cause of the problem:

- The DNA assigned in file /opt/MagellanNMS/cfg/HGDS.cfg may be invalid. Obtain the DNA from your DPN Network Administrator or use a maintenance terminal connected to the switch to obtain the DNA.
- The NCS capability ID and password assigned in file /opt/MagellanNMS/cfg/DmaClrOa.cfg may be invalid. Obtain the correct NCS Capability ID and password from your DPN Administrator.
- The X.25 connection may be down. Use Sun’s X.25 admintool and documentation to trace and debug the X.25 connection.

23 Click Close.

The Command Console Connection Management Dialog closes.

24 The NCS capability, impact, and level for the NCS user ID and password are displayed in the Command Console main window. They should be as follows:

NAMS	Network	Service
	OA/Device	None
	Application/Line	None
Switching	Network	None
	Device	None
	Line	None

If they are not as shown. have your DPN Administrator change them or use a maintenance terminal connected to the switch to change them.

Chapter 14
Configuring Passport alarm clearing

This section contains instructions for setting up Passport alarm clearing to allow operators to do the following:

- clear alarms locally on the Preside Multiservice Data Manager (MDM) workstation
- clear alarms globally on the MDM workstation and from the nodes, using Global Clear or the Global Clear tool

For a first time installation you can use the information in this section to set up alarm clearing, or you can use the MDM Software Configuration tool, as described in the 241-6001-100 *Preside MDM Installation*.

See the following sections for more information:

- "Setting up local alarm clearing" (page 246)
- "Setting up the global alarm clearing tool for Passport" (page 246)
- "Setting up global alarm clearing for Passport" (page 247)
- "Troubleshooting a global alarm clearing problem (Global Clear)" (page 250)
- "Troubleshooting a global alarm clearing problem (Global Clear tool)" (page 255)
- "Types of Passport alarm clearing" (page 257)
- "How alarms from Passport are collected and stored" (page 259)

Setting up local alarm clearing

For local alarm clearing to work, the GMDR server must be configured and running on the Preside Multiservice Data Manager workstation. No additional configuration is required.

Setting up the global alarm clearing tool for Passport

For the global alarm clearing tool to work, the Host Group Directory Services (HGDS) server and the Passport Comms Mgr server (FDTM) must be configured and running on the Preside Multiservice Data Manager workstation. No additional configuration is needed.

Setting up global alarm clearing for Passport

Use the following procedure to set up global alarm clearing for Passport. Setting up global alarm clearing involves the following main steps:

- adding one or more entries to file opt/MagellanNMS/cfg/DmaClrPP.cfg that provides the DMA server with the information required to connect to each group.
- using the Server Administration tool to start the DMA server with the -f option to allow Global Clear
- using the GMDR Administration tool to set up the GMDR server to access the DMA server as one of is subservers

Prerequisites

Before setting up global alarm clearing, first ensure that:

- The Active Alarm List feature is enabled on the switch.

Procedure

1. Using a UNIX editor, open file /opt/MagellanNMS/cfg/DmaClrPP.cfg for editing.
2. Add one or more entries to the file in the following format:

   `:GroupName:UserID:Password:`

   where:

   `GroupName`

   is the name of the group to which the node is a member. The group name corresponds to the FGroup field definition of its included members, as defined in file /opt/MagellanNMS/cfg/HGDS.cfg. The DMA server connects to all groups indicated in this file to send global alarm clearing request messages to the targeted node.

   Maximum 12 characters.

   `UserId`

   is the group user ID. At a minimum, the user ID must have systemAdministration impact and scope of device or higher and a customer ID of 0.

   Maximum 8 characters**.**

`Password`

is a password that corresponds to the user ID.

Maximum 8 characters.

The following is an example of a file entry. For this example, there should also be a group entry named ALL in file /opt/MagellanNMS/cfg/HGDS.cfg.

`:ALL:user:password:`

As soon as a syntax error is found in the file, it is displayed in the Preside Multiservice Data Manager System Log Display and DMA exits.

Once the file is read by the DMA server, each password is removed and an encrypted one is added in the fourth field. The above example would become:

:ALL:user::72eilRnWj7{s{A6hgg7:

3 Start the Server Administration tool from the application main window by selecting **System -> Administration -> Server Administration**.

Note: Your user account must be set up run the *NMSAdmin* toolset at login to be able to see the Server Administration tool in the menus.

4 Using the Server Administration tool, stop the DMA server, if it is running.

See “Logging out as administrator and accessing view mode” (page 379).

5 Log in as the Server Administrator tool administrator by selecting Enable Editing from the Security menu.

See “Logging out as administrator and accessing view mode” (page 379).

6 Edit the server information to ensure that the server starts automatically when the workstation reboots and that the startup command contains the -f option, as follows:

`/opt/MagellanNMS/bin/dma -f`

Optionally, a command line option can be added: -t to configure the inactivity timer.

See “Editing a server” (page 377).

7 Start the DMA server.

8 Start the GMDR Server Administration tool by from the application main window by selecting **System -> Administration ->GMDR Administration**.

9 Log on to the GMDR Administration tool as the administrator by selecting Log in as admin from the **Security** menu.

See “Logging in as the administrator” (page 448).

10 Click **Add**.

The **Add Server** dialog opens.

11 Enter the following information into fields in the Add Server dialog:

- Server Name: DMASERVER
- Host Name: local host or the IP address of the workstation on which the DMA server is running
- User Id and Password: not required

12 Click OK to add the server.

The server appears in the GMDR Servers area of the main window.

13 Open a connection to the DMA server by clicking on DMASERVER in the GMDR Servers list then clicking Connect.

The server state changes to Connecting while GMDR attempts to connect to the server. GMDR attempts to reconnect to a server once every thirty seconds until it is successful, or until the user halts connection attempts by clicking Disconnect. The state changes to Connected once the connection is established.

Troubleshooting a global alarm clearing problem (Global Clear)

Use this procedure to isolate the reason why Global Clear alarm does not work.

If global alarm clearing does not work after configuring it, the most likely causes are configuration errors on the Preside Multiservice Data Manager (MDM) workstation or in the DmaClrPP.cfg file.

In MDM, the most likely causes are as follows:

- The DMA server is stopped or has not been started with the -f option.
- The GMDR server has not been configured with the GMDR Administration tool to set up the DMA server as one of its subservers. The server name used for the configuration must be DMASERVER and the server must be in the Connected state.
- The group entered in file /opt/MagellanNMS/cfg/DmaClrPP.cfg does not have a matching group entry defined in HGDS (file opt/MagellanNMS/cfg/HGDS.cfg).
- The targeted node is not part of any of the groups specified in opt/MagellanNMS/cfg/DmaClrPP.cfg file.

The group user ID associated with the password used to log in to the targeted nodes has insufficient impact or scope, or the wrong password, or customer ID. The customer ID must be zero and the minimum scope and impact should be device and systemAdministration, respectively.

Refer to the 241-6001-310 *Preside MDM Server Reference Guide* for the error messages.

Procedure

1. Start the Server Administration tool from the application window by selecting **System -> Administration -> Server Administration**.

   Note: Your user account must be set up to run the NMSAdmin toolset at login to be able to see the Server Administration tool in the menus.

2. Look for the Host Group Directory Services (HGDS) server in the servers list and double click on it to view the server information.

The server should be Running and should be set to start at reboot.

3 Look for the Passport Comms Mgr server (FDTM) in the servers list and double click on it to view the server information.

The server should be Running and should be set to start at reboot.

4 Look for the GMDR server in the servers list and double-click on it to view the server information.

The server should be Running, and should be set to start at reboot.

5 Look for the DMA server in the servers list and double-click on it to view the server information.

The server should be Running, should be set to start at reboot, and the startup command should include the -f option.

Note: Steps 1-5 and 18-27 need to be completed on the workstation where the network access layer resides (FDTM and HGDS). The other steps need to be completed where the implicated servers reside (possibly on a remote workstation.)

- If the server information is correct and the server is running, go to step 10.
- If the server information is correct but the server is not running, select the server, then go to step 9.
- If the server is not defined or the server information is incorrect, go to step 6.

6 Using the Server Administration tool, stop the DMA server, if it is already running.

See “Logging out as administrator and accessing view mode” (page 379).

7 Log in to the Server Administration tool as the administrator by selecting Enable Editing from the Security menu.

See “Editing a server” (page 377).

8 Edit the server information to ensure that the server starts automatically when the workstation reboots and the startup command contains the -f option, as follows:

```
/opt/MagellanNMS/bin/dma -f
```

See “Editing a server” (page 377).

Note: Optionally, a command line option can be added: -t to configure the inactivity timer.

9 Start the DMA server.

10 Start the GMDR Server Administration tool by selecting **System -> Administration ->GMDR Administration.**

11 The DMA server should appear in the server list, be named DMASERVER, and have a status of Connected.

- If the DMA server appears, is named DMASERVER and is connected, go to step 18.
- If the DMA server appears, is named DMASERVER, but is not connected, go to step 16.
- If the DMA server does not appear, or is not named DMASERVER go to step 12.

12 Log in to the GMDR Administrator tool by selecting **Log in as admin** from the **Security** menu.

See “Logging in as the administrator” (page 448).

13 Click Add.

The Add Server dialog opens.

14 Enter the following information into fields in the **Add Server** dialog:

- Server Name: DMASERVER
- Host Name: local host or the IP address of the workstation on which the DMA server is running
- User Id and Password: not required

15 Click OK to add the server.

The server appears in the GMDR Servers area of the main window.

16 Click on DMASERVER in the servers list.

17 Click Connect.

18 In a UNIX access window, open file /opt/MagellanNMS/cfg/DmaClrPP.cfg and write down the group name and the associated user ID. You will need this information later.

Example:

:<Passport Group Name>:<User ID>::<encrypted password>:

19 In a UNIX access window, open file /opt/MagellanNMS/cfg/HGDS.cfg and look for an FGroup entry that matches the group name in file /opt/MagellanNMS/cfg/DmaClrPP.cfg.

Example: FGroup: ALL

20 You can use an existing FGroup entry in file /opt/MagellanNMS/cfg/HGDS.cfg or define the group entry with its associated members, then restart the HGDS server.

See “Reasons for Passport groups and guidelines for setting them up” (page 125).

21 Start the Command Console from the application main window by selecting **System -> Utilities -> Command Console**.

The **Connection Manager** Dialog opens.

22 Select **Connection Management** from the **Security** menu.

The **Command Console Connection Management** dialog opens.

23 Enter the group name and the user ID from file /opt/MagellanNMS/cfg/DmaClrPP.cfg into the Destination and User Id fields, and enter the associated password in the Password field.

24 Click **Connect.**

The information you entered is authenticated. When authentication is successful, the message Connected to <Passport group name> is displayed.

Example:

```
Connected to ALL
```

25 If authentication is successful the customer ID, scope, and impact may be insufficient for global alarm clearing. Go to step 27.

If authentication is not successful, one or more of the following may be the cause of the problem:

- The user ID and password assigned in file /opt/MagellanNMS/cfg/DmaClrPP.cfg may be invalid. Obtain the correct user ID and password from your Passport Administrator.
- The connection to this part of the network may be down.

26 Using the command line in Command console, type “<Passport_Name> me”.

Ensure that the user ID you are using has a customer ID of 0, and has the scope of network or device, and the systemAdministration privilege.

27 Click **Close**.

The **Command Console Connection Management** Dialog closes.

Troubleshooting a global alarm clearing problem (Global Clear tool)

Use this procedure to isolate the reason why the Global Clear tool does not work.

Procedure

1. Start the Command Console from the application main window by selecting **System -> Utilities -> Command Console**.

   The **Connection Manager** dialog opens.

2. Select **Connection Management** from the **Security** menu.

   The **Command Console Connection Management** dialog opens.

3. Enter the group name, the user ID, and the password.

4. Click **Connect**.

   The information you entered is authenticated. When authentication is successful, the message Connected to <Passport group name> is displayed.

   Example:

   ```
   Connected to ALL
   ```

   If authentication is not successful, one or more of the following may be the cause of the problem:

   - The user ID and password are invalid for that group.
   - The connection to this part of the network may be down.

5. Once authenticated, use the command line in Command console and type “<Passport_Name> me”.

   Ensure that the user ID you are using has a customer ID of 0, and has the scope of network or device, and the systemAdministration privilege.

6. Select **Connection Management** from the **Security** menu.

   The **Command Console Connection Management** dialog opens.

7. Select the connected group and click on **Disconnect.**

8. Reselect the group and enter new values in the User Id and Password fields.

9. Click **Connect**.

10 Click **Close**.

The **Command Console Connection Management** dialog closes.

Error messages

Error messages for the Global Clear requests using Global Clear tool are shown in the following table:

Table 4
Error messages Global Clear requests

Error message	Meaning and action
Alarm not existing on <Module name>.	The alarm has been cleared from the switch.
Insufficient capabilities to clear alarm on <Module name>.	The customer ID is not 0 and/or the scope is less than device and/or impact is less than systemAdministrator.
The Active Alarm List feature is not activated on <Module name>.	The AAL is not provisioned and activated on switch.
Authentication failed on <Module name>.	Wrong user ID and/or wrong password.
<Module name> is not part of any connected group.	The node is not part of any connected group from the Connection Console.
<Module name> is currently unreachable.	The node cannot be reached because of a network problem or the node is locked or down.
Alarm not found.	Default error message to map all other faults.
This type of alarm is not eligible for global clearing.	This type of alarm is not eligible for Global Clear. Only applicable to Passport and DNP-originated alarms.

Types of Passport alarm clearing

Three types of alarm clearing are available to clear Passport alarms: Local Clear, Global Clear, and Global Clear tool. It is recommended that only one of the Global Clear methods be configured by your administrator.

- "Local clear" (page 257)
- "Global clear" (page 257)
- "Global clear tool" (page 258)

A Preside Multiservice Data Manager (MDM) operator can delete alarms from the active alarm lists (AALs) with the Component Information Viewer (CIV) tool or the Alarm Display (AD) in active mode tool by selecting a specific alarm or alarms with the mouse and selecting local or global clearing from a popup menu. For information on clearing alarms, see the Alarm Display and Component Information Viewer sections in the 241-6001-011 *Preside MDM Fault Management User Guide*.

Local clear

Local alarm clearing lets an operator clear alarms locally from the GMDR database on a Preside Multiservice Data Manager (MDM) workstation. When an operator selects local clear with CIV or AD tool, the GUI applications sends a clear request to the GMDR databases. The alarm is then cleared from the GMDR databases on the workstation and the associated FMDR server(s).

Global clear

Global Clear lets an operator clear SET alarms from the Preside Multiservice Data Manager (MDM) servers and from the on-switch active alarm list (AAL). The main reason for removing SET alarms from the AALs is to clean up the lists so that only alarms of interest to the network operator remain. This makes monitoring easier.

Global Clear is initiated in several ways:

- From the Alarm menu by selecting Global Clear
- Using ManClear from a VT-100 terminal or in the UI of the Command Console (CC)

Clearing alarms using Global Clear from the Alarms menu allows many alarms to be cleared at once. Anyone from Alarm Display or Component Information Viewer can globally clear alarms that belongs to the node members of the specified groups in the DMA configuration file.

Global Clear and the ManClear macro uses the DMA architecture for clearing alarms. By default, Global Clear is available from the Alarms menu. Global Clear can be removed from the menu by touching the following file: opt/MagellanNMS/cfg/.DMAGlobalClearDisabled.

When the operator selects Global Clear from the CIV or AD tool, the DMA server sends a clear request to the GMDR databases to clear the alarm local on the workstation. The DMA server also logs on to the node using the information contained in file /opt/MagellanNMS/cfg/DmaClrPP.cfg. For details on how the DMA server performs this function, see the Data Manager Agent (DMA) in 241-6001-310 *Preside MDM Server Reference Guide*.

See “Setting up global alarm clearing for Passport” (page 247).

Network operators using VT100 access or the Command Console tool can delete alarms using the ManClear command with appropriate parameters. See the 241-6001-301 *Preside MDM Customization Administrator Guide* for more information on ManClear.

Global clear tool

The Global Clear tool lets an operator clear SET alarms from the Preside Multiservice Data Manager (MDM) servers and from the active alarm lists (AALs) on the switch. The main reason for removing SET alarms from the AALs is to clean up the lists so that only alarms of interest to the network operator remain. This makes monitoring easier.

Global Clear tool is initiated from the Alarm menu by selecting Start Tool ->Fault ->Global Clear of Alarm.

Clearing alarms using Global Clear tool from the Start Tool ->Fault menu allows only one alarm to be cleared at a time. Using the method, the user needs an up-front authentication with a group before globally clearing an alarm.

How alarms from Passport are collected and stored

In a Passport network, alarms from devices are stored in each individual Active Alarm List (AAL), if the AAL is installed and provisioned on the node. See Activating the Active Alarm List in the 241-6001-100 *Preside MDM Installation*.

These alarms remain in the AAL until the corresponding alarm has been cleared, or until the alarm is manually deleted. In both cases the alarm is removed from the AAL.

Lists of active alarms are collected and maintained in the following places:

- locally on the workstation in a database associated with the FMIP Management Data Router (FMDR) server and in the GMDR database
- in the AAL stored in the node.

When the FMDR server connects to nodes in a group, it requests a dump of each AAL of each node and uses it to update the FMDR database with all the current SET alarms that are not in the FMDR database (if there are discrepancies) and forwards them to GMDR. Once the connection between the FMDR and each node is established, any SET/CLR and MESSAGE alarms are automatically received, computed, and stored into the FMDR and GMDR database.

Alarms stored in the FMDR and GMDR databases can be cleared with local alarm clearing [local to the Preside Multiservice Data Manager workstation] or with global alarm clearing. However, alarms stored in the AALs of each node can only be cleared by means of global alarm clearing.

Chapter 15
Configuring server alarm distribution and workstation status probing

This section contains instructions for setting up the workstation to do the following:

- provide workstation server alarms to other workstations through a GMDR server
- provide workstation server alarms to the Network Control system (NCS) that runs on the DPN switches in your network
- set up the NCS so that it probes the workstation to determine the workstation's status

For a first time installation, you can use the information in this section to set up server alarm distribution and workstation status probing, or you can use the Preside Multiservice Data Manager (MDM) Software Configuration tool, as described in 241-6001-100 *Preside MDM Installation*.

See the following sections for more information:

- "About server alarm distribution and workstation status probing" (page 262)
- "Setting up server alarm distribution through GMDR" (page 263)
- "Setting up server alarm distribution through NCS and workstation surveillance using NCS status probing" (page 264)
- "Troubleshooting server alarm distribution through NCS and workstation surveillance using NCS status probing" (page 267)

About server alarm distribution and workstation status probing

There are two ways in which you can configure a workstation to distribute alarms and status changes from its Preside Multiservice Data Manager (MDM) servers to other workstations in the network.

You can configure the workstation to distribute them to a GMDR server that runs on the workstation, or that runs on another workstation. By setting up a hierarchy of GMDR servers on the MDM workstations in your network, it is possible to forward the workstation's alarms and status changes to some, or to all of the MDM workstations in your network. For a detailed description of how server alarms and status changes are propagated through GMDR, see 241-6001-310 *Preside MDM Server Reference Guide*.

You can also configure the workstation to distribute server alarms and status changes to the NCS that runs on the DPN switches in your network by forwarding them to an OA in the NCS over an X.25 link. The X.25 link connects to a Control Device Manager on the OA. The NCS propagates these alarms and status changes throughout the OAs on all DPN modules in the network. Any workstation that is configured to obtain surveillance information from the NCS receives these alarms and status changes and can display them. For a detailed description of how server alarms and status changes are propagated through NCS, see 241-6001-310 *Preside MDM Server Reference Guide*. This method of alarm distribution only applies to networks that contain DPN switches.

When setting up a connection to an OA to allow the workstation to have its server alarms and status changes distributed throughout network, it is also possible to specify a probing interval that is sent to the NCS in the data packets used to set up the connection over the X.25 link. The NCS uses the probing interval information to poll the workstation at regular intervals. After every poll, the NCS waits for an acknowledgment. If the NCS does not receive an acknowledgment, it creates a workstation alarm and propagates this alarm throughout the OAs in the NCS. Any workstation that is configured to obtain surveillance information from the NCS receives this alarm and can display it. For a detailed description of how server alarms and status changes are propagated using NCS, see 241-6001-310 *Preside MDM Server Reference Guide*.

Setting up server alarm distribution through GMDR

Use the following procedure to set up server alarm distribution through an IMDR server to a GMDR server that is running on this workstation or on another workstation.

If the IMDR server to which server alarms and status notifications are being forwarded is located on another workstation, this Preside Multiservice Data Manager (MDM) workstation and the workstation that is running the IMDR server must both be located on the same LAN. When the IMDR server is located on another workstation on the LAN, you must ensure that the hostname and IP address of the workstation that runs the IMDR server is defined in the file /etc/hosts on this workstation.

To have the server alarms and state change notifications propagated to more workstations than just the one on which the GMDR server resides, you must set up a hierarchy of GMDR servers once you have completed this procedure. For the instructions to set up a hierarchy of GMDR servers, see "Procedure steps" (page 451).

Setting up server alarm distribution through GMDR

1. Log on as root.

   Note: The root account must be set up to run the default Preside Multiservice Data Manager (MDM) user environment.

2. If you are going to distribute the alarms and state change notifications through an IMDR server that runs on another workstation, go to step 3. If not go to step 4.

3. Enter the following command:

   ```
   more /etc/hosts
   ```

   If the host name and IP address of the workstation that runs the IMDR server do not appear, you must enter them into this file. There are two ways to do this:

   - If your network uses a Naming Information Service (NIS), use Sun's Administration Tool Suite to define the hostname in NIS.
   - If your network does not use NIS, edit file /etc/hosts and insert the required hostname and IP address.

4. Using the Server Administration tool, stop the DMA server, if it is already running.

See “Logging out as administrator and accessing view mode” (page 379).

5 Edit the server information so that the DMA server starts up with the following command whenever the workstation is rebooted.

```
/opt/MagellanNMS/bin/dma \
-g <service name> -h <host name>
```

where:

`-g <service name>` specifies the service name for the IMDR server that is to receive the workstation server alarms and status changes. If you omit this option, the default service name of IMDR is used.

`-h <hostname>` specifies the name of the host on which the IMDR server that is to receive the workstation server alarms and status notifications. If you omit this option, they are distributed to the IMDR server on this workstation (localhost).

To enter the startup command and use it for rebooting, see “Editing a server” (page 377).

6 Use the GMDR Administration tool to configure the GMDR server to access the IMDR server (or servers) that you created to gather surveillance data. See “Procedure steps” (page 451).

For each IMDR server you need to provide:

- `Server Name` the name of the IMDR server in the form IMDR or IMDR_<service name>
- `Host Name` the host name or the IP address of the workstation on which the IMDR server is running
- `User/CapabilityID and Password` not required

7 Restart the DMA server.

8 To have the alarms propagated up a hierarchy of GMDR servers, use the instructions in “Procedure steps” (page 451) to set up the hierarchy.

Setting up server alarm distribution through NCS and workstation surveillance using NCS status probing

Use the following procedure to set up server alarm distribution through NCS and, optionally to set up NCS probing of the workstation’s status.

Before you start, you must first ensure that

- The HGDS and NCS Communications Manager (NCSMGR) servers are configured and running.

Setting up server alarm distribution through NCS and workstation surveillance using status probing involves the following main steps:

- editing file /opt/MagellanNMS/cfg/DmaOA.cfg to add the information that the DMA server needs to connect to the NCS
- starting the DMA server with arguments in its startup command to perform server alarm distribution and optionally, to have the NCS probe the workstation

Setting up server alarm distribution through NCS and surveillance using NCS status probing

1 Using a UNIX editor, open file /opt/MagellanNMS/cfg/DmaOA.cfg for editing.

2 Add a single statement to the file in the following format:

```
:DDD ... D:OO ...O:AAA ... A:CC:PPP:X:R:RPOA:
```

where:

D

is the Destination mnemonic. Maximum 12 characters

O

is the mnemonic of the NCS OA containing the destination's Control Device Manager. Maximum 12 characters. This mnemonic must match the OA name entered in the Name field of an OA Member in file /opt/MagellanNMS/cfg/HGDS.cfg.

A

is the DNA of the Control Device Manager. Maximum 16 characters.

Note: This is not the same as the DNA of the MDI access DNA.

C

is the CUG index of the Control Device Manager. Maximum 2 digits.

P

is the packet size on the VC. (Use 128, 256, or 512). Maximum 3 digits.

X

specifies whether the call is to be routed over X.75. Can be Y or N. If N, then R and RPOA are ignored.

R

specifies whether the calls are to be routed over the X.75 facilities of a Remote Private Operating Agency (RPOA). Can be Y or N. If N, the RPOA is ignored.

RPOA

is a code that identifies the RPOA. 4 (BCD) digits.

Example:

```
:CORENCSIF:CORENCS:3021015008:01:512:N:
```

3 Start the Server Administration tool by selecting System -> Administration -> Server Administration.

Note: Your user account must be set up run the NMSAdmin toolset at login to be able to see the Server Administration tool in the menus.

4 Using the Server Administration tool, stop the DMA server if it is already running.

See “Logging out as administrator and accessing view mode” (page 379).

5 Edit the server information so that the DMA server starts up automatically with the following command whenever the workstation is rebooted.

```
/opt/MagellanNMS/bin/dma \
-d [<filename] \
[-p <probing interval>]
```

where:

-d [<filename]

is the name of a file that contains the parameters needed to establish a connection to an OA. The connection is to be used for server alarm distribution through NCS and workstation surveillance using NCS status probing. If you specify the -d option without a file name, the default file / opt/MagellanNMS/cfg/DmaOA.cfg is used.

[-p <probing interval>]

specifies that status probing is to be performed for workstation surveillance. The <probing interval> is the interval in minutes at which NCS probes the workstation and it must be an integer with a minimum

value of 1. If you do not specify the <probing interval>, the default NCS status probe interval of five minutes is used.

See “Editing a server” (page 377).

6 Restart the DMA server.

See “Logging out as administrator and accessing view mode” (page 379).

Server alarm distribution through NCS with or without workstation NCS status probing is now configured.

Troubleshooting server alarm distribution through NCS and workstation surveillance using NCS status probing

If server alarm distribution (with or without NCS status probing) does not work once you have configured it, the most likely causes are configuration errors on the Preside Multiservice Data Manager (MDM) workstation. These are as follows:

- the DMA server is stopped or has not been started with the *-d* option
- if workstation surveillance using NCS status probing is desired, the DMA server has not been started with the -p option
- the NCS OA mnemonic (O) field in file /opt/MagellanNMS/cfg/DmaOA.cfg contains an OA name that does not appear the Name field of an OA Member defined in file /opt/MagellanNMS/cfg/HGDS.cfg
- the configuration parameters are incorrect in file /opt/MagellanNMS/cfg/DmaOA.cfg

Use the following procedure to troubleshoot the server alarm distribution through NCS and workstation surveillance using NCS status probing.

Before beginning this procedure you will need an NCS Capability ID (logon ID) and password that allows you to log into the OA through which workstation server alarms are to be distributed.

Isolating a problem with server alarm distribution through NCS, and workstation surveillance using NCS status probing

1 Start the Server Administration tool by selecting System -> Administration -> Server Administration.

Note: Your user account must be set up run the NMSAdmin toolset at login to be able to see the Server Administration tool in the menus.

2 Look for the DMA server in the servers list and double-click on it to view the server information.

The server must be Running, must be set to start at reboot, and the startup command must include the -d option. If workstation surveillance through NCS status probing is desired, the startup command must also include the -p option.

- If the server information is correct and the server is running, go to step 7.
- If the server information is correct but the server is not running, click on the DMA server in the server list, and select Start from the pop-up menu. Then go to step 7.
- If the server is not defined or the server information is incorrect, go to step 3.

3 Using the Server Administration tool, stop the DMA server, if it is already running.

See “Logging out as administrator and accessing view mode” (page 379).

4 Log in to the Server Administration tool as the administrator by selecting Enable Editing from the Security menu.

See “Editing a server” (page 377).

5 Edit the server information to ensure that the server starts automatically when the workstation reboots and that the startup command contains the -d option.

If you need to have workstation surveillance through NCS status probing, ensure that the startup command also contains the -p option. The command syntax is as follows:

```
/opt/MagellanNMS/bin/dma -d [<filename>] \
[-p [<probing interval]]
```

6 Start the DMA server.

7 Using a UNIX editor, open file /opt/MagellanNMS/cfg/DmaOA.cfg and write down the mnemonic of the NCS OA (OA name), and the DNA of the Device Control Manager. You will need this information later.

Example:
Mnemonic of the destination OA (OA name) = CORENCS
DNA of the Device Control Manager = 2862015009

8 Using a UNIX editor, open file /opt/MagellanNMS/cfg/HGDS.cfg and look for an OA Member whose Name field matches the mnemonic of the destination OA from file /opt/MagellanNMS/cfg/DmaOA.cfg (CORENCS in the example).

If there isn't one, define an OA Member in file /opt/MagellanNMS/cfg/HGDS that corresponds to the OA in file /opt/MagellanNMS/cfg/DmaOA.cfg, then restart the HGDS server using the Server Administation tool.

9 Start the Command Console by selecting System -> Utilities -> Command Console.

The Connection Manager Dialog opens.

10 Select Connection Management from the Security menu.

The Command Console Connection Management dialog opens.

11 In the dialog, enter the destination user ID, and password needed to log into the OA through which server alarms are to be distributed.

12 Click Connect.

The information you entered is authenticated. When authentication is successful, the message Connected to <OA Destination mnemonic> is displayed.

Example:

```
Connected to CORENCS
```

13 Click Close.

The Command Console Connection Management Dialog closes.

14 Enter the following command in the Command Console:

```
OA 1
```

Information similar to the following is displayed:

```
OK TABLE SIZE = 150   UNDEFINED = 144
PE 1 HOST R70 TYPE = OA
     NAME         TYPE            AP NUMBER / ROUTE
IWSIFC            COORDINATOR              0
CONTROL           DEVICE MGR             1 DEFAULT ROUTE
IWSIF             MDI                      2
```

15 Write down the host name, the PE number, the name of the Control Device Manager, and the AP/Route number of the Device Manager (R70, PE1, CONTROL, and 1 in the example).

16 Enter the following command to display the DNA of the Control Device Manager

<host> NCS <PE_number> <Device Manager Number> Q DNA

where:

`host` is the name of the module on which the OA is running (R70 in this example).

`PE_number` is the number of the PE on which the OA is running (1)

Example:

```
R70 NCS 14 1 Q DNA
```

A response containing the DNA of the Device Control Manager appears on the screen.

17 The DNA of the DNA of the Device Control Manager should match the DNA field in file /opt/MagellanNMS/cfg/DmaOA.cfg (2862015009 in the example).

If the DNAs do not match, modify the entry in file /opt/MagellanNMS/cfg/DmaOA.cfg then restart the DMA server using the Server Administration tool.

Chapter 16
Configuring workstation surveillance

This section contains instructions for configuring thresholds and logs output for workstation surveillance. Information is organized into the following sections:

Threshold configuration

The configuration file lets you customize the thresholds at which workstation surveillance generates alarms. You can also set the time interval at which the workstation polls its managed components. The configuration file also includes information on component-assigned fault codes. To change configuration parameters, run the /opt/MagellanNMS/bin/sfm_config script to create the following file:

/opt/MagellanNMS/cfg/sfm.config

You can edit the parameters in this file using any text editor. Prior to undertaking each poll, workstation surveillance reads the configuration parameters from this file. Only future alarms are affected; previous alarms are not affected.

The Server Administration tool requires the following entry to enable workstation monitoring:

/opt/MagellanNMS/bin/sfm

Note: For information on the logs generated by the Server Administration tool, see "Using the Server Administration tool" (page 359). For information on alarms generated by this tool, see 241-6001-501 *Preside MDM Alarms Reference Guide*.

When editing the sfm.config file, take the following points into consideration:

- you can edit and save this file while the scripts are running
- when defining numerical values, include only the number; do not add units
- for any resource, the value for the minor alarm must be lower than the value for the major alarm; the value for the major alarm must be lower than the value for the critical alarm
- always includes at least one space between the parameter name and the configurable value

The table "Configurable workstation surveillance parameters" (page 272) identifies the configurable parameters and the default values.

Table 5
Configurable workstation surveillance parameters

Configurable parameter	Default value	Description
Interval	30	Interval defines the polling interval in seconds. The range is 10-3660 seconds.
CPU_Load_Minor	70	CPU_Load_Minor, CPU_Load_Major, and CPU_Load_Critical define the threshold for minor, major, and critical CPU alarms in terms of percentage of CPU resource used. The range is 1 to 100.
CPU_Load_Major	80	
CPU_Load_Critical	90	
FS_Minor	80	FS_Load_Minor, FS_Load_Major, and FS_Load_Critical define the threshold for minor, major, and critical disk alarms in terms of percentage of disk resource used. The range is 1 to 100.
FS_Major	90	
FS_Critical	95	

(Sheet 1 of 3)

Table 5 (Continued)
Configurable workstation surveillance parameters

Configurable parameter	Default value	Description
Mem_Minor	80	Mem_Load_Minor, Mem_Load_Major, and Mem_Load_Critical define the threshold for minor, major, and critical memory alarms in terms of percentage of memory resource used. The range is 1 to 100.
Mem_Major	90	
Mem_Critical	95	
MDM_Conn		Remote_Connection peer Remote_Connection defines the IP addresses/host names of peer devices. Workstation surveillance periodically checks the connectivity with the IP addresses/host names assigned to the parameter. If you add a description for the managed IP addresses/host names, it will appear in the alarm contents field when the device is in connection alarms. The description should be separated from the IP address/hostname field by at least one space. This connection supports multiple field input, letting you manage more than one device. For example, to manage the connectivity with IP address 1.2.3.4 and host name testhost, input the following into your SFM.cfg file: Remote_Connection 1.2.3.4 Passport 15K Remote_Connection testhost MDM workstation Local_Port_Connection Local_Port_Connection defines the IP addresses/host names of the local port that you want to manage. SFM periodically checks the connectivity with the IP addresses/host names assigned to the parameter. If you add a description for the managed IP addresses/host names, it will appear in the alarm contents field when the device is in port alarms. The description should be separated from the IP address/hostname field by at least one space. This connection supports multiple field input, letting you manage more than one device. For example, to manage the connectivity with IP address 1.2.3.4 and host name testhost, input the following into your SFM.cfg file: Local_Port_Connection 1.2.3.4 Passport 15K Local_Port_Connection testhost MDM workstation

(Sheet 2 of 3)

Table 5 (Continued)
Configurable workstation surveillance parameters

Configurable parameter	Default value	Description
Manage_Port		Remote_Connection peer Remote_Connection defines the IP addresses/host names of peer devices. Workstation surveillance periodically checks the connectivity with the IP addresses/host names assigned to the parameter. If you add a description for the managed IP addresses/host names, it will appear in the alarm contents field when the device is in connection alarms. The description should be separated from the IP address/hostname field by at least one space. This connection supports multiple field input, letting you manage more than one device. For example, to manage the connectivity with IP address 1.2.3.4 and host name testhost, input the following into your SFM.cfg file: Remote_Connection 1.2.3.4 Passport 15K Remote_Connection testhost MDM workstation Local_Port_Connection Local_Port_Connection defines the IP addresses/host names of the local port that you want to manage. SFM periodically checks the connectivity with the IP addresses/ host names assigned to the parameter. If you add a description for the managed IP addresses/host names, it will appear in the alarm contents field when the device is in port alarms. The description should be separated from the IP address/hostname field by at least one space. This connection supports multiple field input, letting you manage more than one device. For example, to manage the connectivity with IP address 1.2.3.4 and host name testhost, input the following into your SFM.cfg file: Local_Port_Connection 1.2.3.4 Passport 15K Local_Port_Connection testhost MDM workstation
Manage_FS	/	Manage_FS defines which file systems that workstation surveillance monitors. Separate multiple file system entries with at least one space.
(Sheet 3 of 3)		

Log configuration for connectivity alarms

You can customize the 3011 0501 connectivity alarm to distinguish the Preside Multiservice Data Manager (MDM) workstation from the common device whenever a connectivity alarm occurs. This customization is achieved by editing the /etc/hosts file to add the following lines:

```
<xxx.xxx.xxx.xxx>    <host_name1>    #NMS_Server
<yyy.yyy.yyy.yyy>    <host_name2>
```

where:

<xxx.xxx.xxx.xxx> is the IP address of the MDM workstation at the other end of the connection.

<host_name1> is the DNS host name associated with the MDM workstation.

<yyy.yyy.yyy.yyy> is the IP address of the common device.

<host_name2> is the DNS host name associated with the common device.

Chapter 17
Configuring the Disruptive Command Safeguard

This section provides the instructions required to set up the Disruptive Command Safeguard feature. This feature only applies to DPN switches.

For initial installation, you can use the information in this section to configure the Disruptive Command Safeguard, or you can use the Preside Multiservice Data Manager (MDM) Software Configuration tool, as described in 241-6001-100 *Preside MDM Installation*.

See the following sections for more information:

About the Disruptive Command Safeguard feature

The Disruptive Command Safeguard is a command input management facility that intercepts potentially disruptive DPN commands entered from a Preside Multiservice Data Manager (MDM) workstation and presents a confirm or cancel message to the operator. The commands intercepted by the Disruptive Command Safeguard are defined in the /opt/MagellanNMS/cfg/DCS.cfg configuration file. You can enable, disable, or query the status of the Disruptive Command Safeguard from the application main window or from the UNIX command line.

The Disruptive Command Safeguard can be called from application programs such as the MDM VT100 operator facility or the Command Console. Systems built on top of the MDM VT100 operator facility using the RNCS primitives can take advantage of the disruptive command library in the same manner that the MDM VT100 operator facility does.

> ***Note:*** The Disruptive Command Safeguard facility does not apply to commands entered through local operator terminals connected directly to the operator port of a packet module or an NM, or to the DPN-50 based NCS VT100 operator terminal facility.

The /opt/MagellanNMS/cfg/DCS.cfg configuration file

The commands intercepted by the Disruptive Command Safeguard are defined in the /opt/MagellanNMS/cfg/DCS.cfg configuration file. A default file is supplied. See "The default /opt/MagellanNMS/cfg/DCS.cfg file" (page 279). You need to have root privileges in order to edit the file.

File format

The opt/MagellanNMS/cfg/DCS/.cfg configuration file consists of a series of lines, each having the following syntax:

```
<KEYWORD> <min_length> <NCS_CAPABILITY> [<MESSAGE>]
```

where:

`<KEYWORD>` is the command keyword for which you want to search

`<min_length>` is the minimum number of characters required to match the keyword

`<NCS_CAPABILITY>` is the user capability expressed in the format TYPE LEVEL IMPACT

`[<MESSAGE>]` is an optional message that is displayed with the confirm or cancel message

Example

Assume the /opt/MagellanNMS/cfg/DCS.cfg file contains the following line:

```
FORMAT 6 SWITCHING DEVICE PRIVILEGED Disk formatting
will cause instability
```

and the Preside Multiservice Data Manager operator issues the following command:

```
R72 2 DISK 0 FORMAT 2 1 R70 2 SEC 512 DIR 1000
```

If the operator has capability SWITCHING DEVICE PRIVILEGED, the Disruptive Command Safeguard facility instructs the NCS access tool to issue the prompt Disk formatting will cause instability, followed by confirm or cancel instructions.

If the operator does not have SWITCHING DEVICE PRIVILEGED capability, no message is issued, since the command is rejected by the module anyway.

The default /opt/MagellanNMS/cfg/DCS.cfg file

A default /opt/MagellanNMS/cfg/DCS.cfg file is included with the Preside Multiservice Data Manager (MDM) software. You can edit this file or use it as a template to create your own file. The contents of the file are shown in the figure "The default /opt/MagellanNMS/cfg/DCS.cfg file" (page 279).

Figure 20
The default /opt/MagellanNMS/cfg/DCS.cfg file

```
#
# Disruptive Command configuration file.
# Syntax:
# Command minimum-length NCS capability (TYPE LEVEL IMPACT) message
#
ACTIVATE 3 SWITCHING LINE CONFIGURATION
COMMIT 3 SWITCHING DEVICE CONFIGURATION
CONFIRM 4 SWITCHING DEVICE CONFIGURATION
DEREGISTER 3 NONE NONE NONE
DISABLE 7 SWITCHING DEVICE SERVICE
ERASE 5 SWITCHING DEVICE PRIVILEGED
FILTER 1 NAMS NETWORK CONFIGURATION
FORMAT 6 SWITCHING DEVICE PRIVILEGED
LOAD 4 SWITCHING DEVICE PRIVILEGED
REFUSE 6 SWITCHING LINE SERVICE
REGISTER 3 NONE NONE NONE
RELOAD 6 SWITCHING DEVICE PRIVILEGED
RESET 5 SWITCHING DEVICE CONFIGURATION
RESTART 7 SWITCHING DEVICE PRIVILEGED
STOP 4 SWITCHING LINE SERVICE
```

Checking, enabling, and disabling the Disruptive Command Safeguard

Preside Multiservice Data Manager (MDM) provides a Disruptive Command Safeguard menu. You can access the menu items from the application main window by selecting System -> Security -> Disruptive Command Safeguard. This toolset is not available when the MDM session launches toolset User.tsets.

MDM Disruptive Command Safeguard menu

The Disruptive Command Safeguard menu provides the following commands:

- Check Status tells you if the Disruptive Command Safeguard is enabled or disabled.
- Enable Safeguard enables the Disruptive Command Safeguard.
- Disable Safeguard disables the Disruptive Command Safeguard.

  Note: The Disruptive Command Safeguard is disabled when Preside Multiservice Data Manager (MDM) is first installed.

See also “Using the Disruptive Command Safeguard” (page 280).

Using the Disruptive Command Safeguard

Use the following procedures to check (query) enable, or disable the Disruptive Command Safeguard from the Preside Multiservice Data Manager (MDM) main window or from a UNIX command line.

Querying, enabling, or disabling the Disruptive Command Safeguard from the menu

1. Log in as root.
2. From the application main window, select System -> Security -> Disruptive Command Safeguard, and one of the following items from the cascading menu:
   - Select Enable Safeguard to have MDM intercept disruptive commands as defined in the /opt/MagellanNMS/cfg/DCS.cfg file.
   - Select Disable Safeguard so that MDM does not intercept disruptive commands as defined in the /opt/MagellanNMS/cfg/DCS.cfg file.

- Select Check Safeguard Status to check whether the Disruptive Command Safeguard is enabled or disabled.

Querying, enabling, or disabling the Disruptive Command Safeguard from the UNIX command line

1 Log in as root.

2 Enter one of the following commands in a UNIX access window:

`/opt/MagellanNMS/bin/dcstool -e`

to enable the Disruptive Command Safeguard so that MDM intercepts disruptive commands as defined in the /opt/MagellanNMS/cfg/DCS.cfg file.

`/opt/MagellanNMS/bin/dcstool -d t`

to disable Disruptive Command Safeguard so that MDM does not intercept disruptive commands as defined in the /opt/MagellanNMS/cfg/DCS.cfg file.

`/opt/MagellanNMS/bin/dcstool -c`

to return a value indicating whether the Disruptive Command Safeguard is enabled or disabled.

Chapter 18
Synchronizing the network time

This section describes Network Time Synchronization (NTS) for Preside Multiservice Data Manager (MDM) and contains procedures for setting up NTS on MDM workstations.

If you already understand how NTS applies to MDM, have planned the timing relationships for your network, and only need to locate the instructions to configure NTS, see “Tasks to set up NTS” (page 306).

If you do not understand how NTS applies to MDM, read “Overview of Network Time Synchronization (NTS)” (page 284) and “Tasks to set up NTS” (page 306).

See the following sections for more information:

- “Overview of Network Time Synchronization (NTS)” (page 284)
- “Tasks to set up NTS” (page 306)
- “Defining an Internet clock as a time source for the primary time server” (page 311)
- “Defining a precise timing device connected directly to the workstation as a time source for the primary time server” (page 313)
- “Defining the internal clock as a time source for the primary time server” (page 313)
- “Defining a DPN OA as a time source on the primary time server” (page 316)

Overview of Network Time Synchronization (NTS)

The overview contains the following sections:

What is NTS

The Network Time Synchronization (NTS) system synchronizes the time of day on Preside Multiservice Data Manager (MDM) workstations and network elements, and ensures that

- time clocks on workstations and network elements show a consistent time of day
- accounting records, alarms, statistics and logs bear a consistent timestamp

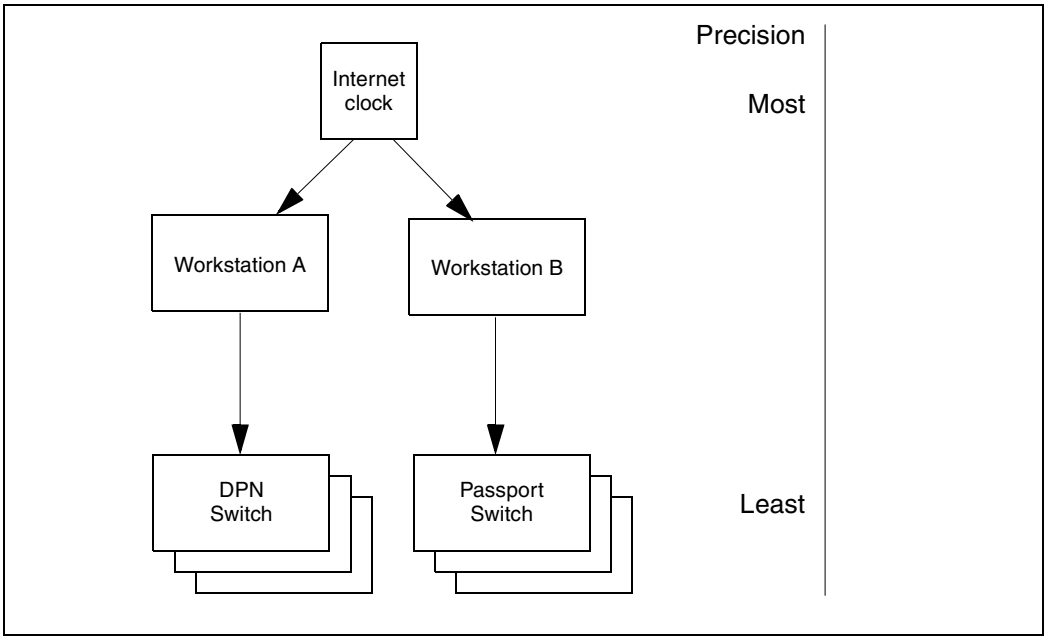
Note: NTS has nothing to do with clocking on synchronous data links—only with synchronizing the time of day.

When NTS is installed, the MDM workstations and network elements form a timing hierarchy in which each device obtains its time of day from a time source, and optionally, acts as a time source for one or more network elements, as shown in figure "A simple timing hierarchy" (page 286).

As you descend the hierarchy, the precision of clocks in network elements decreases. Devices with the most precise clocks are at the top of the hierarchy, and devices with the least precise clocks are at the bottom of the hierarchy.

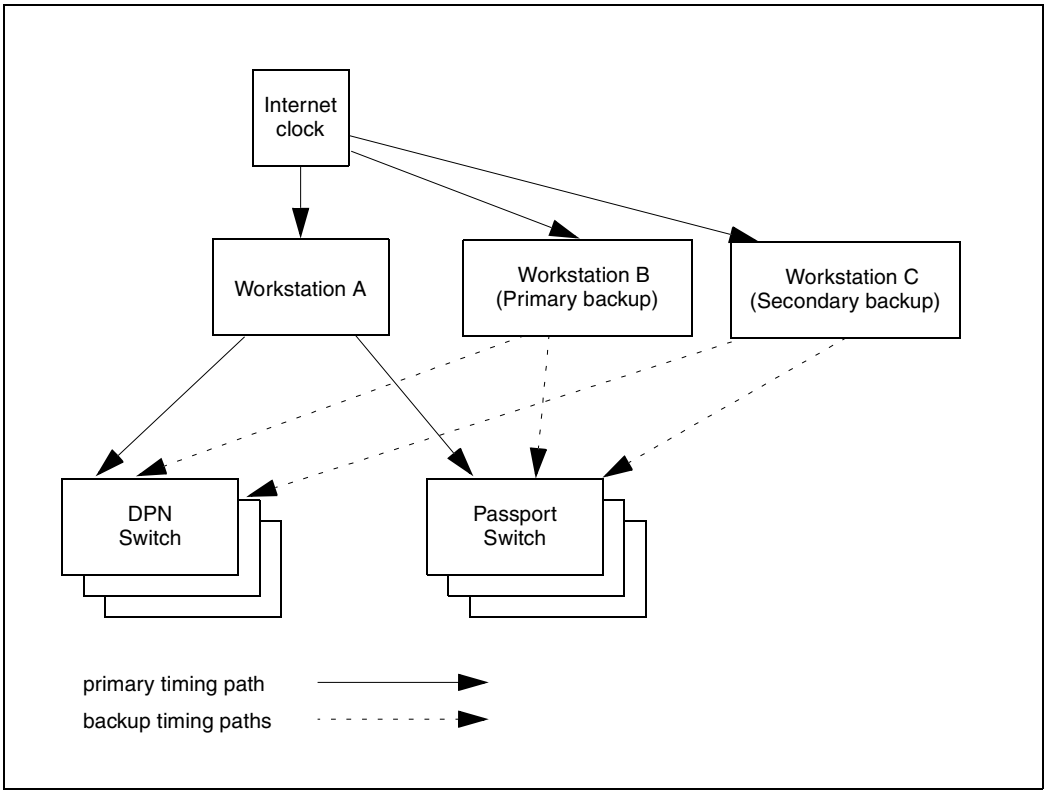
Network elements in a timing hierarchy that provide the time to other devices are known as time servers and those that receive the time are time clients. In the figure "A simple timing hierarchy" (page 286), the Internet clock is the time server for workstations A and B. Workstation A is a time server for the DPN switches and workstation B is a time server for the Passport (Passport) switches. The DPN switches are time clients of workstation A and the Passport switches are time clients of workstation B. Devices containing clocks that have the same precision are known as peers. In the figure "A simple timing hierarchy" (page 286), workstations A and B are identical and have the same precision clock; therefore, they are peers. Peers can obtain the time or provide the time to one another.

Figure 21
A simple timing hierarchy



The relationships shown in the figure "A simple timing hierarchy" (page 286) are oversimplified. In a real timing hierarchy, devices are provisioned as backups. An example of a timing hierarchy with backups is shown in the figure "A timing hierarchy with backups" (page 287). In this figure, the workstations use an Internet clock as a time server. If workstation A fails, primary backup workstation B provides the time to the DPN and Passport switches. If workstations A and B both fail, secondary backup workstation C provides the time to them. Many other backup arrangements are also possible.

Figure 22
A timing hierarchy with backups



Timing relationships are complex, especially in large networks with many backups. Before you can configure NTS on a Preside Multiservice Data Manager (MDM) workstation, ensure that you understand the possible timing arrangements between workstations and other devices in the network. These arrangements are described in the following sections.

What a workstation can have as a time server

A Preside Multiservice Data Manager (MDM) workstation can use several time sources as a time server to set the time of day on its internal clock. These sources are shown in the figure, “What a workstation can use as a time server” (page 290).

In the most basic arrangement, the MDM workstation uses its own internal clock as a time server. The internal clock is the easiest time source to define because it requires no IP connections to an external clock, and no expensive equipment hardware such as a radio clock. The drawbacks to using the internal clock are as follows:

- the internal clock is relatively inaccurate compared with other types of time sources
- each time you wish to update the time you must manually enter the UNIX date command
- updating the time requires frequent and consistent monitoring and intervention by a human operator

Other more precise possibilities include

- a precise timing device that is connected directly to the workstation, such as a radio clock

  A radio clock is designed to receive time signals broadcast from a radio transmitter that uses a national time standard clock, such as an atomic clock, as its time reference.

- a clock that is accessible through the Internet

  The Internet contains a number of primary time servers that are synchronized to national time standard clocks by wire links or radio links. These primary time servers are also connected to one or more secondary time servers throughout the Internet and are kept in synch with the primary time servers by XNTP software that runs on the time servers. You can access a primary or a secondary Internet server and use it as the time source for your network.

- the clock in another workstation

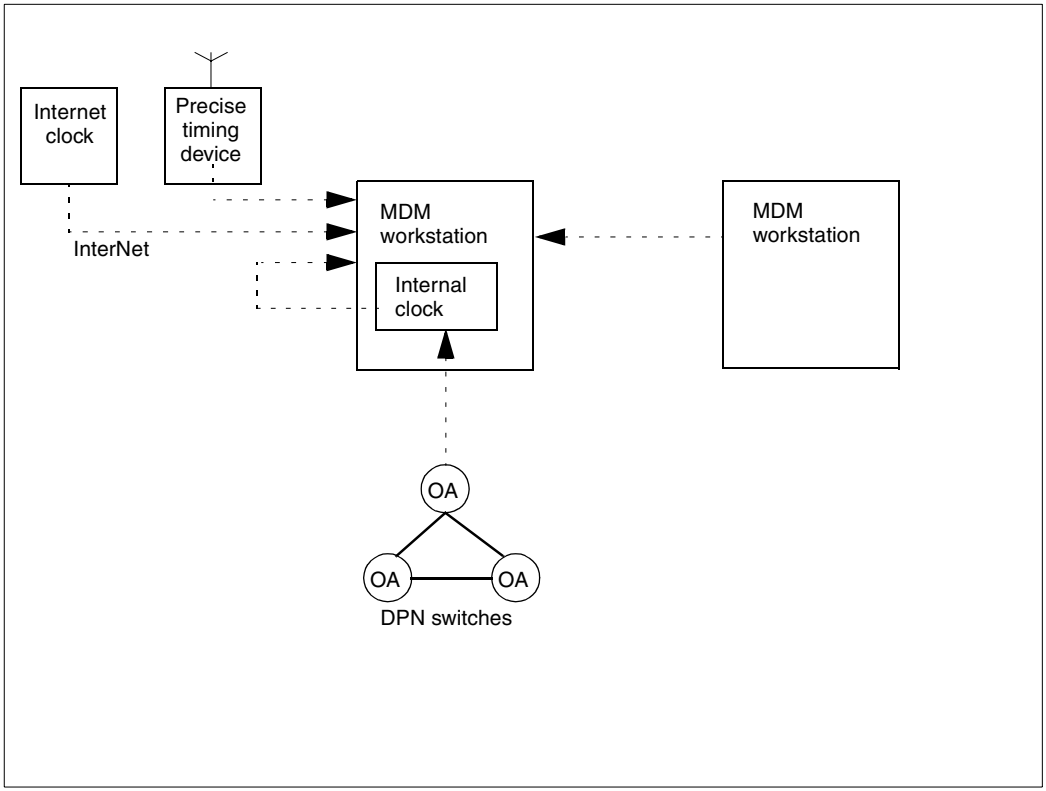
  You can do this when your network contains several workstations and one of them is connected to an accurate time source, such as a radio clock.

- a DPN operations agent (OA)

  In an existing DPN-100 network, the OAs may already be configured so that they synchronize with an accurate clock, such as a radio clock or an atomic clock. In such a situation, you can use an OA as a time source. Because the time on all DPN OAs is kept in sync by the Top DPN OA, any OA can be used as the time source.

You can configure the software on an MDM workstation to access more than one time source to provide backup. However, when you use a DPN OA as a time source, do not configure any other time source for the workstation. If you do, the cron job used to synchronize the workstation to the DPN OA, and the XNTP software used to synchronize the workstation to the other time sources will both attempt to reset the workstation's time. This will lead to timing conflicts and fluctuations.

Figure 23
What a workstation can use as a time server



What a workstation can have as a time client

A Preside Multiservice Data Manager (MDM) workstation can act as a time server for the following time clients:

- another workstation

  When your network contains several workstations, you may want to have one workstation act as a time server for other MDM workstations.

- the TopOA for Network Control System (NCS) that runs on the DPN switches in your network

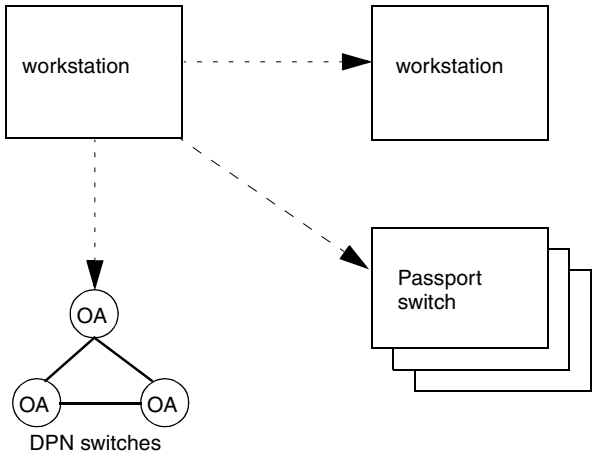
  In some networks, the workstations may have access to a time server that is more precise than any of the existing time sources for the DPN switches. In this situation, you can configure the workstation to provide the time to the Top OA. Because the Top OA synchronizes the time on all DPN OAs, all DPN switches will synchronize their time to the workstation.

  The workstation can only provide the time to the DPN switches or obtain the time from them, it cannot do both.

- Passport (Passport) switches in your network. MDM workstations are the only possible time servers for these switches. If your network contains Passport switches, at least one of the workstations must be configured to act as their time server.

  Note: To act as a time server for Passport switches, an MDM workstation must be connected to the switches by a connection that runs the FMIP protocol. If any other protocol is used, the switches cannot synchronize to the workstation.

Figure 24
What a workstation can have as a time client



Note: An MDM workstation can only provide the time to the DPN switches or obtain the time from them.

Note: If your network contains any Passport switches, at least one workstation must have XNTP software running on it so that it can act as a time server for the switches.

How workstations synchronize the time with everything except DPN

To synchronize the time on Preside Multiservice Data Manager (MDM) workstations, Passport (Passport) switches, and external clocks such as an Internet clock, NTS uses XNTP software installed on each of these devices.

What is XNTP

XNTP is an Internet Standard Recommended Protocol that is built on two protocols: the Internet Protocol (IP) and the User Datagram Protocol (UDP). Although it was developed for synchronizing and distributing the time throughout the Internet, XNTP can be used to synchronize and distribute the time among most network elements that are connected by an IP link. Internet

clocks, Preside Multiservice Data Manager (MDM) workstations, and Passport switches support IP and can run XNTP. As a result, XNTP can be used to synchronize and distribute the time among these devices.

> ***Note:*** Because workstations use X.25 to communicate with DPN switches, a means other than XNTP must be used to synchronize the time on workstations with DPN switches. This task is performed by the syncToDPNtime, syncDPNtime, and syncDPNtime.backup programs described in "How workstations synchronize the time with DPN" (page 303).

XNTP and the Internet

The Internet contains a number of primary time servers that are synchronized to national time standard clocks by wire links or radio links. These primary time servers are connected to one or more secondary time servers throughout the Internet and are kept synchronized to the primary time servers using XNTP. You can configure XNTP on a workstation to access a primary or a secondary Internet server and use it as the time source for the Preside Multiservice Data Manager (MDM) workstations and the Passport switches in your network.

With XNTP, the Internet time servers calculate clock offset and delay between them using timestamps with a resolution of 200 picoseconds that are exchanged at intervals of up to 1000 seconds.

For a detailed description of XNTP, see "Mills, David L. *RFC-1305 Network Time Protocol (Version 3) Specification and Implementation*, University of Delaware, 1992."

XNTP, workstations, and Passport switches

XNTP installed on Preside Multiservice Data Manager (MDM) workstations and Passport (Passport) switches runs as an XNTP subnetwork. Once installed and configured, XNTP performs the following functions:

- automatically select the network element with the most precise clock (lowest stratum number) available from a pool of time servers that are configured on the workstation

  If the network element fails, the XNTP software automatically selects the next most precise time source until it runs out of time sources. Then it uses the workstation's internal clock as a time source.

  If a local clock is configured as a time source along with other time sources, XNTP always uses the workstation's internal clock as the network element of last resort, regardless of its precision relative to the other time sources.

- keep the time synchronized to the device that XNTP selects as the current time server

To determine which network element to use, XNTP software dynamically assigns a stratum number to the device on which it is running. The stratum number indicates the relative accuracy of the clock compared with the clocks on other network elements available. The stratum number ranges from 0 for very precise clocks, such as atomic clocks, to 15 for the least precise clocks. For any given device in a network XNTP dynamically calculates the stratum number of the network element's clock to be a lower value than that of its time server because the server is higher up the timing hierarchy. When XNTP chooses a network element to use as a time source, it selects the network element with the lowest stratum number first, then the next lowest, and so on, until it runs out of configured devices.

To install and configure XNTP on an Preside Multiservice Data Manager (MDM) workstation, you can run the ntsinstall program provided with the MDM software. You can run *ntsinstall* on every workstation that

- uses its internal clock, an Internet clock, or another workstation as a time server
- has a Passport switch or another workstation as a time client

Note: Before running ntsinstall, the administrator should first remove any existing entries for xntpd in the SVMList.cfg file.

The ntsinstall program lets you set up or modify the NTS configuration on an workstation. The configuration data is stored in a configuration file (/opt/MagellanNMS/cfg/NTS.cfg). For details about ntsinstall and the statements in the configuration file, see “About ntsinstall” (page 299).

XNTP and Passport switches

Passport (Passport) switches can obtain the time from Preside Multiservice Data Manager (MDM) workstations, or other time servers. To obtain the time from a workstation, the switches must be connected to at least one workstation with XNTP installed and configured with the ntsintall program. The switches retrieve the time by polling all accessible workstations to which an FMIP connection running over IP exists and determining the best time server to use according to the clock selection algorithm detailed in XNTP specification RFC-1305 Network Time Protocol (Version 3) Specification and Implementation, University of Delaware, 1992. The switches cannot synchronize the time to each other using XNTP, they can only obtain it from an MDM workstation.

There is currently a restriction for XNTP and switches. To act as a time server for Passport switches that are configured as a LAN, a workstation must be connected to the switches by a connection that runs FMIP protocol. If any other protocol is used, XNTP running on the switches is unable synchronize to the workstation.

A Passport switch selects the best available time reference from an internal list of available time servers and continues to obtain its network time by polling the same server until one of the following events occurs:

- The current time server fails or does not respond to a poll.
  The switch software chooses a new source from the list of available time servers.
- The FMIP connection to the current time server shuts down.
  Switch software removes the IP address of that time server from its time server list and chooses an alternate time server.

- A new time server is added to the time server list from a new FMIP connection and XNTP determines that the new time server is more accurate (has a lower stratum number) than any existing time server.
- The switch is reset.
  The switch must wait for MDM servers to re-establish FMIP connections.

  Note: Passport switches cannot maintain or re-establish lost FMIP connections. Once an FMIP connection is lost, software removes the corresponding network address from the time server list. When no time servers remain in the time server list, XNTP continues to run, using the last received network time, until an FMIP connection is re-established.

Time adjustment and polling frequency on workstations and Passport

Time synchronization attributes are found under the Passport (Passport) switch time component. The time component consists of the following attributes:

- syncSource
  indicates the possible sources the switch can synchronize to. The syncSource is usually a Preside Multiservice Data Manager (MDM) workstation.
- syncStatus
  indicates whether the switch is synchronized, unsynchronized, or synchronizing to a source
- moduleTime
  indicates the current date and time on the switch. If the syncStatus is unsynchronized, you can set the time on the switch independent of a synchronized source.
- mainServer
  indicates which of these sources the switch is synchronizing to since you may have many possible synch sources for redundancy

With Passport, you can add a provisionable subcomponent under the Server time component. Provision the IP address of the source you want the switch to synchronize to. The source is usually the MDM workstation. You can also indicate the connection method to this source. The connection choices are as follows:

- vrlp (virtual router, used with Ethernet connectivity)
- ipiFrIPiVc, which is used if the workstation is connected by ipiFR or ipiVC. If you are using ipiFR, the Frame Relay daemon must be running on the workstation. To check this, enter the command at the UNIX prompt:

  ```
  ps -ef | grep frd
  ```

The times on the switch and the syncSource must be within 1000 seconds of each other before the switch will synchronize to another source. If the two are not within 1000 seconds of each other, lock the time server component and then set the module time on the switch to be within 1000 seconds of the source. The time component must be locked because the switch will continue to synchronize and you cannot independently set the time on the switch unless the component syncStatus is unsynchronized.

The procedure, "Synchronizing the time between Passport and the workstation" (page 297) synchronizes the network time. See NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.

Synchronizing the time between Passport and the workstation

1. Stop the time synchronization on Passport (Passport) and a workstation. On the switch, lock all the provisioned time server components for each provisioned server:

   ```
   lock Time Server/<n>
   ```

2. Ensure that the switchtime changes to unsynchronized:

   ```
   d Time syncStatus
   ```

3. The MDM XNTP daemon and the Passport XNTP daemon are used for time synchronization. The MDM XNTP daemon is the Solaris-provided software on the workstation, and the Passport XNTP daemon is the client. Determine whether the daemon is running on MDM by entering the following command at the UNIX prompt:

```
ps -ef | grep xntp
```

WARNING
Out of service
The time server should not be kept out of service for too long to avoid impacting the network, especially if there is no redundant time server configured in the network. The length of time the server should not be out of service varies because it depends on the time drift of the clocks. The average time drift depends on the hardware involved.

4 If the process is still running, terminate the workstation XNTP daemon by entering the following command at the UNIX prompt:

```
kill <process number>
```

5 Ensure that the process has been killed:

```
ps -ef | grep xtnp
```

6 Line up the time on the switch with the time on the workstation. To display the time, from UNIX, type

```
date -u
```

7 On the switch, make sure that the time offset is set to 0. Configure the switch time so that it is set to UTC, and as close as possible to the workstation UTC time: (less than 1000 seconds of UTC):

```
set time offset 0
set time moduleTime <yyyy-mm-dd hh:mm:ss>
```

Note: Root permission is required to change the workstation time. Use the date -u command.

8 Using the NTPQ tool, ensure that the workstations are in sync with their time source before doing anything with the switches.Type:

```
/usr/sbin/ntpq
```

9 At the prompt, type

```
ntpq> peers
```

```
   remoterefidsttwhenpollreachdelayoffsetdisp
==============================================================================
*LOCAL(3)      LOCAL(3) 3 1  26  64  377 0.00 0.5009.75
```

Watch the disp attribute. This attribute indicates the frequency for polling for messages being passed between the switch and the workstation. This value continues to decrease. When it reaches 10.01, the workstation is synchronized to the time server.

10 On the switch, restart synchronization by unlocking the time server components:

```
unlock Time Server/<n>
```

11 Monitor the progress by checking the syncStatus attribute:

```
d Time syncStatus
```

Note: All workstations used as synchronization sources for a switch need to be provisioned as time servers on the switch.

12 After the switch has reached synchronization, that is syncStatus=synchronized, configure the time offset on the switch:

```
set Time offset <user value>
```

Note: Nortel Networks recommends that your networks be operated with the time offset of 0 (on UTC). If you use local time by setting the offset attribute to a non-zero value, then the offsets on all the switches in the network must be the same. Failure to do so may result in difficulties when correlating time between multiple switches.

Variable definitions

Variable	Definition
<n>	is the instance of the server component
<process number>	is the process number of the workstation XNTP daemon
<n>	is the instance of the server component
<user value>	is the value for the offset according to your time zone

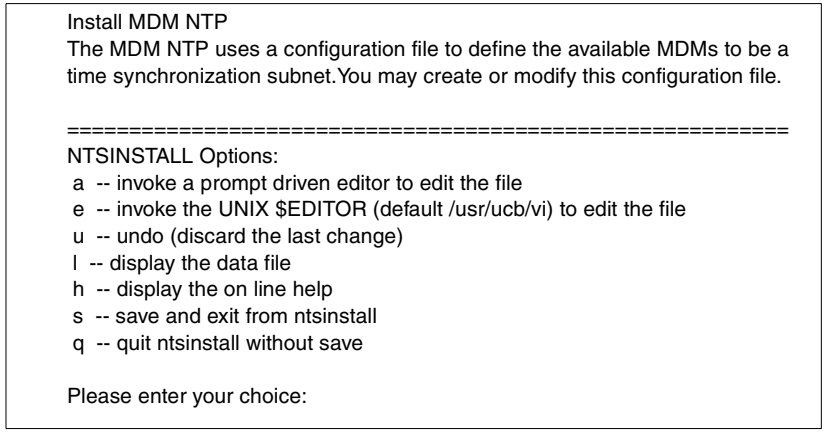
About ntsinstall

The ntsinstall program lets you set up or modify the XNTP configuration for a Preside Multiservice Data Manager (MDM) workstation. The configuration data is stored in a configuration file (/opt/MagellanNMS/cfg/NTS.cfg) that defines the servers and peers for the workstation and lists their IP addresses.

The ntsinstall program provides the main menu shown in the figure "Main menu of ntsinstall" (page 300). This menu lets you to do the following:

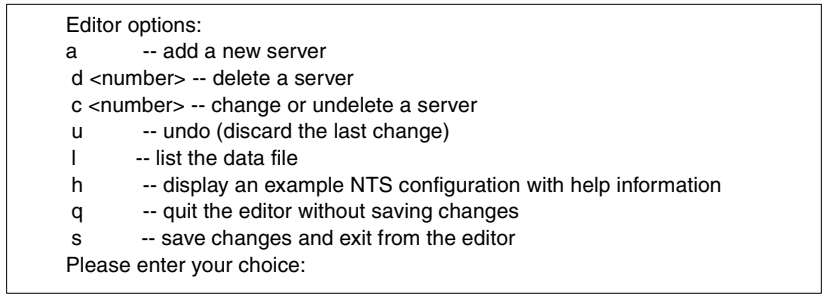
- configure the /opt/MagellanNMS/cfg/NTS.cfg file by responding to a series of prompts
- start a UNIX editor to edit the /opt/MagellanNMS/cfg/NTS.cfg file
- display the contents of the /opt/MagellanNMS/cfg/NTS.cfg file
- display help information

Figure 25
Main menu of ntsinstall



Entering **a** on the main menu to select the prompt driven editor displays the submenu shown in the figure "Edit submenu" (page 301).

Figure 26
Edit submenu



The options on this submenu are as follows:

`a`

add a new server or peer to the NTS.cfg file by responding to a series of prompts requesting data for each field in the file

`d <number>`

delete the line in the file with the specified line number. Use the *l* command to find the line number of the server you want to delete

`c <number>`

change the specified line in the file by responding to a series of prompts requesting new data for each field in the file. Enter new data or press return to leave the field unchanged

`u`

revert to the version of the file that existed before you made the last change

`l`

display the contents of the configuration file

`h`

display the online help for ntsinstall

`q`

quit the editor without saving any changes

`s`

save the changes made during the current session and exit from the editor

About the NTS.cfg configuration file

Each Preside Multiservice Data Manager (MDM) workstation running XNTP in a network must have a /opt/MagellanNMS/cfg/NTS.cfg file that defines its servers, its peers, and their IP addresses. This file also contains the statement driftfile /opt/MagellanNMS/cfg/NTSdrift.cfg.The NTSdrift.cfg file is an internal data file used by the XNTP protocol.

You can use the ntsinstall program to configure or modify the file. The file consists of a series of lines, one for each server or peer defined on the workstation. Each line in the file conforms to the following syntax:

```
<node_type> <IP_address>\
[version <XNTP_version>] [#<comment>]
```

where:

`<node_type>`

identifies the line as defining a server or a peer. For instructions to determine the servers and peers of a MDM workstation, see “Determining the servers and peers for XNTP on workstations” (page 323).

`<IP_address>`

is the IP address of the server or peer

`[version <XNTP_version>]`

is an optional field that is used for specifying the version of XNTP software that is running on the server or peer. You only need to specify the version if the server or peer is running version 1 or version 2 XNTP software. If you are not sure of the version you are running, omit this parameter.

`#<comment>`

is an optional field for adding comments

You can insert blank lines into the file. You can also include comments, provided you precede them with a # symbol.

Determining the XNTP version

Perform the following procedure to find out the version of XNTP that is running on your workstation.

1. Type the command:

   `/user/sbin/xntpdc`

2. Request the version number:

   `version`

   The version of XNTP is displayed.

3. Exit the shell:

   `quit`

How workstations synchronize the time with DPN

Because DPN switches have no direct access to XNTP (no IP connection for network management purposes), the time on a Preside Multiservice Data Manager (MDM) workstation and the time in a DPN network must be exchanged by means of programs that are run by a cron job on each workstation. The programs, called syncDPNtime, syncDPNtime.backup, and syncToDPNtime, are provided with the MDM software.

The workstations can either obtain the time from the DPN switches or provide the time to them.

Providing the time to DPN switches

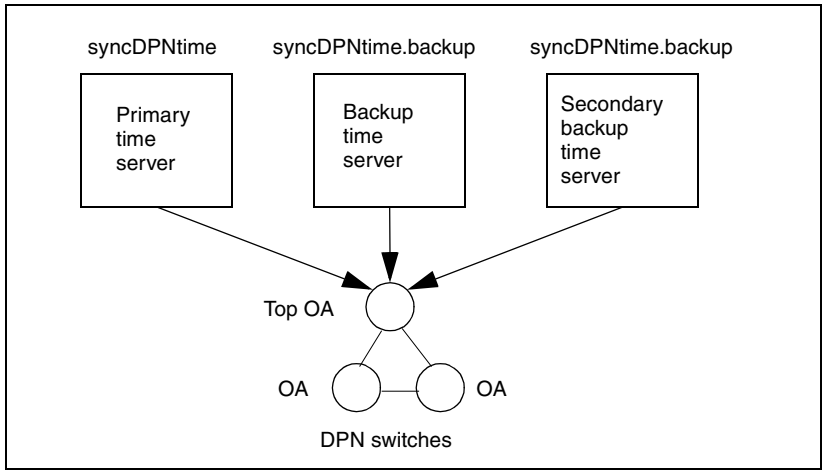
On each Preside Multiservice Data Manager (MDM) workstation that provides the time to DPN switches and maintains time synchronization, you must schedule a cron job to run one of two programs: syncDPNtime or syncDPNtime.backup.

If you have more than one workstation in your network, choose one of them as the primary time server for the DPN switches, a second as backup time server, and a third (if available) as a secondary backup time server. If you have only one workstation, choose it as the primary time server.

On the MDM workstation you choose as the primary time server, schedule the cron job to run the syncDPNtime program as shown in the figure "Programs to run to provide the time to DPN" (page 305). On the workstations that are the backup and secondary backup time servers, schedule the cron job to run the syncDPNtime.backup program.

These two programs establish a connection to the DPN Top OA and send the workstation time. The Top OA provides the time of all other DPN OAs and synchronizes them to that time. The difference between the two programs is that the syncDPNtime.backup also monitors other workstations that are acting as time servers for DPN to determine if it should provide the time to the Top OA.

Figure 27
Programs to run to provide the time to DPN



Obtaining the time from DPN switches

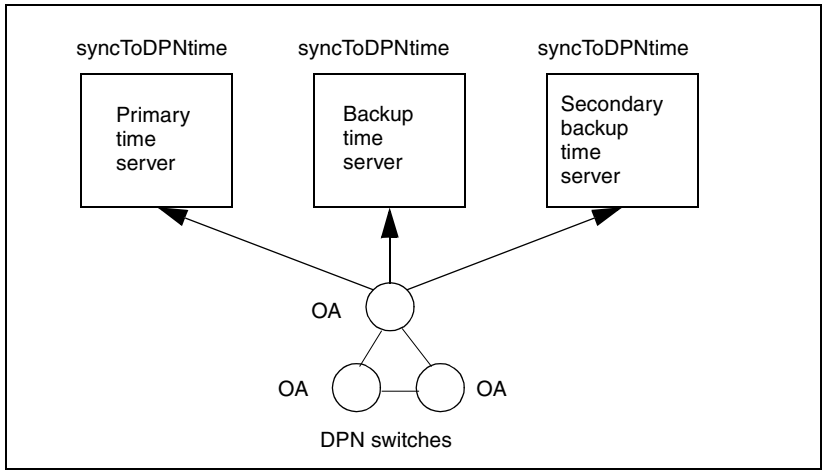
On each Preside Multiservice Data Manager (MDM) workstation that obtains the time from DPN switches and maintains time synchronization, schedule a regular cron job to run the syncToDPNtime program.

Schedule the cron job to run the syncToDPNtime program on each of the workstations obtaining the time from DPN, regardless of whether the workstation is a primary, backup, or secondary backup time server for your network. See the figure “Program to run to obtain the time from DPN” (page 306).

The function of this program is to set up a connection to a DPN Operations Agent (OA), get the DPN time, and set the time on the internal clock of the MDM workstation.

To set up an workstation to obtain the time to DPN, see “Setting up the backup and secondary backup time servers to obtain the time from a DPN OA” (page 331).

Figure 28
Program to run to obtain the time from DPN



Tasks to set up NTS

This section contains a procedure to set up NTS in your network. If you are not familiar with NTS, read “Overview of Network Time Synchronization (NTS)” (page 284).

For first-time installations, you can also use the Preside Multiservice Data Manager (MDM) Software Configuration tool, as described in 241-6001-100 *Preside MDM Installation*.

There are many ways to connect the devices in your network to time sources, arrange timing dependencies between them, and to provide backups. The procedure, “Configuring NTS in your network (suggested method)” (page 309) is satisfactory for most networks.

The procedure asks you to choose one MDM workstation as a primary time server for your network, a second (if available) as a backup time server, and a third as a secondary backup time server. It also asks you to choose an accurate clock accessible through a DPN OA or one or more of the following time servers as the time source for your network:

- an Internet clock
- a precise timing device such as a radio clock

- the internal clock in the workstation

The three workstations provide the time to any Passport switches in the network and act as backups.

For a sample configuration produced by the procedure when you choose a DPN OA as the time source for your network, see the figure "Network that uses a DPN OA as a time server" (page 307). For a sample configuration when you choose any other device the time source, see the figure "Network that uses anything other than a DPN OA as a time server" (page 308).

Figure 29
Network that uses a DPN OA as a time server

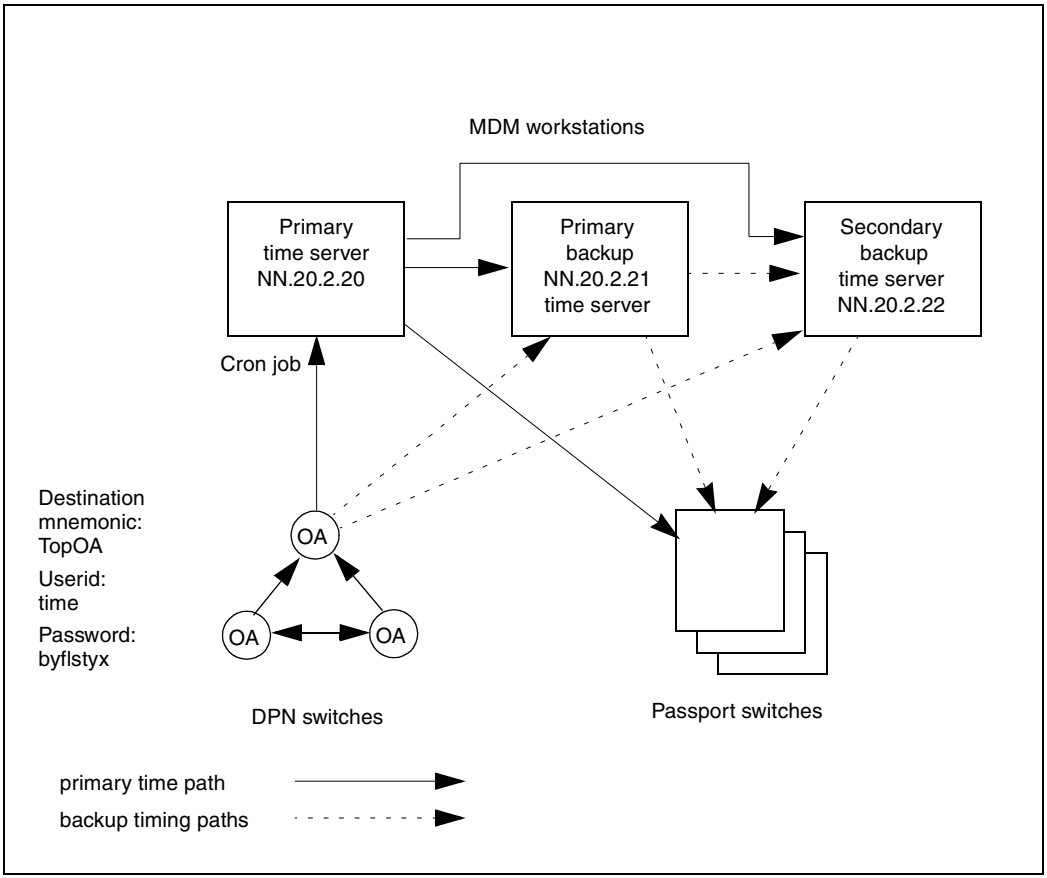
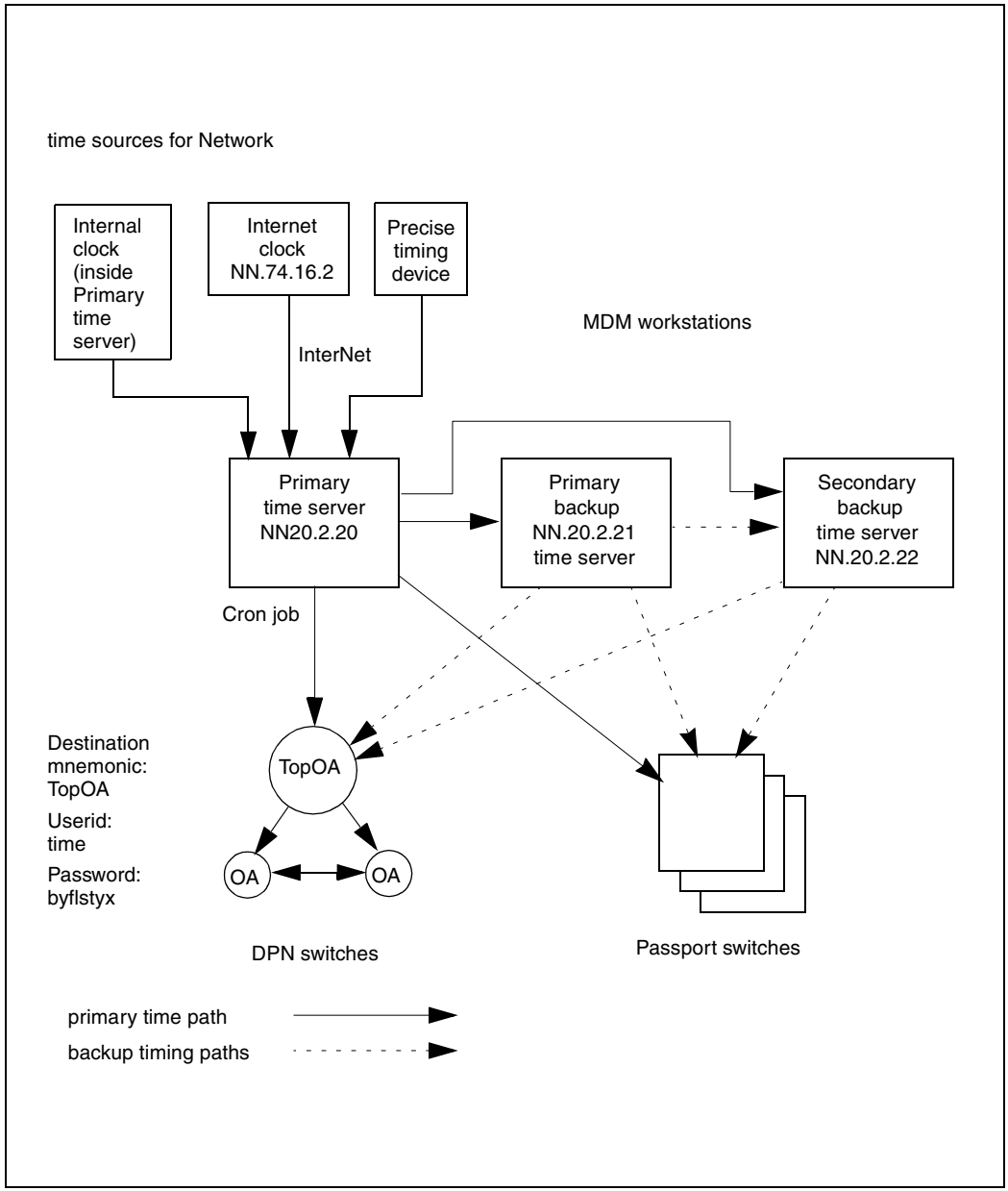


Figure 30
Network that uses anything other than a DPN OA as a time server



Configuring NTS in your network (suggested method)

1 Choose the most precise time sources for your network. Choose a DPN OA or one more of the following time sources:

- an accurate clock accessible through the OAs on DPN switches in your network. If you do not choose this source, this procedure assumes that the Preside Multiservice Data Manager (MDM) workstations are going to provide the time to the Top OA for DPN.
- an Internet clock
- a precise timing device such as a radio clock
- the internal clock in the workstation

Note: If you choose a DPN OA as the time source for your network, do not choose any other time source.

2 Choose one MDM workstation in your network as the primary time server, a second (if you have one) as the backup time server, and a third (also if you have one) as the secondary backup time server.

See “Determining the servers and peers for XNTP on workstations” (page 323).

Note: If you are running MDM in a LAN configuration, the workstation you choose as the primary time server must be the one that has the X.25 or Frame Relay connection to the DPN switches and/or Passport switches in your network.

3 On the workstation you chose as the primary time server:

a. Define each of the time sources you chose in step 1:

an OA for the DPN switches in your network, see “Defining a DPN OA as a time source on the primary time server” (page 316). If you configure this time source on the primary time server workstation, do not configure any other time source.

an Internet clock, see “Defining an Internet clock as a time source for the primary time server” (page 311).

a precise timing device, see “Defining a precise timing device connected directly to the workstation as a time source for the primary time server” (page 313).

the internal clock on the workstation, see “Defining the internal clock as a time source for the primary time server” (page 313).

b. If you defined an OA as the time source in step 3a, and there are any other workstations or any Passport switches in your network, run

ntsinstall to configure the local clock on the workstation to run XNTP. Doing this ensures that XNTP on the other workstations and switches recognizes the workstation a time source.

See “Defining an Internet clock as a time source for the primary time server” (page 311).

c. If you decided in step 1 that the workstations are going to provide the time to DPN, set up a cron job to run the syncDPNtime program and provide the time to the Top OA.

See “Setting up the primary time server to provide the time to the Top OA” (page 320).

4 On the workstation you chose as the backup time server:

a. If you decided in step 1 that the workstations are going to obtain the time from DPN, set up a cron job to run the syncToDPNtime program.

See “Setting up the backup and secondary backup time servers to obtain the time from a DPN OA” (page 331).

b. If you decided in step 1 that the workstations are going to provide the time to DPN, set up a cron job to run the syncDPNtime.backup program and provide the time to the Top OA.

See “Setting up the backup and secondary backup time servers to provide the time to the Top OA” (page 333).

c. Run the ntsinstall program to define the servers and peers for XNTP on this workstation. The primary time server workstation will be this workstation’s server, and the secondary backup time server workstation will be it’s peer.

See “Defining the XNTP servers and peers on backup and secondary backup workstations” (page 329).

5 Repeat step 4 on the workstation you chose as the secondary backup time server. Perform the procedures the same way, except that on the secondary backup workstation, choose the primary time server workstation as the server and the backup time server workstation as the peer.

6 On each workstation, run script /opt/MagellanNMS/system/config/config_sys_sync to allow the NTS to set the time on the workstation.

Defining an Internet clock as a time source for the primary time server

Perform the following procedure on the Preside Multiservice Data Manager (MDM) workstation you chose as the primary time server for your network to define an Internet clock accessible from the MDM workstation as a time source.

If you have access to the Internet, you can connect to one of several specified Internet servers that supply time data using XNTP. The Internet contains a number of primary time servers that are synchronized to national time standard clocks by wire links or radio links. These primary time servers are also connected to one or more secondary time servers throughout the Internet and are kept in synch with the primary time servers by means of XNTP software that runs on the time servers.

You can configure XNTP on the workstation to access a primary or a secondary Internet server and use it as the time source for your network. However, primary servers tend to be busy and less accessible than the secondary servers. Access a secondary time server instead of a primary time server, if you are planning to use an Internet clock as a time source.

For a list of the available Internet servers, open a UNIX access window and view file /opt/MagellanNMS/doc/help/NTSClock.info.

> ***Note:*** The data in file /opt/MagellanNMS/doc/help/NTSClock.info is updated regularly. It is your responsibility to contact the administrator of the time servers to verify the accuracy of the information in the file. The accuracy of the time supplied by the Internet server depends on the server you choose.

Defining an Internet clock as a time source

1. Ensure that your workstation has access to the Internet.
2. Read the /opt/MagellanNMS/doc/help/NTSClock.info file to identify the Internet server to which you want to connect.
3. Contact the administrator of the selected Internet server to verify the address of the server and to identify yourself as a user of the Internet server.
4. Log on to the primary time server workstation as root.

5 Start the ntsinstall program by entering:

/opt/MagellanNMS/bin/ntsinstall

The main menu of the ntsinstall program opens.

6 Start the prompt-driven editor by entering:

a

A submenu opens.

7 Select add a new server by entering:

a

The following prompt is displayed:

```
Type (Server/Peer):
```

8 Define the internal clock as a time source (a server) by entering:

Server

The following prompt is displayed:

```
IP address (1-255.0-255.0.255.0-255):
```

9 Enter the IP address of the Internet clock.

The following prompt is displayed:

```
Version (1, 2, 3, 0 to use the default):
```

10 Enter the version of XNTP software running on the time source (the server). If you don't know the version, press the carriage return key to use the default value. The default value is the same version of XNTP software as the version running on your workstation. The version is only required if the time source is running version 1 or version 2.

The following prompt is displayed:

```
Comment:
```

11 Enter a comment, if desired. It is recommended that you enter a string that describes the clock. For example: *Internet clock, Hal @ 9000 computers.com*

The main menu of the ntsinstall program opens.

12 If you want to define another time source, enter **a** to begin defining it.

If you have defined all time sources, enter **s** to save the information you entered and exit ntsinstall. Then reboot the workstation to activate the XNTP software.

Defining a precise timing device connected directly to the workstation as a time source for the primary time server

Perform the following procedure on the Preside Multiservice Data Manager (MDM) workstation you chose as the primary time server for your network to define a precise timing device connected directly to the MDM workstation as a time source for your network. Many types of clocks fit this description, but a Radio clock is the most common.

A radio clock is an optional device that receives a radio signal and converts the signal to a timing signal for the network. The network time accuracy is guaranteed by the XNTP. Using a radio clock requires that you purchase and connect the radio clock and necessary equipment to receive and convert the radio signal.

For a list of radio clock manufacturers open a UNIX access window and view file /opt/MagellanNMS/doc/help/NTSClock.info.

Note: The data in file /opt/MagellanNMS/doc/help/NTSClock.info is updated regularly. It is your responsibility to contact the manufacturer to verify the accuracy of the information in the file.

Defining a radio clock as a time source

1 Install and configure the radio clock according to the instructions provided with the clock and the XNTP software.

Defining the internal clock as a time source for the primary time server

Perform the following procedure on the Preside Multiservice Data Manager (MDM) workstation you chose as the primary time server for your network. The procedure runs the ntsintall script to define the workstation's internal clock as a time source. For more information about this script, see "About ntsinstall" (page 299).

In step 8, you need to supply the version number of XNTP running on the MDM workstation. Enter a default value or the version number. To find out the correct version number, see "Determining the XNTP version" (page 303).

You must perform the procedure when the workstations in your network are going to obtain the time from a DPN OA and there are other workstations or Passport switches in the network as time clients.

If the workstations in your network are obtaining the time from a DPN OA, the internal clock must be the only time source you define with the procedure.

If the workstations are providing the time to DPN, you may define other time sources on the primary time server workstation.

Defining the internal clock as a time source

1. Log in as root on the workstation you chose as the primary time server.
2. Set the current date and time on the server using the UNIX date command.

CAUTION

Temporary loss of connectivity to Passport devices

Entering the date command may have a serious impact on software processes that are running on the MDM workstation. Connectivity to Passport switches may be lost temporarily when you enter the command.

The syntax for the command is as follows:

`date <yymmddhhmm.ss>`

where:

`yy`

is the year. Values from 70 to 99 represent years 1970 to 1999 and values from 00 to 38 represent years 2000 to 2038.

`mm`

is the month

`dd`

is the day

`hh`

is the hour

`mm`

is the minutes

`ss`

are the seconds

3 Start the ntsinstall program by entering:

`/opt/MagellanNMS/bin/ntsinstall`

The main menu of the ntsinstall program opens.

4 Invoke the prompt-driven editor by entering:

`a`

A submenu opens.

5 Select add a new server by entering:

`a`

The following prompt is displayed:

`Type (Server/Peer):`

6 Define the internal clock as a time source (a server) by entering:

`Server`

The following prompt is displayed:

`IP address (1-255.0-255.0.255.0-255):`

7 Enter the IP address in the following form:

`127.127.1. <ref_id>`

where:

`127.127.1.`

are digits that are part of the special IP address that is reserved for defining the internal clock as a time source (a server)

`<ref-id>`

is a digit from 1 to 4 that uniquely identifies the internal clock you are using as a time server. It is used to distinguish the IP address of the internal clock from the IP addresses of all other possible internal clocks.

Note: the XNTP software always assumes the stratum of the internal clock to be 4 and uses the internal clock as the time source of last resort for the workstation.

The following prompt is displayed:

```
Version (1, 2, 3, 0 to use the default):
```

8 Enter the version of XNTP software running on the time source. If you don't know the version, press the return key to use the default value. The default value is the same version of XNTP software as the version running on your workstation. To find out the correct version number, see "Determining the XNTP version" (page 303).

The following prompt is displayed:

```
Comment:
```

9 Enter a comment, if desired. It is recommended that you enter a string that describes the clock. For example: Internal clock.

The main menu of the ntsinstall program appears.

10 If you want to define another time source, enter **a** to define it.

If you have defined all time sources, enter **s** to save the information you entered and exit ntsinstall. Then reboot the workstation to activate the XNTP software.

Defining a DPN OA as a time source on the primary time server

Perform the following procedure on the Preside Multiservice Data Manager (MDM) workstation you chose as the primary time server to define a DPN OA as a time source.

If you choose to define a DPN OA as a time source for your network, do not define any other time source. When you have completed this procedure, you are instructed to run ntsintall to configure the local clock in this workstation as an XNTP server to provide the time to any other workstations and Passport switches in the network.

The following procedure creates an entry in file /var/spool/cron/crontabs to run the syncToDPNtime program as a cron job. When the cron job runs, the MDM workstation obtains the time from a DPN OA and synchronizes the time of the workstation's internal clock to that of the OA. For the instructions to determine how often to run the cron job, see "Determining how often to run a cron job" (page 319).

Defining a clock accessible through an DPN OA as a time source

1. Log on to your designated time server as root.
2. Enter the following command:

   crontab -e

   A crontab file is opened using a UNIX editor (default vi).
3. Using the following syntax add a line to run the syncToDPNtime program.

   **<run_time> /opt/MagellanNMS/bin/syncToDPNtime **
   <destination> <userid> <passwd> <gmt_offset>

   where:

   <run_time>

   defines the time at which the syncToDPNtime program is to be run. The run time takes the form:

   <minute> <hour> <day_of_month> <month> <day_of_week>

   Entering an asterisk (*) for any of these values means that the program will be run for all possible values.

   <destination>

   is the destination address of the OA configured as the DPN clock master, which is the DPN OA local MDI ID. The destination is often referred to as the DEST MNEM (destination mnemonic).

   <userid>

   is a valid user identifier with the correct system privilege (nams, network service and so on.)

   <passwd>

   is a valid password for the userid

   <gmt_offset>

   is the time difference in minutes between Greenwich Mean Time (GMT) and the time on the workstation. The offset must be specified as though you are travelling around the globe in an easterly direction starting at Greenwich. For example

   A workstation is located in Ottawa, Canada. As you travel in an easterly direction starting at Greenwich, the time difference between Greenwich

and Ottawa is 19 hours. The offset for the workstation is therefore (19 x 60) = 1140.

A workstation is located in Auckland, New Zealand. As you travel in an easterly direction, starting at Greenwich, the time difference between Greenwich and Auckland is 8 hours. The offset for the workstation is therefore s (8 x 60) = 480.

4 Exit the file and save it by pressing Esc, then typing:

```
:wq!
```

5 If you have any other workstations or Passport switches in your network, you also need to run ntsinstall on the workstation to configure XNTP to make the time on workstation's local clock available to them. To do this, see "Defining the internal clock as a time source for the primary time server" (page 313).

Example: Defining a clock accessible through the Top OA as a time source

Assume that the Top OA has a destination mnemonic of topOA, a user ID of time, a password of ticktock and is running Eastern Standard Time (offset of 1140). To define the Top OA as the time source for the network and retrieve the time from the OA once every 24 hours at 00 hours, 15 minutes, enter crontab -e to access file /var/spool/cron/crontabs on the Preside Multiservice Data Manager (MDM) workstation chosen as the primary time server. Then add the following line to the file:

```
15 0 * * * /opt/MagellanNMS/bin/syncToDPNtime topOA \
time ticktock 1140 >/dev/console 2>&1
```

Note: The suffix > /dev/console 2>&1 redirects any output from the command to the console. If you do not redirect the output, it is sent to you as a mail message.

Determining how often to run the cron job

When preforming the procedures that configure the Preside Multiservice Data Manager (MDM) workstation to obtain the time from DPN or to provide the time to DPN, you must set up a cron job to access a DPN OA and provide or obtain the time. How frequently you need to run the cron job depends on two factors: the maximum acceptable time difference between the workstation and DPN switches in your network, and the rate at which the two times drift apart.

Before beginning this procedure you must know the maximum allowable time difference (drift) between the workstation and the Top OA in your network. This value depends on the network configuration and the engineering guidelines applicable to your network.

Determining how often to run a cron job

1 Log in as root to the workstation you chose as the primary time server for your network.

2 Synchronize the time on the DPN switch and on the workstation by entering one of the following commands:

- To synchronize DPN to MDM

  /opt/MagellanNMS/bin/syncDPNtime \ <destination_mnemonic> <userid> <password> \ <offset>

- To synchronize MDM to DPN

  /opt/MagellanNMS/bin/syncToDPNtime \ <destination_mnemonic> <userid> <password> \ <offset>

where:

`<destination>`

is the destination address of the OA configured as the DPN clock master, which is the DPN OA local MDI ID. The destination is often referred to as the DEST MNEM (destination mnemonic).

`<userid>`

is a valid user identifier with the correct system privilege (nams, network service and so on.)

`<passwd>`

is a valid password for the userid

`<gmt_offset>`

is the time difference in minutes between Greenwich Mean Time (GMT) and the time on the workstation. The offset must be specified as though you are travelling around the globe in an easterly direction starting at Greenwich. For example

A workstation is located in Ottawa, Canada. As you travel in an easterly direction starting at Greenwich, the time difference between Greenwich and Ottawa is 19 hours. The offset for the workstation is therefore (19 x 60) = 1140.

A workstation is located in Auckland, New Zealand. As you travel in an easterly direction, starting at Greenwich, the time difference between Greenwich and Auckland is 8 hours. The offset for the workstation is therefore s (8 x 60) = 480.

3 At the same time of day 24 hours later, launch the Command Console tool, log in to the module that is running the Top OA, and display the time on the Top OA:

displayDPNtime <OA name> <userid> <password>

4 Open a UNIX Access window and enter the date command to determine the current setting of the workstation's clock.

5 Note the time difference between the Top OA and the workstation's internal clock.

6 Using the following formula, calculate the frequency for running the cron job:

frequency = (<drift>/<permissible_drift>) + 0.5

where:

frequency

is the number of times to run the cron job in a 24 hour period

<drift>

is the time difference in seconds between the workstation and DPN after the 24 hour period

<permissible_drift>

is the maximum acceptable time difference in seconds between MDM and DPN

Setting up the primary time server to provide the time to the Top OA

Use the following procedure to set up the Preside Multiservice Data Manager (MDM) workstation you chose as the primary time server for your network to provide the time to the Top OA for the DPN switches in your network. As one of its functions, the Top OA synchronizes the time on all of the DPN devices. For this reason, only supply the time to the Top OA and not to any other OA.

Only perform the following procedure if you have decided that the MDM workstations are to provide the time to DPN. Do not perform the procedure if the workstations are to obtain the time from DPN.

Setting up the primary time server workstation to supply the time to the Top OA for the DPN switches involves setting up a cron job to run the syncDPNtime program. The cron job is scheduled by creating an entry in file /var/spool/cron/crontabs. For the instructions to determine how often to run the cron job, see "Determining how often to run a cron job" (page 319).

When it runs, the syncDPNtime program does the following:

- It establishes a connection to a the Top OA for DPN.
- It estimates the propagation delay between the local host and the Top OA. The methodology used is to calculate the average propagation delay over a number of samples. Currently, the number of samples defaults to 3.
- It sets the clock on the Top OA to the time from the primary time server workstation.
- It takes down the connection to the Top OA.

Note: To run the syncDPNtime program to provide the time to DPN, the UserId/Passwd for logging in to the DPN OA needs to have a capability_id with privileges no lower than nams, network, privileged.

Setting up the primary time server to provide the time to DPN

1. Log on as root on the MDM workstation you chose as the primary time server for your network.
2. Enter the following command:

   crontab -e

   A crontab file is opened using a UNIX editor (default vi).
3. Add a line in the following format to run the syncDPNtime program:

   **<run_time> /opt/MagellanNMS/bin/syncDPNtime **
   <destination> <userid> <passwd> <gmt_offset>

   where:

   <run_time>

defines the time at which the syncDPNtime program is to be run. The run time takes the form:

<minute> <hour> <day_of_month> <month> <day_of_week>

Entering an asterisk (*) for any of these values means that the program will be run for all possible values.

`<destination>`

is the destination address of the OA configured as the DPN clock master, which is the DPN OA local MDI ID. The destination is often referred to as DEST MNEM (destination mnemonic).

`<userid>`

is a valid user identifier with the correct system privilege (such as nams and network service)

`<passwd>`

is a valid password for the userid

`<gmt_offset>`

is the time difference in minutes between Greenwich Mean Time (GMT) and the time on the workstation. The offset must be specified as though you are travelling around the globe in an easterly direction starting at Greenwich. For example

A workstation is located in Ottawa, Canada. As you travel in an easterly direction starting at Greenwich, the time difference between Greenwich and Ottawa is 19 hours. The offset for the workstation is therefore (19 x 60) = 1140.

A workstation is located in Auckland, New Zealand. As you travel in an easterly direction, starting at Greenwich, the time difference between Greenwich and Auckland is 8 hours. The offset for the workstation is therefore s (8 x 60) = 480.

4 Exit the file and save it by pressing Esc, then typing:

`:wq!`

Example: Setting up the primary time server to provide the time to DPN

Assume that the top OA has an destination mnemonic of topOA, a user ID of time, a password of ticktock and is running Eastern Standard Time (offset of 1140). To send the time to the top OA at 00:15 every day, open file /var/spool/cron/crontabs by entering crontabs -e and add the following line to the file:

```
15 0 * * * /opt/MagellanNMS/bin/syncDPNtime topOA time
ticktock 1140 >/dev/console 2>&1
```

Note: The suffix > /dev/console 2>&1 redirects any output from the command to the console. If you do not redirect the output, it is sent to you as a mail message.

Determining the servers and peers for XNTP on workstations

To use XNTP on the Preside Multiservice Data Manager (MDM) workstations in your network, you must define the timing relationships among them by running the ntsinstall program on each workstation. The ntsinstall program installs XNTP software and prompts you for configuration data that defines the workstation's servers and peers. The configuration data is written into file /opt/MagellanNMS/cfg/NTS.cfg. See the following sections for information about ntsinstall and the NTS.cfg file:

- "About ntsinstall" (page 299)
- "About the NTS.cfg configuration file" (page 302)

The following series of examples show how to determine the servers and peers for the MDM workstations.

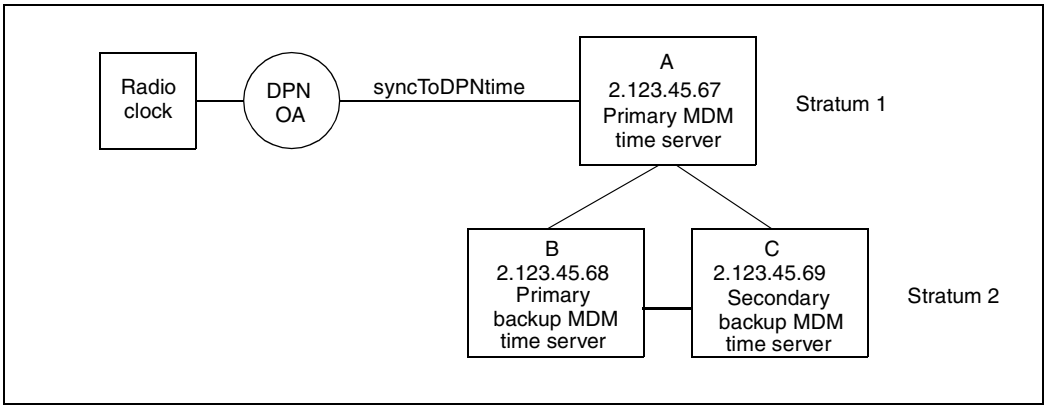
Example 1: Network that uses the Top OA as its time source

The figure "Network in which the time source is a DPN OA" (page 324) shows a simple network of three Preside Multiservice Data Manager (MDM) workstations in which an OA is used as a time source and the time is retrieved from the an OA by means of the syncToDPNtime program running as a cron job on the primary MDM time server. The server-peer relationships for MDM workstations A, B, and C are as follows:

- workstation A receives its time directly from the DPN OA and therefore is at stratum level 1. It has no servers and no peers.

- workstations B and C are peers and use workstation A as their time server. They are therefore both at stratum level 2.

Figure 31
Network in which the time source is a DPN OA



In this configuration, the contents of the file /opt/MagellanNMS/cfg/NTS.cfg on each workstation is as follows:

Workstation A This is the primary time server for the network. It gets its time directly from the Top OA and therefore has no server. It also has no peers. The /opt/MagellanNMS/cfg/NTS.cfg file therefore contains no server or peer definitions.

Workstation B This is a backup time server for the network. Its opt/MagellanNMS/cfg/NTS.cfg file identifies its time server (workstation A) and its peer (workstation C). The contents of the file are as follows:

```
server 2.123.45.67     # MDM time server A
peer   2.123.45 69     # MDM time server C
```

Workstation C This is a backup time server for the network. Its opt/MagellanNMS/cfg/NTS.cfg file identifies its time server (workstation A) and its peer (workstation B). The contents of the file are as follows:

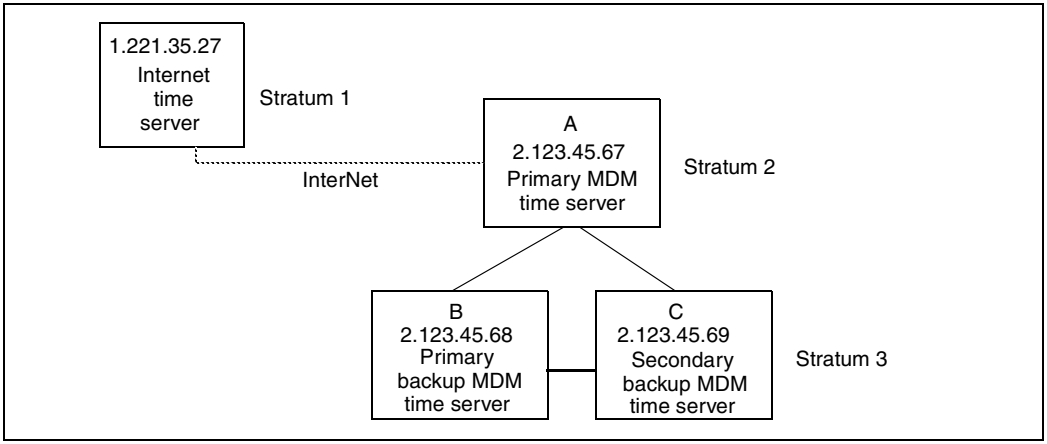
```
server 2.123.45.67     # MDM time server A
peer   2.123.45.68     # MDM time server B
```

Example 2: Network that uses a clock accessible through the Internet as its time source

The figure "Network in which the time source is a clock accessible through the Internet" (page 325) shows a simple network of three Preside Multiservice Data Manager (MDM) workstations in which the time source is an Internet server. The server-peer relationships for workstations A, B, and C are as follows:

- workstation A is the only server at stratum level 2 and has no peers. The time server for workstation A is the Internet server, which is at stratum level 1.
- workstations B and C are the peers of each other and use workstation A as their time server. They are therefore both at stratum level 3.

Figure 32
Network in which the time source is a clock accessible through the Internet



In this configuration, the contents of the /opt/MagellanNMS/cfg/NTS.cfg file on each workstation is as follows.

Workstation A This is the primary time server for the network. Its /opt/MagellanNMS/cfg/NTS.cfg file identifies its time server. The contents of the file are as follows:

server 1.221.35.27 # Internet server. Admin: Hal at 423 984 8746

Workstation B This is a backup time server for the network. Its /opt/MagellanNMS/cfg/NTS.cfg file identifies its time server (workstation A) and its peer (workstation C). The contents of the file are as follows:

```
server 2.123.45.67     # MDM time server A
peer   2.123.45 69     # MDM time server C
```

Workstation C This is a backup time server for the network. Its /opt/MagellanNMS/cfg/NTS.cfg file identifies its time server (workstation A) and its peer (workstation B). The contents of the file are as follows:

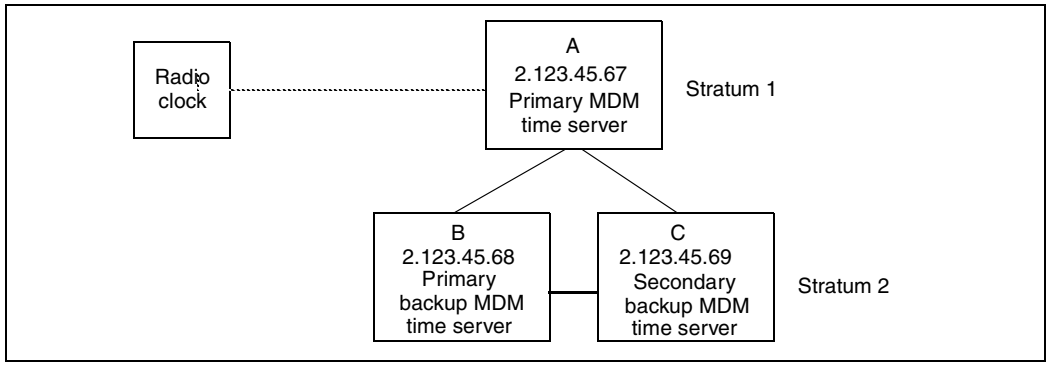
```
server 2.123.45 67     # MDM time server A
peer   2.123.45.68     # MDM time server B
```

Example 3: Network that uses a precise timing device connected directly to the workstation as a time source

The figure "Network in which the time source is a precise timing device (Radio clock)" (page 327) shows a simple network of three Preside Multiservice Data Manager (MDM) workstations in which the precise time source is a radio clock. The server-peer relationships for workstations A, B, and C are as follows:

- workstation A receives its time directly from a radio clock and therefore is at stratum level 1. It has no servers and no peers.
- workstations B and C are the peers of each other and use workstation A as their time server. They are therefore both at stratum level 2.

Figure 33
Network in which the time source is a precise timing device (Radio clock)



In this configuration, the contents of the /opt/MagellanNMS/cfg/NTS.cfg file for each workstation are as follows.

Workstation A This is the primary time server for the network. It gets its time directly from a radio clock and therefore has no server. It also has no peers. The /opt/MagellanNMS/cfg/NTS.cfgfile therefore contains no server or peer definitions.

Workstation B This is a backup time server for the network. Its /opt/MagellanNMS/cfg/NTS.cfg file identifies its time server (workstation A) and its peer (workstation C). The contents of the file are as follows:

```
server 2.123.45.67     # Radio time server. Admin: Jill at 236 9863
peer   2.123.45 69     # MDM time server C
```

Workstation C This is a secondary backup time server for the network. Its /opt/MagellanNMS/cfg/NTS.cfg file identifies its time server (workstation A) and its peer (workstation B). The contents of the file are as follows:

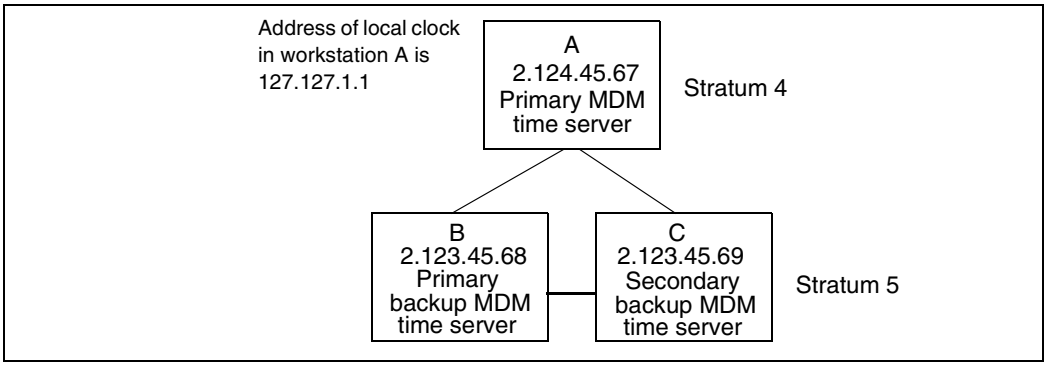
```
server 2.123.45.67     # Radio time server. Admin: Jill at 236 9863
peer   2.123.45.68     # MDM time server B
```

Example 4: Network that uses an internal clock as a time source

The figure "Network in which the time source is the internal clock in one workstation" (page 328) shows a simple network of three Preside Multiservice Data Manager (MDM) workstations in which the time source for the network is the internal clock in one workstation. The server-peer relationships for workstations A, B, and C are as follows:

- workstation A receives its time directly from its internal clock. XNTP always sets its stratum number to 4. It has no servers and no peers.
- workstations B and C are the peers of each other and use workstation A as their time server. XNTP sets their stratum level to 5.

Figure 34
Network in which the time source is the internal clock in one workstation



In this configuration, the contents of the /opt/MagellanNMS/cfg/NTS.cfg file for each workstation are as follows.

Workstation A This is the primary time server for the network. It gets its time directly from its own internal clock which is configured at the server It has no peers. The /opt/MagellanNMS/cfg/NTS.cfgfile therefore contains the following server definition:

server 127.127.1.1 # Local internal clock

Workstation B This is a backup time server for the network. Its /opt/MagellanNMS/cfg/NTS.cfg file identifies its time server (workstation A) and its peer (workstation C). The contents of the file are as follows:

```
server 2.123.45.67     # Workstation A
peer   2.123.45 69     # Workstation C
```

Workstation C This is a secondary backup time server for the network. Its /opt/MagellanNMS/cfg/NTS.cfg file identifies its time server (workstation A) and its peer (workstation B). The contents of the file are as follows:

```
server 2.123.45.67     # Workstation A
peer   2.123.45.68     # Workstation C
```

Defining the XNTP servers and peers on backup and secondary backup workstations

Perform the procedure, "Defining the servers and peers for the backup and secondary backup workstations" (page 329), on each backup and secondary backup Preside Multiservice Data Manager workstation to define the workstations' servers and peers.

For the backup time server workstation, use the procedure to define the primary time server workstation as its time server and the secondary backup time server workstation as its peer. For the secondary backup time server workstation, use it to define the primary time server as its time server and the backup time server workstation as its peer.

For examples of these configurations and what the contents of the NTS.cfg file should look like, see "Determining the servers and peers for XNTP on workstations" (page 323).

Defining the servers and peers for the backup and secondary backup workstations

1. Log onto the server as root.
2. Enter the following command from the UNIX command line:

   `/opt/MagellanNMS/bin/ntsinstall`

   The main menu opens.
3. Enter **a** to start the prompt-driven editor.

   The submenu opens.
4. Select add a new server by entering:

a

The following prompt is displayed:

```
Type (Server/Peer):
```

5 Enter server if you are defining the time server. Enter peer if you are defining a peer.

The following prompt is displayed:

```
IP Address (1-255.0-255.0-255.0-255) :
```

6 Enter the IP address of the server or peer.

The following prompt is displayed:

```
Version (1, 2, 3, 0 to use default):
```

7 Enter the XNTP version running on the server or peer. If you do not know the version of XNTP, press the return key to use the default value. The default value is the version of XNTP that is running on this Preside Multiservice Data Manager (MDM) workstation. The version is required only when the selected time server is running XNTP version 1 or version 2.

The following prompt is displayed:

```
Comment:
```

8 Enter a comment if desired. It is recommended that you enter a text string that describes the server or peer. For example: MDM workstation bcars999.

The submenu opens on the screen.

9 If you want to define another server or peer for this workstation, enter **a** to define the server or peer.

If you have defined all of the servers and peers for this workstation, enter **s** to save your entries and exit ntsinstall. Reboot the workstation to start XNTP running.

10 Log in as root and enter the following command:

date

11 Check the time and date on the workstation. If it differs from the MDM time server by more than 1000 seconds, re-enter the date command with the new time to reset the time on the workstation.

Setting up the backup and secondary backup time servers to obtain the time from a DPN OA

Use the procedure, "Setting up the backup and secondary backup time servers to provide the time to DPN" (page 333), to set up the Preside Multiservice Data Manager (MDM) workstations you chose as the backup and secondary backup time servers in your network to obtain the time from a DPN OA and synchronize to the OA's time.

Only perform the procedure if the MDM workstations will obtain the time from DPN. Do not perform it if the workstations are to provide the time to DPN.

Setting up the backup and secondary backup time server workstations to obtain the time from a DPN OA requires you to set up cron jobs on them to run the syncToDPNtime program. The cron job is scheduled by creating an entry in file /var/spool/cron/crontabs. For the instructions to determine how often to run the cron job, see "Determining how often to run a cron job" (page 319).

To run the syncToDPNtime program, the UserId/Passwd for login to the DPN OA needs to have a capability_id with privileges no lower than nams, network, privileged.

Setting up the backup and secondary backup time servers to obtain the time from DPN

1. Log on as root on the Preside Multiservice Data Manager (MDM) workstation you chose as the backup time server for your network.
2. Enter the following command:

   crontab -e

   A crontab file is opened using a UNIX editor (default vi).
3. Add a line in the following format to run the syncToDPNtime program:

   **<run_time> /opt/MagellanNMS/bin/ **
   **syncToDPNtime <destination> <userid> **
   <passwd> <gmt_offset>

   where:

   <run_time>

defines the time at which the program is to be run. The run time takes the form

<minute> <hour> <day_of_month> <month> <day_of_week>

Entering an asterisk (*) for any of these values means that the program will be run for all possible values.

`<destination>`

is the destination address of the OA configured as the DPN clock master, which is the DPN OA local MDI ID. The destination is often also referred to as DEST MNEM (destination mnemonic).

`<userid>`

is a valid user identifier with the correct system privilege (nams, network service and so on.)

`<passwd>`

is a valid password for the user ID

`<gmt_offset>`

is the time difference in minutes between Greenwich Mean Time (GMT) and the time on the workstation. The offset must be specified as though you are travelling around the globe in an easterly direction starting at Greenwich. For example

A workstation is located in Ottawa, Canada. As you travel in an easterly direction starting at Greenwich, the time difference between Greenwich and Ottawa is 19 hours. The offset for the workstation is therefore (19 x 60) = 1140.

A workstation is located in Auckland, New Zealand. As you travel in an easterly direction, starting at Greenwich, the time difference between Greenwich and Auckland is 8 hours. The offset for the workstation is therefore s (8 x 60) = 480.

4 Exit the file and save it by pressing Esc, then typing:

`:wq!`

5 Repeat this procedure on the workstation you chose as the secondary backup time server.

Setting up the backup and secondary backup time servers to provide the time to the Top OA

Use the procedure, "Setting up the backup and secondary backup time servers to provide the time to DPN" (page 333), to set up the Preside Multiservice Data Manager (MDM) workstations as the backup and secondary backup time servers in your network so that they provide the time to the Top OA of the Network Control System (NCS) for the DPN switches. As one of its functions, the Top OA synchronizes the time of all DPN nodes to the Top OA's time.

Perform this procedure if the MDM workstations are providing the time to DPN. Do not perform it if the workstations are obtaining the time from DPN.

Setting up the backup and secondary backup time server workstations to provide the time to the Top OA for the DPN switches requires you to set up a cron job on both of them to run the syncDPNtime.backup program.

The cron job is scheduled by creating an entry in file /var/spool/cron/crontabs. See "Determining how often to run a cron job" (page 319).

To run the *syncDPNtime.backup* program, the NCS Capability ID and password used to log in to the Top OA needs to have a capability_id with privileges no lower than nams, network, privileged.

Setting up the backup and secondary backup time servers to provide the time to DPN

1. Log on as root on the Preside Multiservice Data Manager (MDM) workstation you chose as the backup time server for your network.
2. Enter the following command:

   crontab -e

   A crontab file is opened using a UNIX editor (default vi).
3. Add a line in the following format to run the syncDPNtime.backup program:

   **<run_time> /opt/MagellanNMS/bin/syncDPNtime.backup **
   **<destination> <userid> <passwd> <gmt_offset> **
   <IP_primary> <IP_backup>...

where:

`<run_time>`

defines the time at which the program is to be run. The run time takes the form:

`<minute> <hour> <day_of_month> <month> <day_of_week>`

Entering an asterisk (*) for any of these values means that the program will be run for all possible values.

`<destination>`

is the destination address of the OA configured as the DPN clock master, which is the DPN OA local MDI ID. The destination mnemonic is often referred to as DEST MNEM (destination mnemonic).

`<userid>`

is a valid user identifier with the correct system privilege (nams, network service and so on.)

`<passwd>`

is a valid password for the userid

`<gmt_offset>`

is the time difference in minutes between Greenwich Mean Time (GMT) and the time on the MDM workstation. The offset must be specified as though you are travelling around the globe in an easterly direction starting at Greenwich. For example:

A workstation is located in Ottawa, Canada. As you travel in an easterly direction starting at Greenwich, the time difference between Greenwich and Ottawa is 19 hours. The offset for the workstation is therefore (19 x 60) = 1140.

A workstation is located in Auckland, New Zealand. As you travel in an easterly direction, starting at Greenwich, the time difference between Greenwich and Auckland is 8 hours. The offset for the workstation is therefore s (8 x 60) = 480.

`<IP_primary>`

is the IP address of the primary MDM time server

`<IP_backup>...`

are the IP addresses of the backup time servers. There can be more than one of them.

4 Exit the file and save it by pressing Esc, then typing:

```
:wq!
```

5 Repeat this procedure on the workstation you chose as the secondary backup time server.

Example: Setting up backup and secondary backup DPN time servers

Assume that the Top OA has a destination of topOA, a userid of time, a password of ticktock and is running Eastern Standard Time (offset of 1140). There are three workstations A, B and C, as shown in the figure "Example of backup and secondary backup time server setup" (page 336). A is the workstation chosen as the primary time server, B is the Preside Multiservice Data Manager (MDM) workstation chosen as the backup time server, and workstation C is the MDM workstation chosen as the secondary backup time server.

Workstation B To define workstation B as the backup time server and to poll workstation A every 24 hours on the 15 minutes to see if it is still alive, add the following line to the /var/spool/cron/crontabs file on workstation B:

```
15 0 * * * /opt/MagellanNMS/bin/syncDPNtime.backup
topOA \
time ticktock 1140 1.34.10.5 > /dev/console 2>&1
```

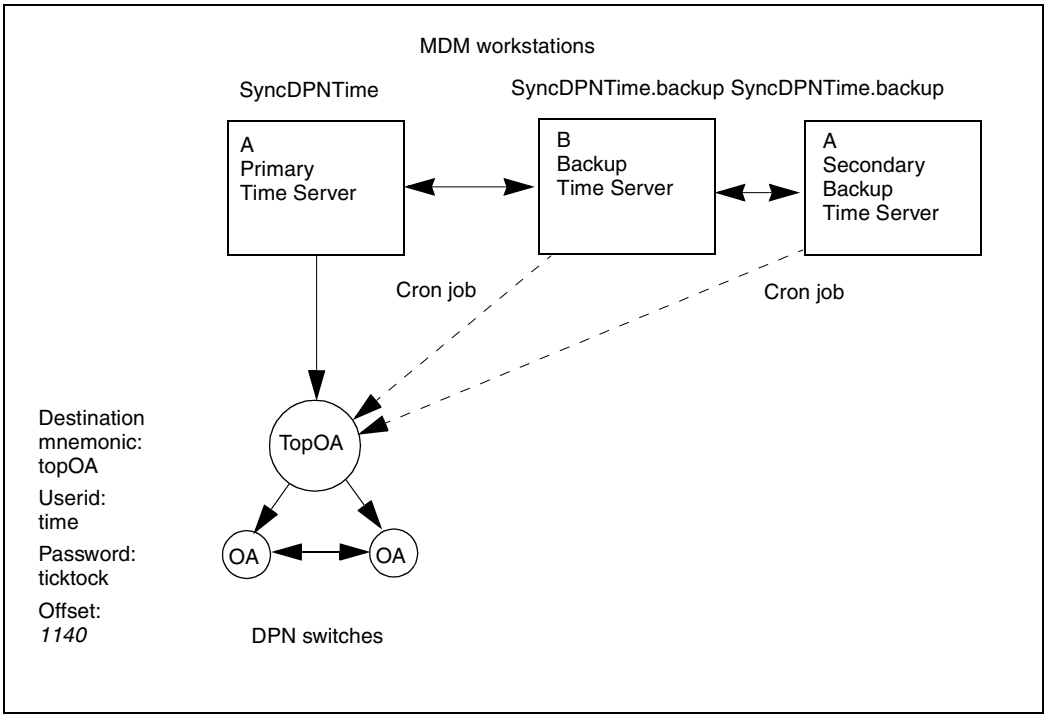
Note: The suffix > /dev/console 2>&1 redirects any output from the command to the console. If you do not redirect the output, it is sent to you as a mail message.

Workstation C To define workstation C as the secondary backup time server and to poll workstation B every 24 hours on the 15 minutes to see if it is still alive, add the following line to the /var/spool/cron/crontabs file on workstation B:

```
15 0 * * * /opt/MagellanNMS/bin/syncDPNtime.backup
topOA \
time ticktock 1140 1.34.10.5 1.34.09.7 >/dev/console
2>&1
```

Note: The suffix > /dev/console 2>&1 redirects any output from the command to the console. If you do not redirect the output, it is sent to you as a mail message.

Figure 35
Example of backup and secondary backup time server setup



Stopping NTS

Use the following procedure to stop the Network Time Synchronization processes.

1. Open the Server Administration tool and select Stop on the Network Time Sync entry in the server list. See “Using the Server Administration tool” (page 359) for more information.
2. Open a UNIX access window and open the crontabs file:

   ```
   crontab -e
   ```

3 Remove the entries that contain the command: syncDPNtime, syncDPNtime.backup, or syncToDPNtime.

What to do if XNTP terminates

If the XNTP terminates, it could mean that there is a time difference greater than 1000 seconds between the workstations server and its local clock:

This situation can occur if

- The time setting was modified on the workstation.
- The time setting was reset. For example, daylight savings time kicked in.

To correct the situation, you must log in as root on the workstation and enter the date command to reset the time to the correct value. Adjust the workstation's internal clock time with UNIX root command "date yymmddhhmm.ss" and restart the XNTP process by rebooting the workstation.

Chapter 19
Configuring remote access

This section contains instructions for setting up the Remote Access tool. See the following sections for more information:

About the Remote Access tool

The Remote Access tool lets you access a remote host that supports the VT-100 user interface either through a Telnet session, or an X.29 PAD session. For instructions to use the Remote Access tool, see 241-6001-804 *Preside MDM Workstation Utilities User Guide*. Using the Remote Access tool requires that interfaces be set up on the Preside Multiservice Data Manager (MDM) workstation to allow you to access the remote host. Four main types of interfaces can be used to access a remote host through the network:

- an IP over X.25 connection
- an IP over Frame Relay connection
- an X3 protocol connection running on an X.25 link
- IP over Ethernet

The following sections contain information about setting up these types of connections for the Remote Access tool.

Configuring TCP/IP access over X.25

To access a remote host with the Remote Access tool using an IP over X.25 connection, an IP over X.25 interface must be configured on the workstation. Sun's *X.25tool* is used for this purpose. For the instructions to set up an interface for IP over X.25 access on the workstation, see 241-6001-100 *Preside MDM Installation* and in the Sun document *Managing SunLink X.25*.

You can specify a host using the Remote Access tool to establish a Telnet session by

- entering an IP address
- entering a host name
- entering the name of a network element that is defined as an SNMP device in file /opt/MagellanNMS/cfg/snm/snmpdir
- entering the name of a Passport group as defined in the Host Group Directory Server file /opt/MagellanNMS/cfg/HGDS.cfg

The set-up required to allow you to use each of these methods is as follows:

IP address or a host name The IP address and host name must be defined in file /etc/hosts. The method to use for defining the IP address and host name depends on whether your network uses a Naming Information Service (NIS). If your network uses a NIS, you need to use Sun's Admin Tool Suite software to set up the IP address and hostname for the workstation. See the Sun documentation that accompanies this software for the instructions to perform this task. However, if your network does not use NIS, use an editor such as vi to enter the host name and IP address of the remote host into file /etc/hosts.

A Passport group For the instructions to configure Passport groups in file /opt/MagellanNMS/cfg/HGDS.cfg, see "Configuring MDM servers for Passport switches" (page 123).

Configuring TCP/IP access over Frame Relay

To access a remote host with the Remote Access tool using an IP over Frame Relay connection, an IP over Frame Relay interface must be configured on the workstation. For the instructions to set up an interface for IP over Frame Relay access on the workstation, see 241-6001-100 *Preside MDM Installation*.

There several ways to specify a host when using the Remote Access tool to establish a Telnet session. These methods and the set-up required to use them are the same as those for TCP/IP access on an IP over X.25 connection. For further information, see “Configuring TCP/IP access over X.25” (page 340).

Configuring access over X.25 through an X.29/X.3 PAD

To access a remote host with the Remote Access tool using X.3 protocol on an X.25 connection, an X.25 interface must be set up on the Preside Multiservice Data Manager (MDM) workstation then a X.29 PAD daemon application must be configured on the workstation. Sun’s X.25tool is used for setting up the X.25 interface and the X.29 PAD daemon application. For the instructions to set up an X.25 link to DPN, see 241-6001-100 *Preside MDM Installation*. For the instructions to set up an X.29 PAD daemon application, see the Sun document: *Managing SunLink X.25*.

You can specify a host by using the Remote Access tool to establish an X.29 PAD session by

- entering a Data Network Address
- entering a host name

When setting up the X.25 interface and the X.29 PAD daemon application, you always have to supply a DNA. Therefore this first method is always available to users of the Remote Access tool. To be able to use a host name, you must define aliases for the DNA when setting up the X.29 PAD daemon application with Sun’s X.25 tool.

Special considerations for Passport 4400 series

If you are configuring remote access to a Passport 4400 series device you need to do the following:

- set up IP (LAN or WAN) connectivity between the workstation and the Passport 4400 series device
- set up the Preside Multiservice Data Manager (MDM) workstation to gather surveillance information from the Passport 4400 series devices in the network and supply this information to the GMDR server.

The IP addresses of each Passport 4400 series device are part of the information that is supplied to GMDR. If the Remote Access tool does not have this information, you will only be able to set up a Telnet session using the IP address of the device. You will not be able to log in using the device name.

Chapter 20
Configuring automatic DBNL disabling

This section describes the automatic Dial Backup Network Link (DBNL) disabling feature, and contains instructions for configuring the feature and cleaning up any accumulated log files the feature produces.

See the following sections for more information:

About the automatic DBNL disabling feature

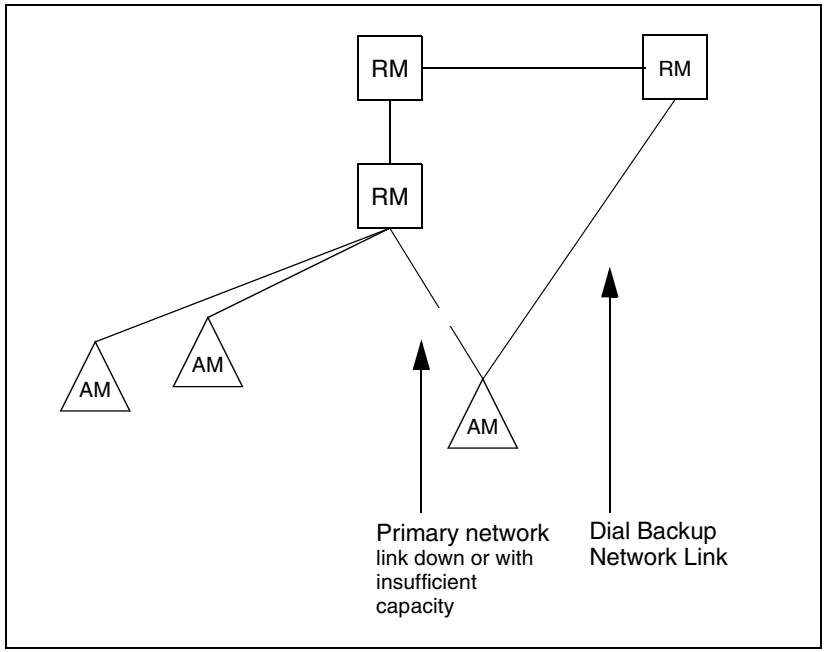
The automatic Dial Backup Network Link (DBNL) disabling feature provides an administrator with information about the activation and deactivation of DBNLs for DPN-100 switches in the network, and with the option of having DBNLs disabled automatically when they are no longer needed.

A Dial Backup Network Link is a backup link that the Network Control System (NCS) activates automatically to establish a direct connection from an Access Module (AM) to a Resource Module (RM) when one of the following happens:

- the primary network link goes down and isolates the AM (or a cluster of AMs) from the RM

- the primary network link runs out of bandwidth to handle current traffic conditions

Figure 36
Dial Backup Network Link



The automatic DBNL disabling feature monitors alarms from the DPN switches in the network. When it detects the presence of a DBNL activation alarm or a DBNL heartbeat alarm indicating that a DBNL has been activated, it sets up a watch on the DBNL and monitors that status of the primary link. Depending on the Operator Data information contained in the alarms, the automatic DBNL disabling feature has the following capabilities:

- For DBNL alarms containing operator data which indicates that a DBNL has been activated due to isolation of an AM (or a cluster of AMs), the feature can be used to deactivate the DBNL when the primary link returns to service and remains stable for a specified period, an optionally, to watch the DBNL only.

- For DBNL alarms containing operator data which indicates that a DBNL has been activated due to any other cause, the feature can be used to watch the DBNL only.

Operation of the automatic DBNL disabling feature

The automatic DBNL disabling feature is implemented by means of the DBNL auto-disabling daemon (DBNLWatch) and the set of utilities (dbnlfindam, dbnlcheck, dbnldisable, dbnlenable, and dbnlapi) shown in the figure "Components of the automatic DBNL disabling feature" (page 346).

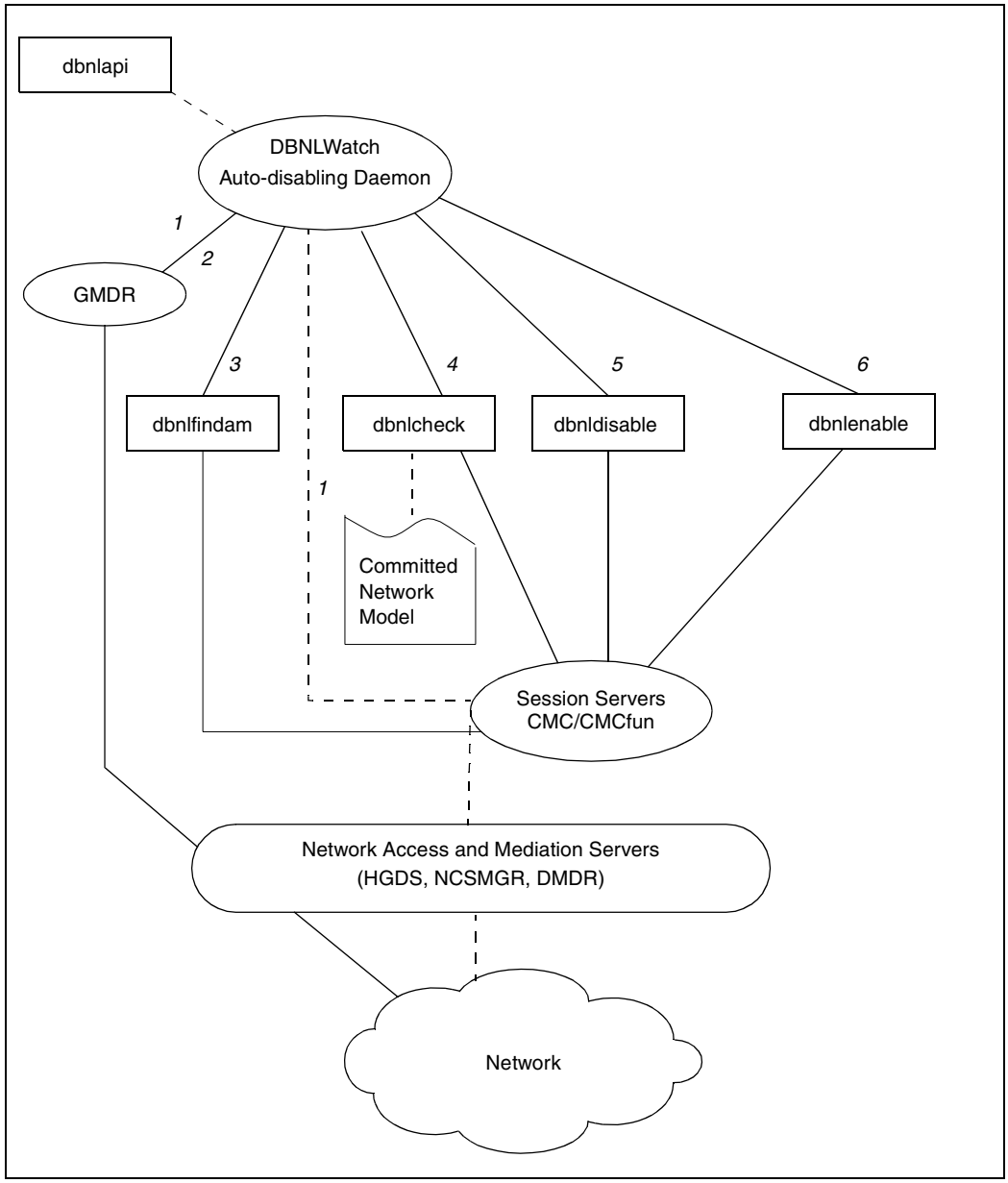
The following sequence describes the operation automatic DBNL disabling feature. Refer to the figure "Components of the automatic DBNL disabling feature" (page 346) while reading this description.

1 When DBNLWatch is started, it does the following:

It connects to the GMDR server specified by the -host and -serv parameters in its startup command to obtain alarms from the DPN network.

It starts and maintains a connection to the OAs in the network specified by parameters PrimaryOAAuth and BackupOAAuth in configuration file /opt/MagellanNMS/cfg/DBNLWatch.cfg.

Figure 37
Components of the automatic DBNL disabling feature



2 When DBNLWatch receives a 10164021 alarm (DBNL activation alarm) or a 10164022 (DBNL heartbeat alarm) containing Operator Data indicating that a DBNL is activated as a result of AM link isolation (Operator Data 04 or 05), DBNLWatch uses parameter MonitorOnly in the configuration file to determine what it should do:

If MonitorOnly just permits monitoring, DBNLWatch starts a passive watch (no attempts are made at disabling the DBNL), and outputs all subsequent alarm information to a log file.

If MonitorOnly permits monitoring and deactivation of the DBNL, DBNLWatch starts an active watch on the DBNL, and performs the following sequence of steps.

3 DBNLWatch calls utility dbnlfindam to determine which end of the DBNL corresponds to the calling AM end. DBNLWatch calls dbnlfindam repeatedly until this determination is made.

4 At intervals specified by configuration file parameter CheckTimer, DBNLWatch calls dbnlcheck which probes the DPN module with NCS commands to determine if the primary link is up. To formulate the commands dbnlcheck makes use of information from the committed Network Model to map DPN node names to nams_ids.

5 If the primary network link is still found to be up after it is checked the number of times specified by parameter CheckTries, DBNLWatch calls dbnldisable to disable the DBNL.

If the DBNL is successfully disabled, the process continues at step 6.

If the DBNL fails to disable, DBNLWatch calls dbnldisable at intervals specified by configuration file parameter DisableTimer until either the DBNL is successfully deactivated, or it has reached the number of attempts specified by configuration file parameter EnableTries. Should the DBNL fail to deactivate after the number of attempts specified by EnableTries, the sequence starts back at step 4.

6 After the waiting period specified by parameter EnableWait, DBNLWatch calls dbnlenable to re-enable the DBNL port and make the DBNL available again.

If the port enables, DBNLWatch ends the active watch on the DBNL.

If the port fails to re-enable, DBNLWatch calls the dbnlenable utility at intervals specified by configuration file parameter EnableTimer until either the DBNL is successfully deactivated, or DBNLWatch has called the utility the number of time specified by configuration file parameter EnableTries. Should the DBNL fail to deactivate after the number of attempts specified by EnableTries, the sequence starts back at step 4.

7 DBNLWatch drops a watch on a DBNL automatically under the following circumstances:

if the DBNL is watched for period exceeding the value specified by MaxWatchTime without receiving a DBNL heartbeat alarm

if DBNLWatch receives a 10164020 alarm indicating that DBNL has been deactivated by other means, such as by operator commands

Utility dbnlapi provides an API-like interface that can be used at any time to obtain a list of the DBNLs that are currently being watched by DBNLWatch. For the instructions to use this utility and a sample of its output, see “Obtaining a list of the DBNLs that are currently being watched” (page 355).

Types of DBNL activation handled by the automatic DBNL disabling feature

The automatic DBNL disabling feature can be used to watch DBNLs on receipt of 10164021 (DBNL activation) alarms or 10164022 (DBNL heartbeat) alarms. These alarms include Operator Data codes. Although the feature can be used to monitor and disable DBNLs for alarms containing some of these codes, it can only be used for monitoring DBNLs for others. The operator data codes and the ability to monitor and disable DBNLs or monitor DBNLs only are shown in the following table.

Table 6
Operator codes, their meanings, and the ability to monitor and disable

Operator Data Code	Description	Monitor and disable	Monitor only
00	DBNL activated manually	N	Y
01	DBNL activated due to the loss of a Resource Module (RM)	N	Y
02	DBNL activated due to an increase in RM distance	N	Y
04	DBNL activated due to fault isolation of a cluster of Access Modules (AMs)	Y	Y
05	DBNL activated due to fault isolation of a single AM	Y	Y
08	DBNL activated to provide bandwidth on demand	N	Y

Compatibility of DPN software with the automatic DBNL disabling feature

The DBNL feature is backwards compatible with networks containing DPN switches that are running software generics lower than G33, with the following restrictions:

- The capability that allows a customer to choose whether they can turn off or turn on the automatic DBNL disabling feature is not supported in pre-G33 networks.
- DBNL heartbeat alarms are not generated in pre-G33 networks. Therefore, should the workstation reboot, any DBNLs that are enabled when the reboot occurs cannot be disabled with the feature. The enabled DBNLs must be disabled manually.

Log files produced by the automatic DBNL disabling feature

DBNLWatch writes log information into a set of cycling log files at each of the steps in the sequence described in "Operation of the automatic DBNL disabling feature" (page 345). This set of cycling log files consists of one log file for each day of the week, named as follows:

/opt/MagellanNMS/data/DBNLWatchLog.<n>

where:

<n> is a number between 0 and 6 that indicates the day of the week at which the log file was created. 0 is Sunday and 6 is the Saturday immediately after it.

At the beginning of each new day, the log file for the same day of the previous week is overwritten with information about DBNLs that are currently being watched, starting at the top of the file.

Should DBNLWatch be restarted, log information is appended to the current day's file; the log file is overwritten only when DBNLWatch detects a change of day. This ensures that the current day's log information is still available if DBNLWatch is restarted.

Nevertheless, the log files can grow and consume excessive amounts of disk space, especially if the connection to the main and backup OAs is unstable. Such files can be deleted manually by entering commands to remove the files, or automatically by setting up a cron job to run these commands on a scheduled basis. For the procedures to clear log files manually or with a *cron* job, see "Cleaning up accumulated log files" (page 356).

The following paragraphs contain samples of the log information produced by DBNLWatch during its various phases of operation.

DBNLWatch is started, connects to the GDMR server, and establishes connections to the main and backup OAs specified in the configuration file:

```
DBNLWatch: started Mon Jun 3 22:14:44 1996

Mon Jun 3 22:14:44 1996
Connected to server GMDR on workstation local host
```

```
CC_status  1041 The following NCS destination has been
established:

CORENCS
CAPABILITY   MATRIX     CURRENT
 NAMS        NETWORK    PRIVILEGED
             OA/DEVICE  PRIVILEGED
             APP/LINE   PRIVILEGED
 SWITCHING   NETWORK    PRIVILEGED
             DEVICE     PRIVILEGED
             LINE       PRIVILEGED
```

DBNLWatch detects the arrival of a DBNL activation alarm or a DBNL heartbeat alarm, and sets up a watch on the DBNL, for monitoring purposes only. When the following log is produced, parameter MonitorOnly is set to Y in the configuration file, or the DBNL is activated due to a cause other than AM or AM cluster isolation.

```
Wed Jul  3 20:54:12 1996
Starting Monitoring Only Watch for:
 Link: DBNL:PM AC2256 PE 1 PI 1 PO 3:PM R32 PE 7 PI 7
PO 3:
 Time: 1996 07 03 20 54 12
  SEQ: 1489 NTP: 10164022 OP: 2001
 Watch phase: DBNL being monitored only.
DBNL has been activated due to RM loss (no auto-
disabling)
```

DBNLWatch detects a DBNL activation alarm or a DBNL heartbeat alarm, and sets up a watch on the DBNL for monitoring and DBNL deactivation purposes. When this log is produced, parameter MonitorOnly is set to N in the configuration file and the DBNL is activated due to AM or AM cluster isolation.

```
Wed Jul  3 21:43:20 1996
Starting Watch for:
 Link: DBNL:PM A6002 PE 13 PI 13 PO 6:PM R60 PE 6 PI 6
PO 6:
 Time: 1996 07 03 21 47 05
   SEQ: 14770 NTP: 10164021 OP: FF04
 Watch phase: Initializing Watch.
activated due to isolation.
```

DBNLWatch runs dbnlfindam to determine the AM end of the DBNL:

```
Wed Jul  3 21:43:20 1996
Identifying the AM side (0) for:
 Link:DBNL:PM A6002 PE 13 PI 13 PO 6:PM R60 PE 6 PI 6
PO 6:
 Time: 1996 07 03 21 47 05
  SEQ: 14770 NTP: 10164021 OP: FF04
Watch phase: Identifying AM side.
```

DBNLWatch runs dbnlcheck to verify whether the primary link is up:

```
Wed Jul  3 21:43:26 1996
Checking connectivity (0/0) for:
 Link: DBNL:PM A6002 PE 13 PI 13 PO 6:PM R60 PE 6 PI 6
PO 6:
 Time: 1996 07 03 21 47 05
  SEQ: 14770 NTP: 10164021 OP: FF04
 Watch phase: Waiting for main link to come back.
```

After running dbnlcheck the number of times specified by CheckTries in the configuration file, and determining that the primary link is still up, DBNLWatch produces a log similar to the following:

```
Wed Jul  3 21:47:08 1996
Disabling:
 Link: DBNL:PM A6002 PE 13 PI 13 PO 6:PM R60 PE 6 PI 6
PO 6:
 Time: 1996 07 03 21 47 05
  SEQ: 14770 NTP: 10164021 OP: FF04
 Watch phase: Waiting for main link to come back.
as the main link has been up for at least 150 seconds.
```

DBNLWatch runs dbnldisable to attempt to disable the DBNL:

```
Wed Jul  3 21:47:08 1996
Trying (0) to disable:
Link: DBNL:PM A6002 PE 13 PI 13 PO 6:PM R60 PE 6 PI 6
PO 6:
Time: 1996 07 03 21 47 05
 SEQ: 14770 NTP: 10164021 OP: FF04
Watch phase: Trying to disable the DBNL.
```

DBNLWatch runs dbnlenable to re-enable the DBNL port:

```
Wed Jul  3 21:47:17 1996
 Trying (0) to enable:
 Link: DBNL:PM A6002 PE 13 PI 13 PO 6:PM R60 PE 6 PI 6
PO 6:
 Time: 1996 07 03 21 47 05
  SEQ: 14770 NTP: 10164021 OP: FF04
Watch phase: Trying to re-enable the DBNL port.
```

DBNLWatch successfully re-enables the DBNL port and drops the watch:

```
Wed Jul  3 21:47:20 1996
Watch for:
   Link: DBNL:PM A6002 PE 13 PI 13 PO 6:PM R60 PE 6 PI
6 PO 6:
    Time: 1996 07 03 21 47 05
     SEQ: 14770 NTP: 10164021 OP: FF04
    Watch phase: Trying to re-enable the DBNL port.
removed after 4 minutes.  Port re-enabled.
```

Setting up the automatic DBNL disabling feature

Use the following procedure to set up the automatic DBNL disabling feature.

Prerequisites

Before setting up the automatic DBNL disabling feature ensure that:

- The attribute *auto disabling allowed* is set to *yes* for the dialup link. This attribute can be found under the component

  ```
  PM/<mnemonic> PE/<n> PI/<m> PO<z> UTP UTP_Dial_Up
  ```

  On DPN, this attribute can be found by issuing the command

  ```
  PI <m> PO <z> Q DIAL
  ```

- Access privileges associated with the OA name, NCS capability_id, and password are sufficient to allow the feature to disable DBNLs. For most cases the scope and impact required are as follows:

  ```
  SWITCHING  DEVICE SERVICE
  ```

- The network access servers (HGDS and NCSMGR) have been configured and are running.

- The servers needed to gather surveillance information (DMDR and GMDR) are configured and running.
- A properly configured and committed Network Model exists that contains information about the nodes in the network.

  The Network Model must be saved in ASCII (portable) format and committed (saved as the startup model). It must also contain accurate information on the nodes in the network and their NAM_ID attribute.

- You have read "Operation of the automatic DBNL disabling feature" (page 345) and understand how DBNLWatch uses the service parameters in file /opt/MagellanNMS/cfg/DBNLWatch.cfg.

Configuring automatic DBNL disabling and starting DBNLWatch

1. Log on to Preside Multiservice Data Manager (MDM) as root.
2. Using a UNIX editor such as vi, or the built-in file editor provided with CDE, open file /opt/MagellanNMS/cfg/DBNLWatch.cfg.
3. Modify the parameters in the file to suit your requirements.

   For explanations of the parameters to be modified, look at the comments in the file itself. For more detailed explanations to manage the DBNL auto-disabling daemon, see 241-6001-310 *Preside MDM Server Reference Guide*.
4. Save the file and exit from it.
5. Ensure that permissions for the configured file are read and write for the root user only.

   ```
   chmod 600 /opt/MagellanNMS/cfg/DBNLWatch.cfg
   ```
6. Using the Server Administration tool, start DBNLWatch with the following startup command and ensure that DBNLWatch restarts automatically when the workstation is rebooted.

   ```
   /opt/MagellanNMS/bin/dbnlwatch [-v] [-n] \
   [-host <GMDR host name>] [-serv <GMDR service name>] \
   [-log <log file prefix>] \
   [-cfg <configuration file name>]
   ```

   For explanations of the parameters in the DBNL startup command, see 241-6001-310 *Preside MDM Server Reference Guide*.

For the instructions to use the Server Administration tool to start DBNLWatch and to ensure that it restarts on automatically on reboot, see “Using the Server Administration tool” (page 359).

Obtaining a list of the DBNLs that are currently being watched

The automatic DBNL disabling feature is equipped with a dbnlapi utility that provides an API-like interface which can be used to obtain information about the DBNLs currently being watched, at any time. To run the utility, enter the following command:

```
/opt/MagellanNMS/bin/dbnlapi -l
```

A sample of the output from this utility is as follows:

```
DBNL:PM AC2256 PE 1 PI 1 PO 3:PM R32 PE 7 PI 7 PO 3:
  Time: 1996 07 03 20 54 12
  SEQ:  1489  NTP: 10164022  OP: 2001
  Watch phase: DBNL being monitored only.
  Up: 0  Attempts: 0  Managed for(s): 52

DBNL:PM A6002 PE 13 PI 13 PO 6:PM R60 PE 6 PI 6 PO 6:
  Time: 1996 07 03 21 47 05
  SEQ:  14770  NTP: 10164021  OP: FF04
  Watch phase: Trying to disable the DBNL.
  Up: 5  Attempts: 1  Managed for(s): 3

DBNL:PM A6002 PE 13 PI 13 PO 4:PM R60 PE 6 PI 6 PO 4:
  Time: 1996 07 03 21 47 05
  SEQ:  14773  NTP: 10164021  OP: FF04
  Watch phase: Waiting for main link to come back.
  Up: 4  Attempts: 7  Managed for(s): 3
```

Cleaning up accumulated log files

Removing accumulated log files should not normally be necessary because there is one log file for each day of the week, and information can only accumulate in a log file for a one week period, then the file is automatically overwritten. Nevertheless, should it become necessary, there are two ways to clean up current log files: manually by entering a command, or automatically by running the command as a cron job.

Cleaning up log files manually

1. Log in as root.
2. Enter the following command to remove a log file:

   /bin/cp /dev/null \ /opt/MagellanNMS/data/ DBNLWatchLog.<n>

   where:

   <n> is a number from 0 to 6 that represents the day of the week on which the log file is generated. 0 is Sunday and 6 is the Saturday immediately after it.

Cleaning up log files with a cron job

1. Log in as root.
2. Enter the following command:

   crontab -e

   A crontab file is opened using a UNIX editor:

3. Add the following cleanup command to the crontab file. We broke up the command into two lines to fit here, but in the file you must enter it all on one line.

   <run_time> /bin/cp /dev/null /opt/MagellanNMS/data/ DBNLWatchLog.<n>

   where:

   <run_time>

   defines the time at which the command is to run. The time takes the form:

   <minute> <hour> <day_of_month> <month> <day of week>

Note: Entering an asterisk for one of these subparameters means that the cron job will run for all possible values of the subparameter.

`<n>`

is a number from 0 to 6 which represents the day of the week on which the log file is generated. 0 is Sunday and 6 is the following Saturday.

4 Exit from the file and save it.

Example

The following command runs every Friday at midnight to clean up a file created back on Tuesday of the same week:

```
01 00 * * 5 bin/cp /dev/null \ /opt/MagellanNMS/data/
DBNLWatchLog.2
```

Chapter 21
Using the Server Administration tool

This section explains the purpose of the Server Administration tool, provides instructions for using the tool, and information about the user interface.

About the Server Administration tool

The Server Administration tool lets you view information about Preside Multiservice Data Manager (MDM) servers and create, modify, delete, start, and stop the servers. The tool has two modes of operation: a view mode and an edit mode. In view mode, the tool lets you do the following:

- choose a host (workstation) on which to view information about servers
- select a server and view its start-up command and parameters
- select a server and view its log file
- print or refresh the contents of the main window
- get help information for the server

In edit mode, the tool lets you perform all of the tasks in view mode plus:

- select a server, then edit the startup command and automatic restart parameters for the server
- add or remove a server
- start or stop a server
- edit the server's configuration file(s)
- change the start-up order of the servers on a local host, or on a remote host that is running MDM 14.3 or later.

The tool also displays a log of all server activity that has occurred since the last system restart.

For information about the user interface, see "User interface" on page 385. For procedures associated with the tool see the following sections:

- "Starting the Server Administration tool" on page 362
- "Connecting to a host" on page 363
- "Viewing a server" on page 364
- "Viewing logs associated with a server" on page 365
- "Accessing the edit mode" on page 366
- "Adding a new server" on page 367

Starting the Server Administration tool

Use this procedure to start the Preside Multiservice Data Manager Server Administration tool.

Prerequisites

The SVM daemon is running.

Procedure steps

1 From the application main window, select **System** -> **Administration** -> **Server Administration**.

The Server Administration window opens. The Server Administration tool is now automatically in view mode.

Connecting to a host

When you start the Server Administration tool, by default it starts in view mode and provides access to information about servers on the local host (local workstation). Use this procedure to connect to a remote host so that you can work on its servers.

Prerequisites

Before you begin, ensure that you have started the Preside Multiservice Data Manager Server Administration tool.

Procedure steps

1. From the **Options** menu, select **Choose host.**

   The **SVM Host** dialog opens.

2. In the dialog's host list, click on the host name of the workstation whose servers you wish to manage.

   The host name becomes highlighted.

3. Click **OK**.

   The **SVM Host** dialog closes and information about servers on the host appears in the server list of the **Server Administration** window.

   The name of the host you chose is displayed in the connection information field. An example of the information that appears in the connection information field is: **Connected to SVM daemon on bcaruff9**.

Viewing a server

Use the following procedure to view information about a server and its restart parameters.

Prerequisites

Before beginning this procedure, ensure that you have:

- started the Preside Multiservice Data Manager Server Administration tool
- connected to a remote host, if the server you want to view is not on the local host

Procedure steps

1 In the server list, click on the name of the server to select it.

2 From the **Edit** menu, select **View**.

The **SVM View Server** dialog opens. The dialog displays information about the server you selected.

3 If you wish to obtain help information on the server, such as the syntax of the server start-up command, click **Help on server.**

Note 1: The Help on server button is disabled for custom servers that you create yourself or any servers that are not defined in the server list file: /opt/MagellanNMS/lib/cfg/SVMServerInfo.cfg.

Note 2: Software obtains the help information from the local host. If you are viewing information while connected to a remote host but it is not running the same release of software as the local host, there may be differences between the help information and the software on the remote host. For example, the parameters for the start-up commands may differ.

4 Click **OK** when you have finished viewing the information.

The dialog closes.

Viewing logs associated with a server

Use the following procedure to view the application log file associated with a server.

Procedure steps

1. In the server list, click on the name of the server to select it.
2. Right click and select **View logs** to launch the Log Browser to view the server's application logs.

   Note: This **View Logs** menu item is only enabled for servers that support the .alog format

Accessing the edit mode

Use this procedure to log in with an edit password and access the edit mode from the view mode.

When the Server Administration tool is started for the first time on the local host or remote host, no edit password exists. Use this procedure to create one while accessing the edit mode for the first time.

Prerequisites

Before you begin, ensure that you have:

- started the Preside Multiservice Data Manager Server Administration tool
- connected to a remote host, if the server you want to work on is not on the local host
- the administration password, if this is not the first time you are accessing the edit mode on this host

Procedure steps

1. From the **Security** menu, select **Authorize**.

   The **SVM Enter Authorization Password** dialog opens.

2. If this is the first time anyone has opened this dialog on this host, and no edit password exists, click OK. If a password exists, go to step 6.
3. From the Security menu, select **Change Password**.
4. Enter a new password of your choice in the **New Password** field. Be sure to remember this edit password, for future use.
5. Click OK.

   The system software remembers the password, closes the dialog, and the Server Administration tool is in edit mode.

6. If you are opening the dialog and a password is already set, enter the password in the **Password** field
7. Click **OK**.

   The system software authenticates the password. If it is valid the dialog closes and the Server Administration tool is in edit mode.

Adding a new server

Use this procedure to add a new server.

Prerequisites

Before you begin ensure that you have:

- started the Preside Multiservice Data Manager (MDM) Server Administration tool
- connected to a remote host, if the server you want to add is not on the local host
- accessed the edit mode

Procedure steps

1. From the **Edit** menu, select **New server.**
2. Are you connected to the local host, or to a remote host?
   - If you are connected to the local host, the **SVM New Server List** dialog opens and lists six types of server. Go to step 3.
   - If you are connected to a remote host, an empty **SVM New Server** dialog opens. Go to step 7.
3. Click on the arrow next to the type of server that you wish to add.

   The list expands and shows the servers that are members of the type of server.

   Hint: If you want to know which servers belong to a type of server without expanding the list, see "Types of servers" on page 369.
4. Click on the name of the server you wish to add, or click **Custom serve**r if you wish to create your own server.

   The name of the server becomes highlighted.
5. If you are not sure what the server does or what its relationship to other servers is, click **Help on server**.

   A Netscape browser window opens that provides access to this information for the highlighted server.
6. Click **Select Server**.

   The **SVM New Server** dialog opens. Fields in this dialog contain the default values for the server.

7 In the **Descriptive name** field, enter a unique name for this server up to 22 characters in length.

8 In the **Startup command** field, enter the startup command for the server. Mandatory parameters are indicated by angle (<>) brackets. Ensure that you enter values for these mandatory parameters and that you delete the angle brackets.

9 In the **Description** field, enter a description for the server. This can be a description of your choice.

10 If you wish to have the server restart automatically when the MDM workstation is rebooted, click **Automatic startup at reboot time**.

11 If you are creating a MDM server, the **Preferred kill signal** menu button is disabled.

If you are creating a custom server, select the UNIX signal you want to use to stop the server with the **Preferred kill signal** menu button.

Note: The **Preferred kill signal** menu button only provides you with a subset of the UNIX kill signals, These are: **SIGHUP**, **SIGQUIT**, **SIGKILL**, **SIGTERM**, **SIGUSR1**, and **SIGUSR2**. For details about these signals refer to the signal(5) man page. You can add or delete signal options from this menu button by customizing X-resources in file /opt/MagellanNMS / lib/app-defaults/C/Svmadm. For information about customizing X-resource files, see 241-6001-301 *Preside MDM Customization Administrator Guide*.

12 Using the restart setup parameter buttons, set up the parameters that the system will use to automatically restart the server if it exits.

For a description of these buttons and how they are used to set up restart times, see Restart parameter buttons (page 360).

13 Do one of the following to save the server information:

- Click **OK** to close the dialog.
- Click **Save** to leave the dialog open.
- Click **Save and Start** to start the server and leave the dialog open.

Job aids

See Table 7 for the categories of server and the servers in each category.

Table 7
Types of servers

Type	Servers
System/Base	
	Host Group Directory Server (HGDS)
	Context Server (CTXSVR)
	Log Collector (OAMC)
	Passport Communications Manager (FDTM)
	Multi-Nodal Name Server, Level 2 (MNSD)
	Multi-Nodal Name Server Agent (MNSDAGENT)
	Workstation Surveillance Server (SFM)
	Secure FTP Daemon (launchSecureFTPD)
	DPN NCS Communications Manager (NCSMGR)
	Customer Database Server (CDBSERVER)
	Security Audit Log Collector (SALCSERVER)
	MPE Communications Manager (NDTM)
Fault Management	
	Data Manager Agent (DMA)
	Injected Management Data Router (IMDR)
	SNMP Proxy Agent (SPA) on MPE 9500
	General Management Data Router (GMDR)
	Passport Management Data Router (FMDR)
	SNMP Management Data Router (SMDR)
	DPN Management Data Router (DMDR)
	Network Model Co-ordinator (DNMNMC)
	Network Model Surveillance Updater (SURNUP)
	Network Model Server (NMSERVER)
	Network Model Edit Server (EDSERVER)

(Sheet 1 of 3)

Table 7 (Continued)
Types of servers

Type	Servers
	Network Data Access Mediator (NDAM)
	SNMP Trap Server (TSVR)
	SNMP Data Collection Daemon (GENDCD)
	Real Time Alarm Collection (RTACCOL)
	VPN Monitor Extractor (VPNMonitorExtractor)
	VPN Monitor Server (VPNMonitorServer)
	DPN DBNL Auto Disabling Daemon (DBNLWATCH)
	Passport Command Access Server (ETESERVER)
	Fault Device Access Agent (PSVAGENT)
	SNMP IP Discovery Server (IPDSVR)
	MPE Management Data Router (NMDR)
	MDM SNMP Proxy Agent (SPA)
	GMDR Agent (GMDRAGENT)
	NM Agent (NMAGENT)
	RTAC Agent (RTACAGENT)
Configuration Management	
	Data Synchronization Server (DATASYNCSVR)
	Backup Controller (NSCTLBK)
	Restore Controller (NSCTLRST)
	Passport Backup Provider (PBCKPP)
	Passport Restore Provider (PRSTPP)
	Passport 4400 Restore Provider (PRSTPP4400)
	Passport 4400 Backup Provider (PBCKPP4400)
	Passport 4460 Restore Provider (PRSTPP4460)
	Passport 4460 Backup Provider (PBCKPP4460)

(Sheet 2 of 3)

Table 7 (Continued)
Types of servers

Type	Servers
	Passport Nodal Provisioning Configuration Server (PCSERVER)
	Passport Configuration Model Server (PCMS)
	Nodal Provisioning Configuration Manager (CONFIGMAN)
	DPN PM File Access Server (PFAS)
	DPN PM File Access Software Download (PFAS)
	End-to-End Server (ETESERVER)
	Network Configuration Database Server (NCDSVR)
Performance Management	
	Data Viewer Data Collection Daemon (PMDCD)
	Data Viewer Agent (PMAGENT)
	Performance Measurement Stream Processor (PMSP)
Accounting/Data Collection	
	MDP Disk Manager (MDPDISKMGR)
	MDP Passport File Manager (MDPPPMGR)
	MDP File Prober Manager (MDPFPMGR)
	MDP Passport Data Model Manager (MDPDMM)
	MDP Vector File Manager (MDPVSSMGR)
	MDP DPN File Collector (MDPCOL)
	MDP DPN File Manager (MDPDPNMGR)
	MDP File Mover Manager (MDPFMMGR)
	MDP Statistics Retrieval System Server (MDPSRS)
	MDP MPE Collector Manager (MDPMCMGR)
	MDP MPE File Manager (MDPMPEMGR)
Custom	Empty server template

(Sheet 3 of 3)

Editing the configuration file for a server

Some of the servers have one or more configuration files that a customer can edit. Use this procedure to edit a configuration file associated with a server.

Prerequisites

Before you begin, ensure that:

- you have started the Preside Multiservice Data Manager Server Administration tool
- are connected to the local host. Editing a configuration file is only permitted on the local host, not the remote host
- you have accessed the Edit mode
- the UNIX file and group permissions associated with your UNIX account allow you to edit the file

Procedure steps

1 In the server list, click on the name of the server whose configuration file(s) you want to edit.

The name of the server becomes highlighted to indicate that it is selected.

2 From the **Edit** menu, select **Configuration -> Edit <configuration filename>** for configuration files or **Configuration -> Launch <configuration toolname>** for a configuration tool.

The vi editor opens, or an administrator tool opens if there is one associated with the server.

Note 1: If you are connected to a remote host, the ability to edit the configuration file is disabled, and the Edit configuration menu item is grayed out.

Note 2: If you do not have permission to edit the file, the menu shows Configuration -> View <configuration filename>.

3 Make the changes to the file.

Note 1: If you do not have permission to edit the file, the menu shows Configuration -> View <configuration filename>.

Note 2: If the editor that opens is an administrator tool you may be prompted for a password to log in and make changes to the file.

4 If you need help on the syntax of a configuration file, click **Help on Server**

A Netscape window opens that provides access to information about the server and its configuration file(s).

Note: Software obtains the help information from the local host. If you are editing a server while connected to a remote host and it is not running the same release of software as the local host, there may be some differences between the help information on the local host and the software on the remote host. For example, the parameters for the start-up commands may differ.

5 Save the file and exit from it.

6 Start the server to make use of the modified configuration file.

Starting a server

Use this procedure to start a stopped or newly created server.

Prerequisites

Before you begin, ensure that:

- you have started the Preside Multiservice Data Manager Server Administration tool
- you have accessed the Edit mode
- the server you wish to start has a state of **Not Started**, **Quit,** or **Failed**. You cannot start a server that has any other state.

Procedure steps

1. In the server list, click on the name of the server you wish to start.

   The information for the server becomes highlighted to indicate that the server is selected.

2. From the **Options** menu, select **Start**.

   In the server list, the server's state changes to **Running**. In the activity log, a log appears showing the time and date at which the server was started.

   It may take a while for the server to start if it relies on information from another server that is not started. While waiting for the other server the software first attempts a series of fast restarts. You set the number of these fast restarts and the interval between them in the **SVM New Server** dialog when you add the server, or in the **SVM Edit Server** dialog when you edit the server. After the software runs out of fast restarts, it begins a set of slow restarts. You also set the number of these restarts and the interval between them when you add the server. The software continues to attempt these slow restarts the number of times you specified before it finally gives up trying to start the server.

Changing the start-up order of servers

You can change the start-up order of servers in the server list of the Preside Multiservice Data Manager (MDM) Server Administration window.

By changing the start-up order, you can ensure that a server that provides information to another server is started first.

Prerequisites

Before you begin, ensure that:

- you have started the Preside Multiservice Data Manager (MDM) Server Administration tool
- you are connected to the local host or a remote host that is running MDM release 14.3 or greater
- you have accessed the Edit mode

Procedure steps

1. Click on a server in the server list to select it.

   The server becomes highlighted to indicate that it is has been selected

2. Click the up arrow to move the server up the list or the down arrow to move the server down the list.

   The software automatically saves the start-up order of the servers. Moving a server causes information about the event to appear on the activity log area of the window.

Stopping a server

Uses this procedure to stop a server that is in the **Running** or **Exited** state.

Prerequisites

Ensure that:

- you have started the Preside Multiservice Data Manager (MDM) Server Administration tool
- you have accessed the Edit mode
- the server you wish to stop is in the **Running** or **Exited** state. You cannot stop a server in another state.

Procedure steps

1 In the server list, click on the name of the server you wish to stop.

The information for the server becomes highlighted to indicate that the server is selected.

2 From the **Options** menu, select **Stop**.

In the server list, the server's state changes to stopped. In the activity log, a log appears showing the time and date at which the server was stopped.

The software displays a log in the following format in the MDM Log Display tool:

```
<server_name> stopped by signal 9
<server_name> restarted (<restarts>/<max_restarts>)
```

where:

`<server_name>` is the name of the server being stopped.

`<restarts>` is the restart number. See Server list (page 344) for more information.

`<max_restarts>` is the maximum number of restarts configured for the server.

Editing a server

Use this procedure to edit a server that is stopped.

Prerequisites

Ensure that:

- you have started the Preside Multiservice Data Manager Server Administration tool
- you have accessed the Edit mode
- you have stopped the server

Procedure steps

1. In the server list, double-click on the server you wish to work on.

   The server is selected in the server list and the **SVM Edit Server** dialog opens. The dialog displays the current information for the server.

2. Change the information by modifying fields or resetting buttons.

3. If you are not sure about what to enter in the fields, click **Help on server**

   A Netscape window opens that provides access to information about the server and its configuration file(s).

   Note: Software obtains the help information from the local host. If you are editing a server while connected to a remote host and it is not running the same release of software as the local host, there may be some differences between the help information on the local host and the software on the remote host. For example, the parameters for the start-up command may differ.

4. Do one of the following to save modified server information:

   - Close the dialog, click **OK** if the server is running. The server is automatically restarted.
   - Click **Save and Restart** to leave the dialog open, and restart a server that is already running.

Deleting a server

Use this procedure to ensure delete a server that is not defined as a permanent server.

Prerequisites

Ensure that:

- you have started the Preside Multiservice Data Manager Server Administration tool
- you have accessed the **Edit** mode
- you have stopped the server
- the server is in the **Not Started**, **Quit** or **Failed** state

Procedure steps

1. In the server list, select the server you wish to delete.
2. From the **Edit** menu, select **View server**

   The **SVM View Server** dialog opens.
3. Look at the field labelled **Permanent entry**

   This field takes its value from a field called permanent entry in file opt/MagellanNMS/cfg/SVMList.cfg. When it is set to False you can delete the server. However, when it is set to true, you cannot remove the server.
4. Is the value of the **Permanent entry field True** or **False?**
   - If it is set to **False**, you can delete the server, continue at step 5
   - If it is set to **True**, edit file opt/MagellanNMS/cfg/SVMList.cfg and change the setting of the permanent entry field to **False**. Save the file, exit from it, then continue at step 5
5. Click **OK** to close the dialog.
6. Right-click on the server name and select **Remove**.

   The server is removed from the list.

Logging out as administrator and accessing view mode

Use this procedure to return to the view mode of the tool, if you are already in edit mode.

Procedure steps

1. From the **Security** menu, select **Unauthorize**.

   The **SVM Confirm Unauthorization** dialog opens.

2. Click **Yes** to confirm the return to view mode.

   The dialog closes and the tool enters view mode.

Printing server management data

Use this procedure to print server management data that is displayed in the main window.

Procedure steps

1. From the **File** menu, select **Print**.

   The **SVM Print** dialog opens.

2. In the printer list, click on the button beside the name of the printer on which you wish to print the server information.

   By default, both types of server information are selected to be printed out: information in the server list and information in the activity log.

3. For the information you do not want included in the printout, click **Print server list,** or **Print server event logs**.

4. Click **OK**.

   The **SVM Print** dialog closes and server information is sent to the printer.

Cleaning up log files

Server management data gradually accumulates in two files: /opt/MagellanNMS/data/svm/SVM.errors and /opt/MagellanNMS/data/svm/SVM.logs. If you have been experiencing numerous server problems, these files can become very large. Should disk space become scarce, you can free up some room by deleting these files or by trimming down their contents.

The following is an example of the commands you enter to trim these files down to 20 records (lines) each on a workstation called hosta.

```
cd /opt/MagellanNMS/data/svm
mv SVM.errors errors
tail -20 errors > SVM.errors
chmod +w SVM.errors
mv SVM.logs logs
tail -20 logs > SVM.logs
chmod +w SVM.logs
rm errors logs
```

Cleaning up log files using mdmlogclean

A log clean up process called mdmlogclean removes log files from a server after a certain number of days. The mdmlogclean process is run from the command line as the root user.

The mdmlogclean log file has the naming convention: /opt/MagellanNMS/data/log/mdmlogclean/mdmlogclean.alog. The directory that the logs are located in determines the retention time of certain logs. The mdmlogclean process has the following command line arguments:

```
mdmlogclean
[-help]
[-v]
[-file <file name>]\
[-logFile [<log level set>]] \
```

where:

`-help` provides the usage information to the user.

`-v` verbose is set if specified.

`-file <mdmlogclean config>` specifies the configuration file that defines log directories where log files should be deleted after a given retention period. The default is /opt/MagellanNMS/cfg/MDMClean.cfg, if an option is not specified.

`[-logfile <logLevels>]` optionally, writes logs of a given level to a log file. Levels are one or more of the following, separated by commas: FATAL, ALERT, CRIT, ERROR, WARN, INFO, NOTICE, DEBUG, TRACE.

The configuration file /opt/MagellanNMS/cfg/MDMClean.cfg separates the records by a line feed. Consecutive non-empty lines constitute a single record.

```
Directory: /opt/Magellan/data/log/oam
RetentionDays: 30


Directory: /opt/MagellanNMS/data/log/svmdmn
RetentionDays: 30
```

Determining why a server will not start or exit

The two most reasons why a server will not start or exits are:

- the server depends on another server that is not started, or that is taking longer than expected to initialize
- the server is configured incorrectly

Use this procedure to find and correct the source of the problem.

Procedure steps

1. From the MDM toolset, select **System -> Administration -> System Log Display**. Then try to start the server from the Server Administration tool. If the server exits, look at the System Log Display to why the server didn't start. If the information is not provided, go to step 2.
2. Access the edit mode.
3. Click on the name of the server that will not start or has exited.
4. From the **Edit** menu, select **Help on server.**

   A Netscape window opens that provides access to information about the server and its configuration file(s).
5. In the help information, look at the section titled **Start-up command**. Ensure that the syntax of the start-up command you entered conforms to the help information, and correct it, if necessary.

   If you entered the start-up command correctly, there is another problem, continue at step 5.
6. In the help information, look at the section titled **Dependencies**. This section contains information about the servers that the server relies on.
7. Are the servers that this server relies on started?
   - If they are not started, start the servers then attempt to restart this server.
   - If they are started, there is another problem. Continue at step 7.
8. In the help information look up the meaning of the error codes or error message displayed in the log information. In many cases the help information will provide you with corrective action to take.
9. If none of the previous actions corrects the problem, the next most likely problem is incorrect setup of a configuration file. In the help information

look up information about the configuration files, examine the contents of the configuration files to ensure they are set up correctly.

10 If none of these steps solves the problem, contact Nortel Networks.

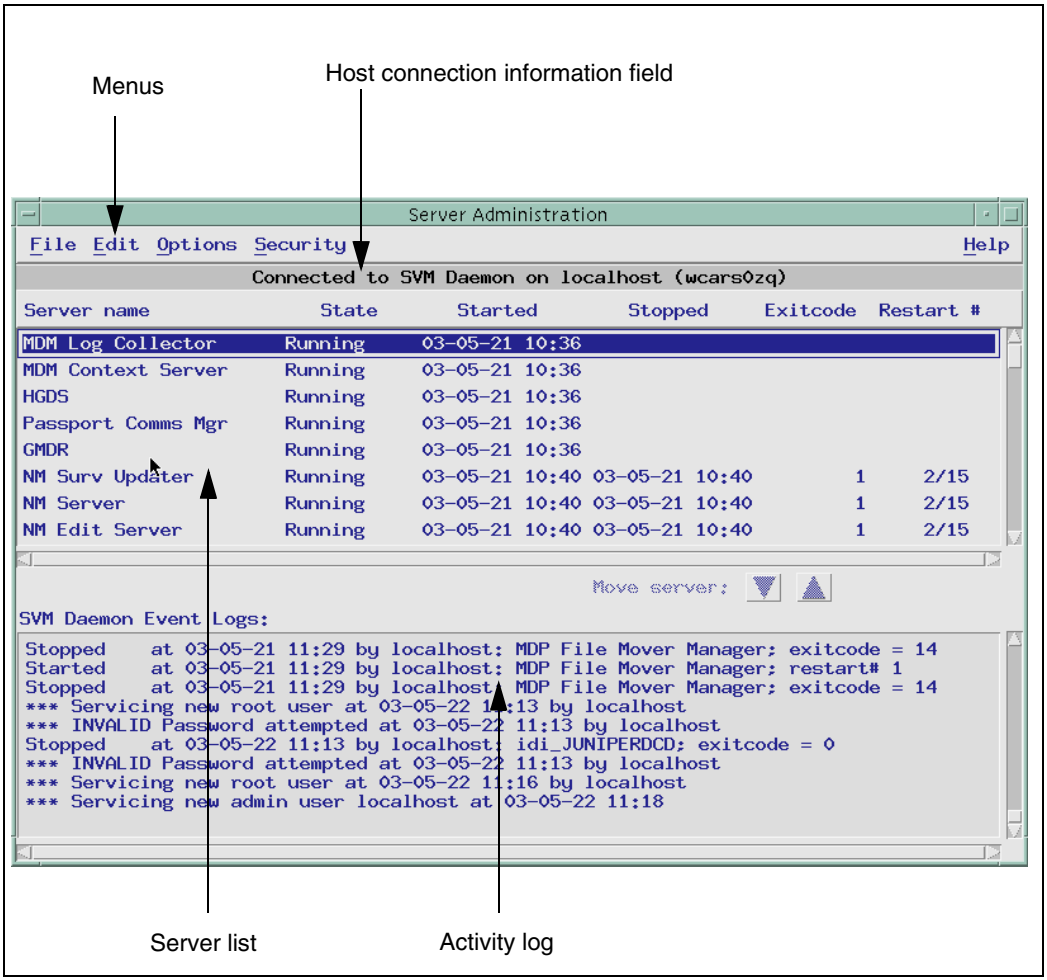
User interface

Server Administration window

The **Server Administration** window is shown in the Figure 35 on page 341.

This section contains the following topics:

Figure 38
Server Administration window



File menu

The **File** menu contains the following commands:

- **Print** opens the **SVM Print** dialog. This dialog lets you print information about a server on the printer defined by environment variable $LPDEST. The value of this variable is set in your user account's set-up files.

- **Refresh server list** updates the server list with a new copy from the Server Daemon (SVMDMN) process.
- **Exit** closes the Server Administration tool.

Edit menu

The **Edit** menu contains the following commands:

- **New server** opens the **SVM New Server Selection** dialog. This dialog lets you add a new server to the server list.

  The **New server** command is only enabled when the tool is in edit mode.

- **Edit server** opens the **SVM Edit Server** dialog. This dialog lets you change the operating parameters of a server that is selected in the server list and to restart the server automatically when the workstation is booted.

  The **Edit** server command is only enabled when the tool is in edit mode.

- **Configuration -->Edit <configuration filename>** opens the configuration file associated with the server in the vi editor for editing. This menu item is available when the user of the SVMAdmin session has permission to overwrite the configuration file.
- **Configuration -->View <configuration filename>** opens the configuration file associated with the server in the vi editor to be viewed (read-only). This menu item is available when the user of the SVMAdmin session does not have permission to overwrite the configuration file.
- **Configuration -->Launch <configuration toolname>** launches the configuration edit tool used for the server. This menu item is used when there is a configuration edit tool used for the server. The edit tool handles user permissions after it has been launched.
- **View logs** launches the Log Browser to view the selected server's logs from the file /opt/MagellanNMS/data/log/<servername>/<servername>.alog. See "Log Browser dialog" on page 395.

- **View server** opens the **SVM View Server** dialog. This dialog displays the startup command and the operating parameters of a server that is selected in the Server List.

  The **View server** command is enabled when the tool is in view mode or in edit mode.

- **Remove** server deletes a server that is selected in the server list. You can only remove a server whose state is **Not Started**, **Quit** or **Failed**. It is only possible to remove a server that has not been configured as permanent. See "Permanent entry field" on page 397.

  The **Remove server** command is only enabled when the tool is in edit mode.

- **Help on server** opens a Netscape window that provides access to help information about the server. This help information includes the suggested descriptive name of the server, the syntax of the start-up command, and information about configuration files associated with the server.

Options menu

The **Options** menu contains the following commands:

- **Choose host** opens the **SVM Host dialog.** This dialog lets you select the host for which server information is displayed in the window of the tool.
- **Start** starts a server selected in the server list. This command is enabled after you have been authorized to perform this function. Select **Security**, and then **Authorize** from the Server Administration window. See "Accessing the edit mode" on page 366.
- **Stop** stops a running server that is selected in the server list and prevents the system from attempting to restart it automatically. This command is enabled after you have been authorized to perform this function. Select **Security**, and then **Authorize** from the Server Administration window. See "Accessing the edit mode" on page 366.

Security menu

The **Security** menu contains the following commands:

- **Authorize** puts the tool in edit mode. When you select this command, the **SVM Enter Authorization Password** dialog opens and prompts you for a password. Once you enter a valid password, the tool enters the edit mode, the **New**, **Edit**, **Remove, Start** and **Stop** commands become active.

  The **Authorize** command is only enabled when the tool is in view mode.

- **Unauthorize** causes the tool to leave the edit mode and accesses the view mode. When you select this command, the **SVM Confirm Unauthorization** dialog opens and prompts for confirmation that you wish to leave edit mode. Clicking **OK** confirms this command, the tool enters the view mode, the **View** command becomes active in the **Edit** menu, and the **New**, **Edit**, **Remove, Start** and **Stop** commands become inactive.

  The **Unauthorize** command is only enabled when the tool is in edit mode.

- **Change password** lets you change the current password required to access editing mode and to set a password if no password yet exists. When you select this command the **SVM Change Authorization Password** dialog opens, and prompts you for the existing password and a new password. If you are running the tool for the first time and no password exists, enter a carriage return for the old password.

  The **Change password** command is only enabled when the tool is in edit mode.

Help menu

The **Help** menu contains the following commands:

- **On Context** displays context-sensitive help information. When you select this menu item, a question mark is displayed on the screen. Moving this question mark to various fields and buttons in the window and clicking the select mouse button displays help information about the field or button selected.

- **On Window** displays general help information about the Server Administration tool.

Host connection information field

The host connection information field indicates the host name of the workstation for which server information is being displayed.

Server list

The server list displays information about the servers on the workstation whose host name is displayed in the host connection information field. For each server, it shows the current state of the server, when it was last started, when it last stopped running, the most recent exit code, and the number of times it has been restarted. Fields in the server list are as follows:

- **Server name** is a descriptive name assigned to the server.
- **State** is the state of the server, which is one of the following:

  Not started indicates that the server has not been started since the SVMDMN process was started or since it was added to the list.

  Running indicates that the server has been started automatically by the SVMDMN process or by an administrator.

  Exited indicates that the server has exited unexpectedly and is awaiting a restart. When a server is in this state, information about the server is displayed on a yellow background.

  Quit indicates that the server has shut itself down. No restarts are being attempted. When a server is in this state, information about the server is displayed on a red background.

  Failed indicates that the server has exceeded all restart limits. No further attempts to restart it automatically are being made. When a server is in this state, information about the server is displayed on an orange background.

  Note: An asterisk (*) that appears in front of any state except Not started indicates that the server is in a slow restart cycle. The Failed state is always prefixed with an asterisk.

- **Started** is the date and time at which the server was last started. If the server has never been started, the field is blank.
- **Stopped** is the date and time at which the server last exited or was stopped. If the server has never exited or been stopped, this field is blank.
- **Exitcode** is the return code used by the server on its last exit. If the server has never been started or has never stopped running, this field is blank. An exit code of 50 means that the server will not be restarted (that is, its state will be set to Quit). All other exit codes are server-specific.
- **Restart#** is the number of times the server has been restarted after exiting. If the server has never been started, or has never stopped running, this field is blank. This value is always shown as the current number of restarts over the maximum number of restarts configured for that server (for example, 3/15). The restart number is incremented each time the server exits and restarts. The restart number resets to 1 when the server is stopped and restarted.

Server Functions pop-up menu

The **Server Functions** pop-up menu appears when you right-click the mouse anywhere in the server list. This menu contains the following choices:

- **New server** opens the **SVM New Server Selection** dialog. See "Adding a new server" on page 367.
- **Edit server** opens the **SVM Edit Server** dialog. See "Editing a server" on page 377.
- **Configuration -->Edit <configuration filename>** opens the configuration file associated with the server in the vi editor for editing. This menu item is available when the user of the SVMAdmin session has permission to overwrite the configuration file.
- **Configuration -->View <configuration filename>** opens the configuration file associated with the server in the vi editor to be viewed (read-only). This menu item is available when the user of the SVMAdmin session does not have permission to overwrite the configuration file.

- **Configuration -->Launch <configuration toolname>** launches the configuration edit tool used for the server. This menu item is used when there is a configuration edit tool used for the server. The edit tool handles user permissions after it has been launched.
- **View logs** launches the Log Browser to view logs the selected server's logs in the file /opt/MagellanNMS/data/log/<servername>/<servername>.alog. See "Log Browser dialog" on page 395.
- **View server** opens the **SVM View Server** dialog. See "Viewing a server" on page 364.
- **Remove server** removes a server from the server list. See "Deleting a server" on page 378.
- **Help on server** opens a Netscape window that provides access to help information about the server. This help information includes the suggested descriptive name of the server, the syntax of the start-up command, and information about configuration files associated with the server.
- **Start server** starts a server that is selected in the server list. See "Starting a server" on page 374.
- **Stop server** stops a server that is running and prevents the system from attempting to restart it automatically. See "Stopping a server" on page 376.

The **New**, **Edit**, **Remove Start**, and **Stop** commands are only enabled after you have been authorized to perform these functions. You must select **Security**, and then **Authorize**, and enter a valid password before these commands are enabled. The **View** command does not require authorization.

Activity log

The activity log displays information about events that occur on servers present since the most recent system restart. The activity log displays all events in chronological order, with the most recent events first.

These events can be the result of internal server conditions, of your actions, or the actions of other users of the Server Administration tool either on this workstation or on remote hosts.

Activity log pop-up menu

The activity log pop-up menu opens when you right-click the mouse on any portion of the activity log. This menu contains the following choices:

- **Copy** copies the selected text from the activity log to the cut and paste buffer.
- **Select all** selects all of the text in the activity log.
- **Deselect all** deselects all text in the activity log.

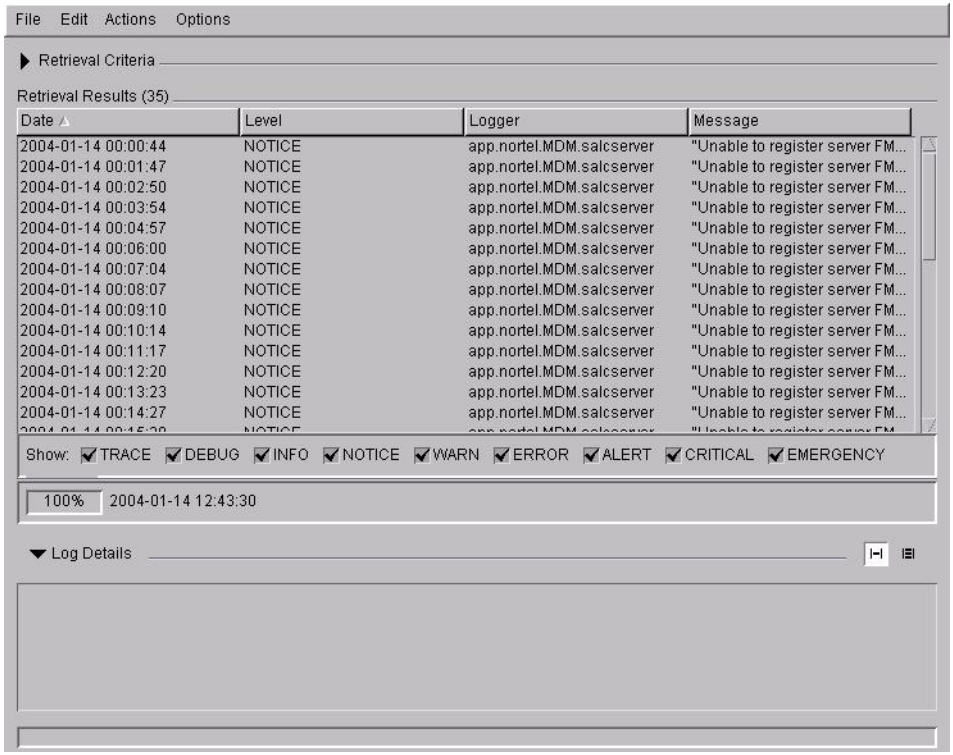
Dialogs

The Server Administration tool is equipped with the dialogs described in the following sections:

Log Browser dialog

The **Log Browser** displays the log files associated with the server.This dialog is invoked from the **Edit menu --> View logs** for the selected server or by right-clicking on the selected server name and selecting **View Logs**. See "Viewing logs associated with a server" on page 365.

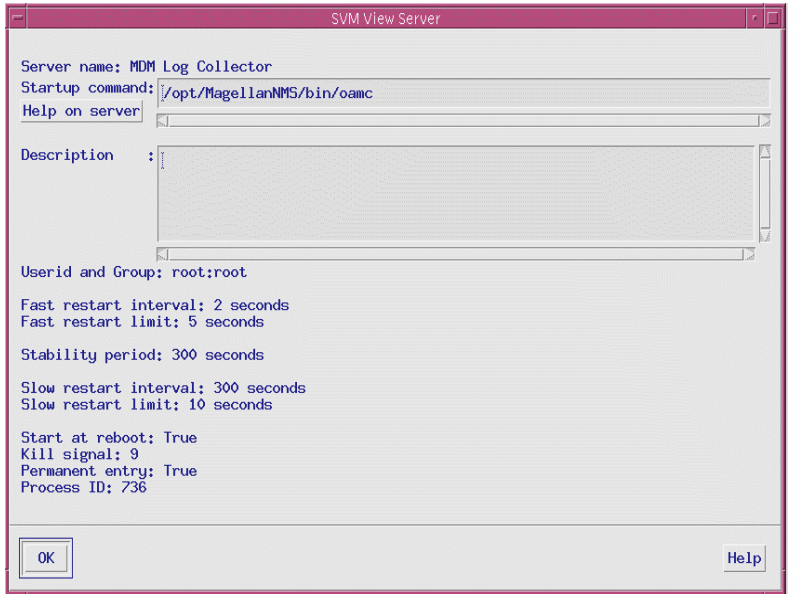
Figure 39
Log Browser



SVM View Server dialog

The **SVM View Server** dialog displays current information about the server and its restart parameters. For an explanation of the **Permanent entry** field, see "Permanent entry field" on page 397. For an explanation of the remaining fields in this dialog, see "SVM View Server dialog" on page 396.

Figure 40
SVM View Server dialog



OK button

The OK button closes the dialog.

Help button

The Help button displays a description of the fields and buttons in the dialog.

Help on server button

The Help on server button opens a Netscape window that provides access to help information about the server. This help information includes the suggested descriptive name of the server, the syntax of the start-up command, and information about configuration files associated with the server.

Permanent entry field

The value of the **Permanent entry** field is the value of the option named permanent_entry in the file /opt/MagellanNMS/cfg/SVMList.cfg. This option determines whether you can remove the server. When it is set to True, you cannot remove the server. To remove the server, set permanent_entry to False and restart the Preside Multiservice Data Manager servers.

When you add new servers using the Server Administration tool, permanent_entry is set to False.

For information on stopping a server, see Preferred kill signal menu button (page 354).

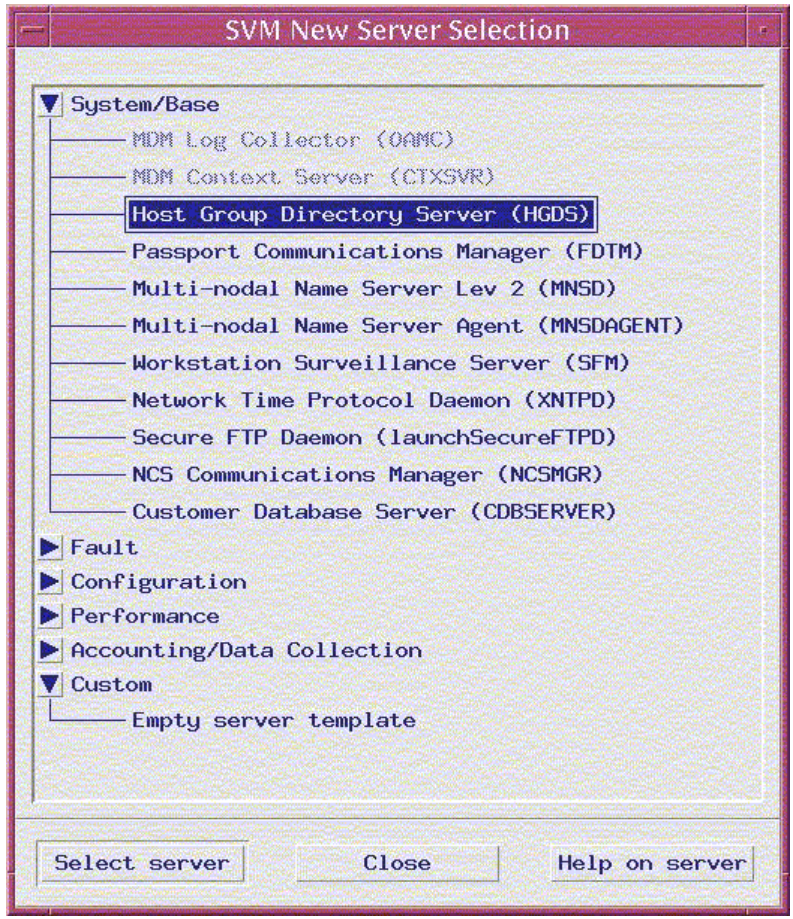
SVM New Server Selection dialog

This dialog lets you select a new server to add from a list of six types of servers: System/Base, Fault, Configuration, Performance, Accounting/Data Collection, and Custom. This dialog only opens when you are connected to the local host.

Clicking on the arrow to the left of any of the six types of servers in the New Server List dialog expands the list of servers to show the servers that belong to the type of server (System/Base, Fault...). Clicking on the name of a server in the expanded list selects the server in preparation for adding the server.

Clicking on the arrow to the left of any of the six types of servers contracts the list and hides the servers that belong to the type of server.

Figure 41
SVM New Server Selection dialog



Select server

Once you have expanded the list and clicked on the name of a server you want to add, clicking the **Select server** button opens an **SVM New Server** dialog that contains default values for the server you selected.

Close

Clicking the **Close** button closes the **New Server List** dialog and cancels the addition of any server that you have selected in the server list.

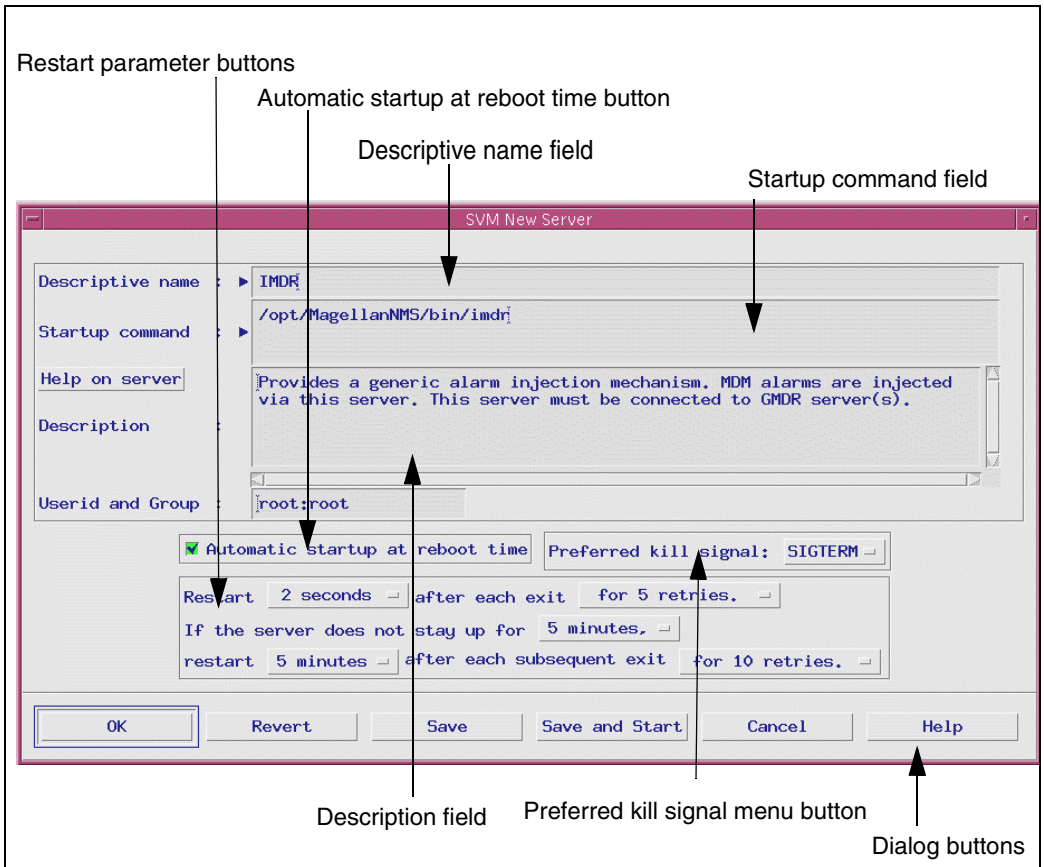
Help on server

Clicking the **Help on Server** button opens a Netscape window that provides access to help information about the server. This help information includes the suggested descriptive name of the server, the syntax of the start-up command, and information about configuration files associated with the server.

SVM New Server dialog

The **SVM New Server** dialog lets you set up a new server on the current host.

Figure 42
SVM New Server dialog



Note: This illustration shows the contents of the dialog if you are adding a server to remote host. On a remote host, the fields are empty. On a local host, the fields contain default values.

The **SVM New Server** dialog for new servers contains the fields and items described in the following sections When you are connected to a local host, fields in the dialog contain default values, but when you are connected to a remote host, fields in the dialog are empty.

Descriptive name field

The **Descriptive name** field accepts a name for the server with a maximum length of 22 characters. This name must be unique.

Startup command field

The **Startup command** field accepts the absolute pathname of the server and arguments required to start the server. The absolute pathname must contain fewer than 512 characters, and the absolute pathname with the arguments must contain fewer than 1024 characters.

For the startup commands to start all basic Preside Multiservice Data Manager (MDM) servers, see 241-6001-310 *Preside MDM Server Reference Guide*.

The following command starts an FMIP Management Data Router (FMDR) server for a group called TREES, a user ID of thawkes, and a password of grapefruit:

```
/opt/MagellanNMS/bin/fmdr -g TREES -u thawkes -p
grapefruit
```

Help on server button

Clicking the **Help on Server** button opens a Netscape window that provides access to help information about the server. This help information includes the suggested descriptive name of the server, the syntax of the start-up command, and information about configuration files associated with the server.

Description field

The **Description** field contains information on the server and what it is used for.

Automatic startup at reboot time button

The **Automatic startup at reboot time** button starts the server automatically using the command entered in the **Startup command** field whenever the workstation is rebooted.

This parameter is displayed as **Start at reboot** in the **SVM View Server** dialog, and is the autostart option in the svmcmd utility.

Preferred kill signal menu button

Preferred kill signal lets you set the UNIX kill signal used to stop a server when a user selects a server from the servers list, then chooses **Stop** from the **Options** menu or from the server list pop-up menu. You can only modify the preferred kill signal for a server you create. You cannot modify the preferred kill signal for a Preside Multiservice Data Manager (MDM) defined server. For example, you cannot modify this signal for the MDM Log Collector (OAM) server.

Only a subset of all UNIX signals are provided in the menu button. These are: **SIGHUP**, **SIGQUIT**, **SIGKILL**, **SIGTERM**, **SIGUSR1**, and **SIGUSR2**. For details about these signals refer to the signal(5) man page. You can add or delete signal options from this menu button by customizing X-resources in file /opt/MagellanNMS /lib/app-defaults/C/Svmadm. For information about customizing X resource files, see 241-6001-301 *Preside MDM Customization Administrator Guide*.

Restart parameter buttons

These buttons set parameters that govern how the system software attempts to restart the server automatically when the server exits.

When a server exits, the Server Administration software attempts a series of fast restarts (fast restart cycle) on the server. If these fail, it attempts a series of slow restarts (slow restart cycle) before it finally gives up attempting to restart the server.

Parameters to set up restarts are as follows:

`Restart <n> seconds after each exit for <n> retries`

specifies the fast restart cycle

`Restart <n> seconds after each exit`

specifies the delay between each restart in the fast restart cycle.

This parameter is displayed as the **Fast restart interval** in the **SVM View Server** dialog and is the fri option in the svmcmd utility.

`for <n> retries`

specifies the number of restarts to be performed before the tool stops attempting fast restarts and begins attempting slow restarts

This parameter is displayed as the **Fast restart limit** in the **SVM View Server** dialog and is the frl option in the svmcmd utility.

`If the server does not stay up for <n> minutes, restart <n> minutes after each subsequent exit for <n> retries`

specifies the slow restart cycle

`If the server does not stay up for <n> minutes`

specifies how long the server must stay running before it can be considered stable enough to be moved back into fast restart cycle should another restart occur

This parameter is displayed as the **Stability period** in the **SVM View Server** dialog and is the sp option in the svmcmd utility.

`restart <n> minutes after each subsequent exit`

specifies the delay between each restart in the slow restart cycle

This parameter is displayed as the **Slow restart interval** in the **SVM View Server** dialog and is the sri option in the svmcmd utility.

`for <n> retries`

specifies the number of times the server is restarted in the slow restart cycle before the software gives up attempting restarts. If it does, the software displays **Failed** in the **State** column of the server list.

This parameter is displayed as the **Slow restart limit** in the **SVM View Server** dialog and is the srl option in the svmcmd utility.

Help on server button

The Help on server button opens a Netscape window that provides access to help information about the server. This help information includes the suggested descriptive name of the server, the syntax of the start-up command, and information about configuration files associated with the server.

Dialog buttons

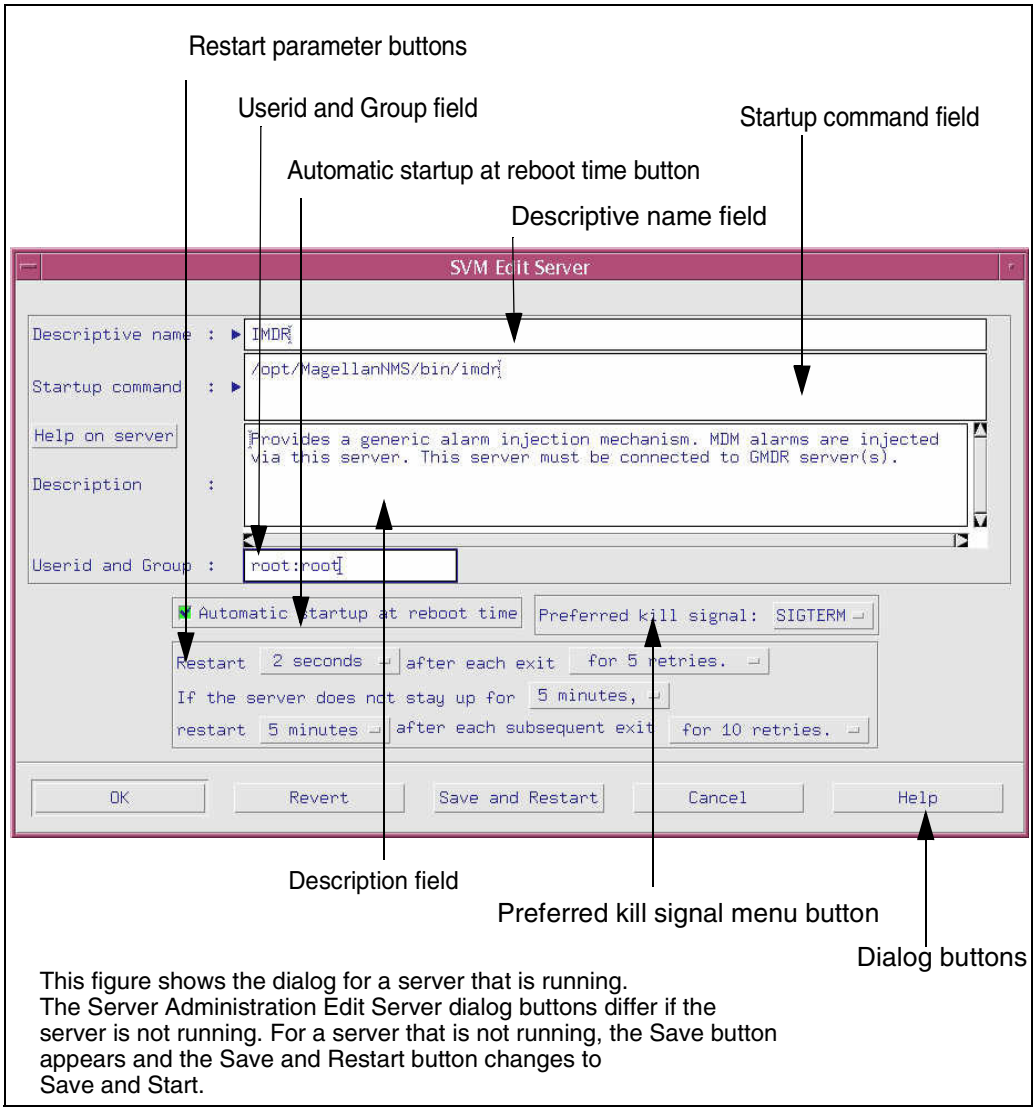
The dialog buttons at the bottom of the **SVM New Server** dialog are as follows:

- **OK** saves the values you entered in the dialog, and closes the dialog.
- **Revert** clears all editable information from the dialog, resets all fields to their
- default values, and leaves the dialog open.
- **Save** stores all data you entered, clears the fields of the dialog, and leaves the dialog open, but does not start the server.
- **Save and Start** stores all data you entered, clears the fields of the dialog, leaves the dialog open, and starts the server.
- **Cancel** closes the dialog without saving any of your entries.
- **Help** displays help information.

SVM Edit Server dialog

The **SVM Edit Server** dialog lets you modify the operating parameters of a server and start the server.

Figure 43
SVM Edit Server dialog



This figure shows the dialog for a server that is running. The Server Administration Edit Server dialog buttons differ if the server is not running. For a server that is not running, the Save button appears and the Save and Restart button changes to Save and Start.

The **SVM Edit Server** dialog contains the items described in the following sections:

Descriptive name field

The **Descriptive name** field accepts a name for the server with a maximum length of 22 characters. This name must be unique.

- If the server is configured as permanent (see "Permanent entry field" on page 397), the descriptive name is displayed in light grey and you can view it, but not modify it. Examples are: MDM Log Collector and MDM Context Server.
- If the server is one not configured as permanent, you can modify the server name.

Startup command field

The **Startup command** field accepts the absolute pathname of the server and the arguments required to start the server. The absolute pathname must contain fewer than 512 characters, and the absolute pathname with the arguments must contain fewer than 1024 characters.

If the server is configured as permanent, the pathname for the startup command cannot be modified. You can, however, change the startup command arguments freely.

For the startup commands to start basic Preside Multiservice Data Manager (MDM) servers, see 241-6001-310 *Preside MDM Server Reference Guide*.

Description field

The **Description** field contains information on the server and what it is used for.

UserID and Group field

The **UserID and Group** field specifies the Userid and Group setting for the server when it is launched. The default setting for both Userid and Group is root. The format is for this field is the Userid setting, colon (:), Group setting, for example, root : root.

> ***Note:*** Changing the default setting increases server security and can help to prevent users from writing data to protected file systems.

Automatic restart at reboot time button

The **Automatic restart at reboot time** button causes the server to start automatically using the command entered in the **Startup command** field whenever the workstation is rebooted.

Preferred kill signal menu button

The **Preferred kill signal** menu button performs the function described in "Preferred kill signal menu button" on page 403.

Restart parameter buttons

The **Restart parameter** buttons perform the functions described in "Restart parameter buttons" on page 403.

Dialog buttons

The dialog buttons at the bottom of the **SVM Edit Server** dialog are as follows:

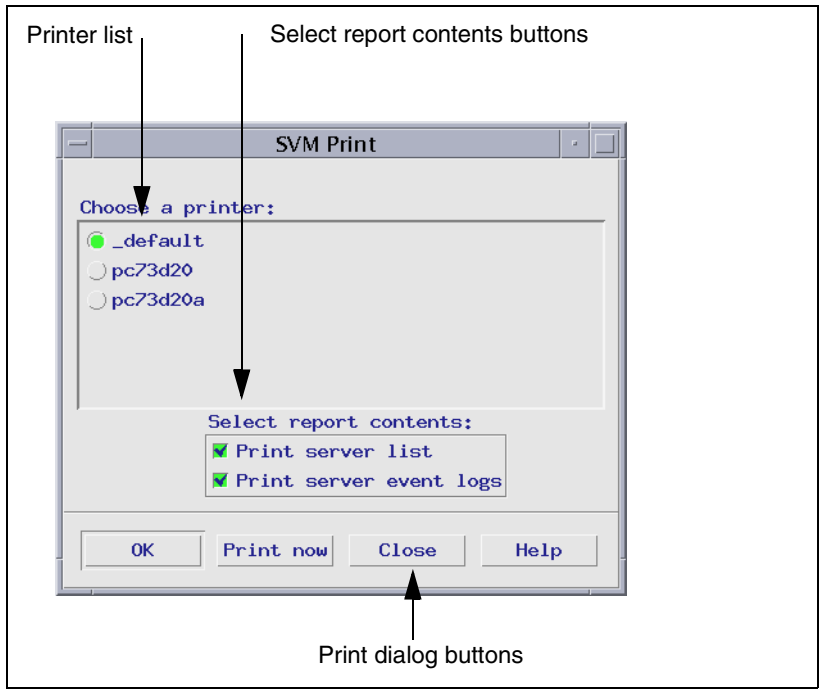
- **OK** saves the values you entered in the dialog, and closes the dialog. If the server is already running, it is restarted.
- **Revert** clears all editable information from the dialog, resets all fields to the values that they had when they were last saved, and leaves the dialog open.
- **Save and Restart** stores all data you entered, leaves the dialog open, and restarts the server. This button only appears in the dialog for a server that is running.
- **Cancel** closes the dialog without saving any of your edits.

- **Help** displays help information for the dialog itself.
- **Help on Server** opens a Netscape window that provides access to help information about the server. This help information includes the suggested descriptive name of the server, the syntax of the start-up command, and information about configuration files associated with the server.

SVM Print dialog

The **SVM Print** dialog lets you print information about a server.

Figure 44
SVM Print dialog



The dialog contains the items described in the following sections:

- Printer list (page 362)
- Select report contents list (page 362)
- "SVM Print dialog buttons" on page 411

Printer list

The **Choose a printer** list displays a list of all of the printers that you can select to print information about thePreside Multiservice Data Manager (MDM) servers. MDM software builds this list by executing the UNIX lpstat command in the background. The tool makes the assumption that all of the printer names displayed are valid and that the printers are working.

Select report contents list

The **Select reports contents** list let you to select the type of information to be printed. The choices are as follows:

- **Print server list** prints the contents of the server list.
- **Print server event logs** prints the contents of the activity log.

SVM Print dialog buttons

The SVM Print dialog buttons are as follows:

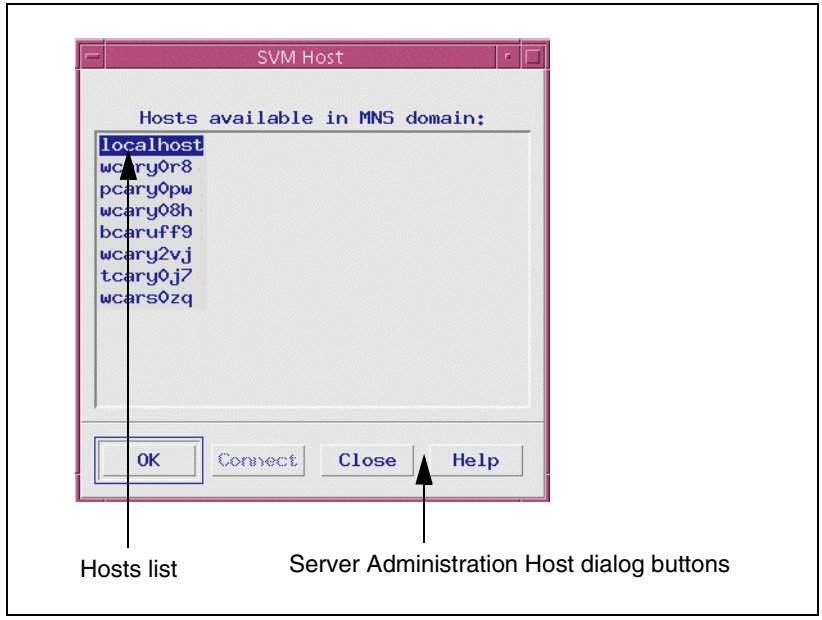
- **OK** prints the contents of the server list, the activity log, or both of these, according to the setting of the select report buttons, then closes the Print dialog.
- **Print now** prints the contents of the server list, the activity log, or both of these, according to the setting of the select report buttons, but leaves the SVM Print dialog open.
- **Close** closes the SVM Print dialog without printing.
- **Help** displays help information about the SVM Print dialog.

SVM Host dialog

The **SVM Host** dialog lets you select the host for which server information is displayed in the main window of the Server Administration tool.

To open this dialog from the **Options** menu, select **Choose host**.

Figure 45
SVM Host dialog



The **SVM Host** dialog contains the items described in the following sections:

- "Hosts list" on page 412
- "SVM Host dialog buttons" on page 413

Hosts list

The hosts list displays the host names of all Preside Multiservice Data Manager (MDM) workstations that are part of the multi-nodal naming service (MNS) domain to which this workstation belongs. For an explanation of what an MNS domain is, see Configuring Multi-nodal Naming Service domains (page 179).

The host name called localhost is always displayed in the hosts list and represents the MDM workstation that you are working on. The host names of the other workstations displayed are those that belong in the same MNS domain as this workstation.

SVM Host dialog buttons

The **SVM Host** dialog buttons are as follows:

- **OK** connects to the host name that is highlighted in the dialog and closes the dialog.
- **Connect** connects to the host name that is highlighted in the dialog, and leaves the dialog displayed on the screen.
- **Close** closes the dialog without selecting a new host.
- **Help** displays help information.

Instead of selecting the host name by clicking **OK**, you can place the cursor on the name of the host and double-click the mouse. This selects the host name and closes the window.

SVM Enter Authorization Password dialog

The **SVM Enter Authorization Password** dialog prompts you for a password to access the edit mode of the Server Administration tool.

If there is an existing password, enter it in the **Password** field, then click **OK** to close the dialog and access the edit mode.

If this is the first time the tool has been started and no password is set, press enter in the Password field. This closes the dialog and accesses the edit mode. Then set a password by selecting **Security**, and then **Change Password**.

Figure 46
SVM Enter Authorization Password dialog

The buttons in this dialog are as follows:

- **OK** validates the password, and if it is valid, closes the dialog and accesses the edit mode.
- **Clear** deletes characters entered in the Password field and leaves the dialog open.
- **Cancel** closes the dialog without validating the password.
- **Help** provides access to information about the dialog.

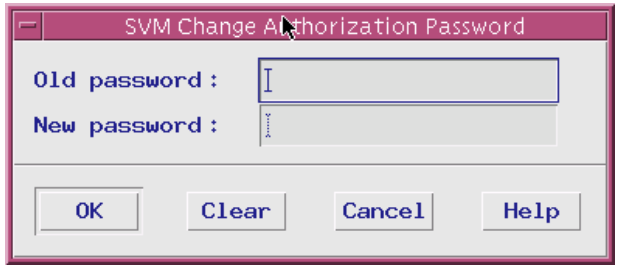
SVM Change Authorization Password dialog

The **SVM Change Authorization Password** dialog lets you change the existing password for accessing the edit mode of the Server Administration tool, or to set a password if none exists.

If there is an existing password, enter it in the **Old Password** field, enter the new password in the **New Password** field, then click **OK**.

If this is the first time the tool has been started and no password exists, do not enter anything in the **Old Password** field, just enter a password in the **New Password** field, then click **OK**.

Figure 47
SVM Change Authorization Password dialog



The buttons in this dialog are as follows:

- **OK** validates the old and new passwords, and if they are valid resets the password and closes the dialog.
- **Clear** deletes characters entered in both fields and leaves the dialog open.
- **Cancel** closes the dialog without validating the passwords.
- **Help** provides access to information about the dialog.

SVM Confirm Unauthorization dialog

The **SVM Confirm Unauthorization** dialog causes the tool to leave the edit mode and access the view mode.

When you select the **Unauthorize** command from the **Security** menu, the **SVM Confirm Unauthorization** dialog opens and prompts for confirmation that you wish to leave edit mode. Clicking **OK** confirms this command. The tool enters the view mode, and the **View** command becomes active in the **Edit** menu, and the **New**, **Edit**, **Remove, Start** and **Stop** commands become inactive.

The **Unauthorize** command is only enabled when the tool is in edit mode.

Confirmation dialogs

A confirmation dialog asks you to affirm an action before the software carries it out. The Server Administration tool has a number of similar confirmation dialogs. Buttons in these dialogs are as follows:

- **Yes** confirms the action you are taking. These actions include:
  - — closing the Server Administration dialog for new servers or the Server Administration dialog to edit servers without saving any edits you have made
  - — deleting a server you have selected for removal
  - — saving information entered in the **SVM New Server** dialog or the **SVM Edit Server** dialog.
  - — discarding new information you entered in the **SVM New Server** dialog for new servers or changes you made in the **SVM Edit Server dialog.**
- **No** dismisses the confirmation dialog without taking any action
- **Help** displays help information

Keyboard shortcuts

The Server Administration tool provides the following useful shortcuts:

- `Ctrl + R` refreshes the server list.
- `Ctrl + E` closes the Server Administration tool and any of its dialogs that are open.
- `Ctrl + N` opens the **SVM New Server** dialog.
- `Ctrl + I` opens the **SVM Edit Server** dialog.
- `Ctrl + S` starts a server that is selected in the server list.
- `Ctrl + T` stops a server that is selected in the server list.

Chapter 22
The svmcmd utility

This section contains information on the svmcmd utility, which provides a command line interface to the server daemon process. See the following sections for more information:

About the svmcmd

The svmcmd incorporates most of the same functionality provided by the Preside Multiservice Data Manager (MDM) Server Administration tool. That is, it provides facilities to query the list of SVM-managed servers, start and stop those servers, and add and delete servers. This functionality is provided in the form of a command line utility rather than a GUI interface.

Use the svmcmd to perform SVM management operations from either a UNIX shell command line, or incorporate svmcmd commands in scripts written in any suitable scripting language, such as ksh or perl.

For more information on the Server Administration tool, see "Using the Server Administration tool" (page 359). For more information on the server daemon process, see 241-6001-310 *Preside MDM Server Reference Guide*.

Command syntax

The svmcmd utility has the following syntax:

```
/opt/MagellanNMS/bin/svmcmd [-v] [-host <host_name>]
[-list [<server_name>]] [-api]
[-start [-e|-exactMatch] <server_name>]
[-stop [-e|-exactMatch] <server_name>]
[-delete <password> <full_server_name>]
[-add <password> <full_server_name> <server_cmd> [<autostart> [<fri>
   [<frl> [<sri> [<srl> [<sp> [<signal>]]]]]]]]
```

where:

`-v` specifies that the command is executed in verbose mode, meaning additional messages are displayed.

`-host <host_name>` specifies a host on which a server daemon (svmdmn) is running. The default value of host_name is localhost. This option mirrors the remote management capability of the SVM Administration tool.

`-list [<server_name>]` displays the list of managed servers. If you specify a server_name, only the information for that single server is displayed. The server_name is left-matching, which means that all servers whose names begin with the specified character sequence are listed.

`-api` specifies that a list output is in SVMList.cfg API format. That is, the format of the output matches the format of entries in the cfg file. Normal output is in a more readable display format.

`-start [-e|-exactMatch] <server_name>` specifies the name of a server to start running. If you do not specify the -exactMatch option, the server_name is left-matching, which means that all servers whose names begin with the specified character sequence are started. If you specify the -exactMatch option, only the server_name with the exact same name is started.

`-stop [-e|-exactMatch] <server_name>` specifies the name of a server to stop running. If you do not specify the -exactMatch option, the server_name is left-matching, which means that all servers whose names begin with the specified character sequence are stopped. If you specify the -exactMatch option, only the server_name with the exact same name is stopped.

`-delete <password> <full_server_name>` specifies the name of a server to be deleted from the list. If there is no password, use a pair of double quotes (“”). If the full_server_name contains spaces, enclose it in a pair of double quotes. Also, the full_server_name must match exactly; there is no left-matching.

`-add <password> <full_server_name> <server_cmd> [<autostart> [<fri> [<frl> [<sri> [<srl> [<sp> [<signal>]]]]]]]` specifies the name of a server to be added to the list. If there is no password, use a pair of double quotes (“”). If either the full_server_name or the server_cmd contain spaces, enclose them in a pair of double quotes. The full_server_name is restricted to 22 characters and the server_cmd is restricted to 1024 characters.

The remaining options are the following SVM server startup parameters:

`autostart` specifies whether the server starts automatically whenever the workstation is rebooted. You can set this option to 0 for false or 1 for true. The default value is 0.

`fri` is the time, in seconds, of the fast restart interval. The default value is 2.

`frl` is the time, in seconds, of the fast restart limit. The default value is 5.

`sri` is the time, in seconds, of the slow restart interval. The default value is 300 (5 minutes).

`srl` is the time, in seconds, of the slow restart limit. The default value is 10.

`sp` is the time, in seconds, of the stability period. The default value is 300 (5 minutes).

`signal` specifies the preferred UNIX kill signal that you use to stop a server. The default value is 15, which represents SIGTERM.

The default values of the SVM server startup parameters are suitable for most uses. For more information on these parameters, see “Automatic startup at reboot time button” (page 403), “Preferred kill signal menu button” (page 403), and “Restart parameter buttons” (page 403).

Note: The -list, -start, -stop, -delete, and -add options of the svmcmd utility are all mutually exclusive. You cannot combine multiple svmcmd operations in a single command line instance.

The -list, -start, and -stop options all support left-matching of the server name. Left-matching means that when you specify the first few characters of a server name, the operation is performed on all servers whose names begin with those characters.This matching is especially useful for starting and stopping similar servers. For example, if all FMDR servers are prefixed with FMDR, you can start all FMDR servers as a group by specifying a command such as
`-start FMDR`.

Examples

To list all SVM-managed servers, enter

```
/opt/MagellanNMS/bin/svmcmd -list
```

To stop server FMDR_DBNL, enter

```
/opt/MagellanNMS/bin/svmcmd -stop FMDR_DBNL
```

To add server Level 2 MNS and the command with which to start it, enter

```
/opt/MagellanNMS/bin/svmcmd -add "mypswd" "Level 2
MNS" "/opt/MagellanNMS/bin/mnsd 2 localhost barsec5"
```

To delete server Level 2 MNS, enter

```
/opt/MagellanNMS/bin/svmcmd -delete "mypswd" "Level 2
MNS"
```

Chapter 23
Using the GMDR Administration tool

This section describes the GMDR Administration tool and provides instructions for using it. See the following sections for more information:

GMDR Administration tool

The GMDR Administration tool lets you do the following to a General Management Data Router (GMDR) server running on the local workstation or on a remote workstation:

- configure the GMDR server to collect surveillance data from the surveillance servers, and from devices that are not supported by Preside Multiservice Data Manager (MDM), by means of an inbound API. The surveillance servers gather raw surveillance information from nodes in the network.
- monitor connections between the GMDR server and the surveillance servers from which it collects surveillance data
- view and reset a GMDR database that contains statistics gathered by the GMDR server

- view a list of components and subcomponents that are being monitored by a GMDR server
- view logs about changes in the states of connections to the surveillance servers and about database resets
- trigger a state walk to obtain the current states of one or all modules that are managed by an FMDR, or NMDR server

GMDR Administration window

The menus, areas and buttons on the **GMDR Administration** window are described in the following sections.

The window contains the items described in the following sections:

File menu

The **File** menu contains the following command:

- **Exit** closes the GMDR Administration tool and all of its dialogs. You are warned if the GMDR server configuration has been altered, but not saved.

Options menu

The **Options** menu contains the following commands:

- **Connect to another GMDR** opens the **GMDR Servers** dialog and lets you connect to a GMDR server running on any host that is accessible through the LAN.

- **Connect to selected subGMDR** lets you connect to a subordinate GMDR that is selected in the **GMDR Subservers** area.

Security menu

The **Security** menu contains the following commands:

- **Login as admin** displays the **GMDR Admin Login** dialog and lets you to log in as the administrator.
- **Logout from admin** disables access to the restricted administrative functions. This command is enabled if your are logged in as the administrator.
- **Set admin password** opens the **GMDR Admin Password** dialog which lets you to set the GMDR admin password. This command is enabled if you are logged in as the administrator.

Subserver Actions menu

The **Subserver Actions** menu contains the following commands:

- **Resynch selected FMDR with device(s)** or **Resynch selected NMDR with device** opens the **Resynch Request** dialog which allows you to perform a state walk and obtain the states for one or more Passport or MPE 9500 nodes. To make this command active and perform a state walk, you must be logged in as the administrator, have selected the FMDR server for Passport and the NMDR server for MPE 9500 that controls the component(s) on which you wish to perform the state walk. The FMDR or NMDR server must also be in the Connected state.

  Note: Active alarms may be obtained from the node only if the Active Alarm List feature (Passport release PCR 5.1 or higher) is installed and provisioned on the node.

- **Display selected subserver statistics** opens the **Server Statistics** dialog to display various statistical information about a server. To make this command active you must have selected a GMDR, FMDR, NMDR, DMDR, NDAM or IMDR server that is in the Connected state.
- **Reset selected subserver database** opens the **Database Reset** dialog. If you click **OK**, all of the components and alarms in the selected subserver database are removed.

GMDR Subservers area

The **GMDR Subservers** area displays the following information:

- the state of connections between the GMDR server and the surveillance servers from which it collects surveillance data
- the name of the host on which a surveillance server is running
- the date and time at which the server entered its current state
- for subordinate GMDR servers for which a criticality threshold has been set, the current value of the criticality threshold

When you start the GMDR Administration tool for the first time, the **GMDR Subservers** area is empty because no connections have been defined to the surveillance servers. To define them, see "Procedure steps" (page 451).

The state of a connection can be one of the following:

- **Connected** indicates that the GMDR server is connected to the surveillance server. The administrator has manually connected the server, or the connection was established automatically when the GMDR server started.
- **Connecting** indicates that the GMDR server is attempting to connect to the surveillance server. When a connection is dropped, or if the initial connection is unsuccessful, GMDR attempts to connect to the server every 30 seconds until it succeeds, or until you click **h**. If the server remains in the Connecting state for a long time, see "Failed or lost connections" (page 465).
- **Disconnected** indicates that the GMDR server is not connected to the surveillance server. The administrator has manually disconnected the server, the server may never have been connected, or the connection was refused due to an invalid password.

GMDR Database Statistics area

The **GMDR Database Statistics** area displays the following information which is updated automatically once per minute, or whenever you click **Refresh**:

- the date and time at which the GMDR database was last reset
- the number of active alarms

- the alarm arrival rate
- the number of components (modules) and sub-components being surveilled
- the number of links and dial links (DBNL, DNL, BWOD) being surveilled

Statistical information for the connected servers is also available through the **Display selected subserver statistics** command of the **Subserver Actions** menu.

Messages area

The **Messages** area alerts you to server connection state changes and database resets, and provides a reason for each event.

Buttons

The GMDR Administration window contains the following buttons:

- **Connect** connects the GMDR server to the selected server. This button is enabled if the server is in the Disconnected state and you are logged in as the administrator. If the GMDR server is unable to connect, it tries to connect once every 30 seconds until it succeeds, or until you click **Disconnect**.
- **Disconnect** disconnects the GMDR server from the selected server. This button is enabled if the server is in the Connecting or the Connected state and if you are logged in as the administrator. Disconnection is temporary. and is not saved to the configuration file. When you restart the GMDR server, GMDR automatically attempts to reconnect to the disconnected server.
- **Add** opens the **GMDR Add Server** dialog which prompts you for the server's name, host, connection user ID and password. This button is enabled if you are logged in as the administrator.
- **Edit** opens the **GMDR Edit Server** dialog which allows you to modify the selected server's name, host, connection user ID and password. This button is enabled only if the server is in the Disconnected state and you are logged in as the administrator.

- **Remove** deletes the selected server from the GMDR server set of available servers. This button is enabled if the server is in the Disconnected state and you are logged on as the administrator.
- **Refresh** updates the database statistics.
- **Show Components** opens the **GMDR Components** dialog. This dialog lets you view the list of components stored in the database and lets the administrator delete components from the database.
- **Show Clients** opens the **GMDR Clients** dialog. This dialog lets you view the clients that are connected to the GMDR server.
- **Reset Database** opens the **Database Reset** dialog. This dialog lets you reset the GMDR database. This button is enabled if you are logged in as the administrator.
- **Reset Alarm/State** opens the **Reset Alarm/State** dialog. This dialog lets you remove all alarms and reset the state of all components to UNKNOWN. This button is enabled if you are logged in as the administrator and the software you are running is version 13.4 or later.

Dialogs

For information about the dialogs of the GMDR Administration tool, see the following sections:

- "GMDR Admin Login dialog" (page 429)
- "GMDR Admin Password dialog" (page 429)
- "GMDR Add Server and GMDR Edit Server dialogs" (page 430)
- "Find available server dialog" (page 431)
- "GMDR Components dialog" (page 432)
- "Database Reset dialog" (page 433)
- "Reset Alarm/State dialog" (page 434)
- "GMDR Servers dialog" (page 434)
- "GMDR Clients dialog" (page 434)
- "Resynch Request dialog" (page 434)
- "Server Statistics dialog" (page 434)

- “Error, warning, question, and information dialogs” (page 435)

GMDR Admin Login dialog

The GMDR Admin Login dialog lets you log in with a password to perform administrative procedures using the GMDR Administration tool.

When you are logged in, the following items turn black to indicate that they are enabled:

- **Logout from admin** and **Set admin password** commands from the **Security** menu.
- **Connect**, **Disconnect**, **Add**, **Edit**, and **Remove** buttons of the GMDR Servers list. Whether these buttons are active also depends on the state of the server that is selected in the GMDR Server list.
- the **Reset DB** and **Reset Alarm/State** buttons in the GMDR Database Statistics area of the window
- the **Delete** button in the **Components** dialog

GMDR Admin Password dialog

The **GMDR Admin Password** dialog lets you set a new administrator password.

The dialog prompts you for the old admin password. Enter the old password and click **OK**. The dialog then prompts you for the new password. The password is displayed on the screen as a series of asterisks (*). The minimum length of the password is 5 characters and the maximum length is 12.

You are then asked to re-enter the new password. If the new passwords match, the password is updated and the dialog closes. Otherwise, you are again prompted for the new password.

The default password is a null string. Therefore, when you set the password for the first time, just click **OK** when you are prompted for the old password.

Click **Cancel** to abort the password setting operation and close the dialog.

GMDR Add Server and GMDR Edit Server dialogs

The **GMDR Add Server** dialog lets you add a new surveillance server to the GMDR server list. The **GMDR Edit Server** dialog lets you modify the definition for an existing surveillance server. Except for a different dialog title, both dialogs are identical.

The fields in these dialogs are as follows:

- **Server Name** is the name of a surveillance server from which the GMDR server collects surveillance information. This field is mandatory; omitting it opens an error dialog when you click **OK**.
- **Host Name** is the name of the workstation on which the surveillance server is running. This field is mandatory, omitting it opens an error dialog when you click **OK**.
- **Find Available Server** invokes the **Find available server** dialog, which lists the Preside Multiservice Data Manager (MDM) surveillance servers that are available on a host. When you select an entry in the **Find available server** dialog, the selected server name and host are copied into the proceeding two fields. See “Find available server dialog” (page 431).
- **User/Capability Id and Password**
  - For an FMDR or NMDR server, they are the user ID and password for a group of nodes.
  - For a DMDR server, they are the NCS Capability ID and password for an OA group.
  - For DMA and IMDR servers, or a subordinate GMDR server, these fields are not required, and can be left empty.
  - For an NDAM server, these fields are required only if the NDAM server is running in secure mode.
    A userid and password are needed by the GMDR and NDAM servers only if required by the NDAM server running in secure mode.
  - For an SMDR server, the userid is required to identify the GMDR server. The userid is automatically filled in if none is specified.

- **Criticality Threshold** is only enabled if the name of a subordinate GMDR server (GMDR or GMDR_<name>) is entered in the Server Name field. The threshold is the minimum level of criticality a component must have to allow the subordinate GMDR server to report alarm and state change information for that component. The criticality of a component is defined in the GMDR section of 241-6001-310 *Preside MDM Server Reference Guide*, along with the GMDR command line options related to resynchronization and notification.

  Permissible values are from 0 to 255. By default, this field is empty which indicates a criticality threshold of 0. A value of 0 means that alarms and state changes are collected for all components regardless of the criticality assigned to them in the configuration files. When specifying a value for this field, take into account the criticality of the component in the configuration files, and the arrangement of hierarchical GMDR servers in your network.

Click **Cancel** to abort the adding of a new server or the editing of a server, and to close the dialog.

To add or modify a server, see,"Configuring GMDR to access the surveillance servers" (page 450).

Find available server dialog

The **Find available server** dialog lists the servers available on a given host. With this dialog, you can select a Preside Multiservice Data Manager surveillance server for the **GMDR Add Server** and **GMDR Edit Server** dialogs without having to type in its coordinates.

The fields in this dialog are as follows:

- **Surveillance Servers and Host** lists the available servers on a host
- **Selection** displays the current selection. If you type a host name here and click the Find Match button, the list is refreshed to display the available servers on that host.

Either double-click the list entry or click **OK** to close the dialog and transfer the server name and host name to the **Add Server** dialog.

Click Find **Match** to refresh the dialog with the list of available servers on the host identified in the **Selection** field.

Click **Cancel** to close the dialog without selecting a server.

GMDR Components dialog

The **GMDR Components** dialog displays information about the components, subcomponents, and links in the GMDR database from which the GMDR server is collecting surveillance information.

Lists in the dialog are as follows:

- **Components** lists of all of the components and links in the database
- **Subcomponents for** lists the subcomponents for a component or link that is selected in the Components: list

The **Components** list can be populated in the following ways:

- by selecting a component in the **Components** or **Subcomponents** for list
- by entering the component name at the keyboard
- by clicking **Get** Context

Fields in the dialog are as follows:

- **Raw State** displays the current raw state of the selected component or subcomponent, as calculated by the servers that supply information to the GMDR server.
- **Ack State** displays the current alarm acknowledgment state (ACKED or UNACKED) of the selected component or subcomponent, as it is set with the Alarm Acknowledgment tool.
- **Criticality** displays the criticality assigned to the selected component or link in the configuration files. See the GMDR section in 241-6001-310 *Preside MDM Server Reference Guide* for command line options related to resynchronization and notification congestion.

You may use the following upper row of buttons to perform actions on the component displayed in the **Component** field:

- **Find** locates a component in the Components: list and displays its subcomponents in the Subcomponent for list. The lists scroll until the component is visible. A warning dialog appears if the component is not found.
- **Delete** removes a component, all of its subcomponents, and all of its alarms from the GMDR database. The Delete button is enabled if you are logged in as the administrator. The component deletion is propagated down to the connected servers of the GMDR database. Additionally, the component deletion is propagated to clients of GMDR and may be reflected in the network model, depending on the option selected for the SURNUP server (see the Surveillance Network Model Updater section in 241-6001-310 *Preside MDM Server Reference Guide*).
- **Get Context** gets the name of a component or subcomponent that has been put into context while you were working with another Preside Multiservice Data Manager (MDM) tool and displays the name in the **Component** text field. The **Components** list scrolls to the name of the component, and the component name changes color to indicate that it is selected.
- **Put Context** puts the current component in context for use in other MDM tools and applications

You may use the following lower row of buttons to perform actions on the dialog:

- **Close** dismisses the dialog
- **Refresh** updates the dialog with the latest information from the database
- **Help** provides online help on the dialog

Database Reset dialog

The **Database Reset** dialog confirms the removal of all component and alarm information that is stored in the GMDR database.

Resetting the database also reloads the GMDR component criticality configuration as defined in the configuration files, including the overrides file.

Reset Alarm/State dialog

The **Reset Alarm/State** dialog confirms the removal of all alarms and the resetting of all component states to UNKNOWN.

GMDR Servers dialog

The **GMDR Servers** dialog lists the GMDR servers that are running on workstations which belong to the same level 2 MNSD Domain as this workstation, and lets you select a GMDR server on one of these workstations to work on. For an explanation of what a level 2 MNSD Domain is, see "Configuring Multi-nodal Naming Service domains" (page 223).

GMDR Clients dialog

The GMDR Clients dialog lists the clients that are using the services of the GMDR server, and the time at which the connection was established.

Resynch Request dialog

The **Resynch Request** dialog lets you run a state walk to obtain the states for Passport and MPE nodes that are managed by an FMDR and an NMDR server respectively.

> ***Note:*** Active alarms may be obtained from the node only if the Active Alarm List feature (Passport release PCR 5.1 or higher) is installed and provisioned on the node.

To run a state walk on a single module, enter the name of the module in the **Module Name** field, then click **OK**.

To run a state walk on all modules managed by the FMDR or NMDR server, click **OK**.

Click **Cancel** to abort the setting up of the state walk and to close the dialog.

Server Statistics dialog

The **Server Statistics** dialog displays statistical indicators for a server that is selected in the **GMDR Subservers** area. Selecting a connected subordinate GMDR server or an, FMDR, DMDR, or IMDR server in the server list and clicking **Display Server Statistics** on the **Subserver Actions** menu opens the **Server Statistics** dialog.

The dialog consists of a text panel that displays the statistical information and three command buttons to **Refresh** the display, **Cancel** the dialog and call online **Help**.

When you invoke the dialog, it initially displays the "?" character. When data retrieval is completed, any data fields for which no data was received are data filled with the "-" character.

The statistics indicates provided are the

- name and host of the target server
- number of components (modules) and sub-components being surveilled
- number of links and dial links (DBNL, DNL, BWOD) being surveilled (Dial Links are only available for DMDR servers)
- number of active alarms and the alarm arrival rate
- number of stored status records and the status record arrival rate (DMDR servers only)
- Raw State Change Notification arrival rate (IMDR servers only)
- OSI State Change Notification arrival rate (FMDR servers only)

When an indicator does not apply to the target server type or the statistical information is not available, the dialog displays a question mark '?'. For example, FMDR servers do not manipulate Dial Links, so for an FMDR server, the Number of dial links statistics field displays a question mark.

Error, warning, question, and information dialogs

The GMDR Administration tool is equipped with error, warning, question, and information dialogs.

Error dialogs

Error dialogs indicate an error condition. You must respond before you can proceed. Click **OK** to return to the application at the point before the error condition occurred, and fix the error condition before continuing.

Warning dialogs

Warning dialogs indicate the possibility of disrupting service. You must respond before you can proceed. Click **OK** to proceed. Click **Cancel** to return to the application at the point before the dialog was presented.

Question dialogs

The question dialogs ask questions to which you must respond before you can proceed. Click **Yes** to perform the action asked by the question. Click **No** to proceed without performing the requested action.

Information dialogs

The information dialogs convey information of interest. Click **OK** to confirm that you have read the information and to close the dialogs.

Keyboard shortcuts

The GMDR Administration tool provides the following useful shortcut:

- Ctrl + E closes the GMDR tool.

Non-administrative procedures

See the following sections for information on how to perform non-administrative procedures. These procedures can be performed by any user of the GDMR Administration tool:

Navigation

Starting the GMDR Administration tool

Start the GMDR Administration tool from the Preside Multiservice Data Manager main window.

When you start the GMDR Administration tool on a workstation that is deployed in a LAN configuration, the tool attempts to connect to the GMDR server in context, as defined by the Service Selection tool. For information, see "Using the Service Selection tool" (page 467).

On a workstation that is deployed in a stand-alone configuration, the tool connects to the local GMDR server. When the GMDR Administration tool is started, you may use the GMDR Servers dialog to connect to any GMDR server in the network and monitor the server or perform administrative procedures. See “Connecting to a GMDR server running on a remote host” (page 439) for the instructions to do this.

Procedure steps

1 From the application main window, click **System** -> **Administration** -> **GMDR Administration**.

The **GMDR Administration** window opens.

When the window opens for the first time, fields are blank and remain blank until you perform procedure “Configuring GMDR to access the surveillance servers” (page 450).

When the window opens after you have already configured GMDR to access the surveillance data servers, the surveillance servers from which the GMDR server collects its surveillance information appear in the GMDR Servers list.

When you start the tool you only have access to the GMDR non-administrative functions. All of the administrative functions are disabled and grayed out. To enable these functions, you must log in as an administrator, as described in “Logging in as the administrator” (page 448).

Connecting to a GMDR server running on a remote host

Use this procedure to connect the GMDR server that is running on a remote host.

Procedure steps

1. From the **Options** menu, click **Connect to another GMDR**.

   The **GMDR Servers** dialog opens. The dialog lists the GMDR servers on all of the hosts that belong to the same MNSD level 2 Domain as this workstation.

2. Do one of the following:

   - Double click the name of the host in the **Servers** list.
   - Enter a host name in the **Connect to GMDR running on host** field, then click **OK**.
   - Click **Cancel** to close the dialog without connecting to another server.

Connecting to a subordinate GMDR server

Use this procedure to connect the GMDR server to a subordinate GMDR server that is running on a remote host, or that is running on the same host as the superior GMDR server.

Procedure steps

1. In the **GMDR Subservers** area, click on the name of a subordinate GMDR server.

   The row that contains the name of the subordinate GMDR server changes color to indicate that it has been selected.

2. From the **Options** menu, select **Connect to Selected sub GMDR**.

   The state of the server changes to **Connecting**, then to **Connected**.

   If the GMDR server is unable to connect to the subordinate GMDR server, its state remains Connecting and the GMDR server attempts to connect to the subordinate server every 30 seconds, until it succeeds or you click Disconnect. If the state does not change to Connected, see “Failed or lost connections” (page 465).

Viewing the states of connections to the surveillance servers

Look at the fields in the GMDR Servers list in the **GMDR Administration** window.

For a list and description of the states for the connections to the surveillance servers, see “GMDR Subservers area” (page 426).

For the instructions to troubleshoot lost or failed connections to a surveillance server, see “Failed or lost connections” (page 465).

Refreshing the database statistics

The statistics displayed in the **GMDR Database Statistics** area of the window are updated automatically once a minute. Click **Refresh** to update the statistics immediately.

Viewing non-GMDR server statistics

Use this procedure to display statistics information for a non-GMDR server that provides data to GMDR.

Procedure steps

1. Scroll down the servers list until you find the name of the FMDR, IMDR, or DMDR server you wish to get information about.
2. Click on the name of the server to select it.
3. From the **Subserver Actions** menu, click **Display selected subserver statistics**.

   The **Server Statistics** dialog opens.

Viewing a list of modules and their components

Use this procedure to view a list of the links, components, and subcomponents that are stored in the GMDR database and their current state and criticality values.

Procedure steps

1. In the **GMDR Administratio**n window, click **Show Components**.

   The **GMDR Components** dialog opens. The **Components** section displays a list of all components and links known to the database.

2. In the **Components** list, click on the name of a component.

   The **Subcomponents** list displays the subcomponents for the selected component. The subcomponent list's title is updated with the name of the selected component. Both lists are sorted alphabetically.

   The **Raw State** and **Acked State** fields display the current states for the selected component and the **Criticality** field displays the **Criticality** value assigned to the component in the configuration files.

3. In the **Subcomponents** list, click on the name of the subcomponent.

   The **Raw State** and **Acked State** fields display the current states for the selected subcomponent and the **Criticality** field displays the **Criticality** value assigned to the subcomponent in the configuration files.

Viewing a list of surveillance servers connected to GMDR

Use this procedure to view a list of the GMDR clients.

Procedure steps

1. Click **Show Clients**.

   The **GMDR Clients** dialog opens. The dialog contains a list of the surveillance servers that are connected to the GMDR server, the host names of the workstation on which the surveillance servers are running, and the time and date at which they were connected.

Finding a component in the Components dialog

Use this procedure to find a component in the **Components** dialog without having to scroll through the **Components** list.

Procedure steps

1. Click **Show Components** in the GMDR Administration window.

   The **GMDR Components** dialog opens.

2. Enter the component name in the **Component** text field using any of the following methods:

   - Enter the component name from the keyboard
   - Select a component in the **Components** or **Subcomponents** list.
   - Click **Get Context** to get the component last put in context using the GMDR Administration tool or another tool.

3. Click **Find**.

   The lists scroll until the component and its subcomponents are visible. The subcomponent changes color to indicate that it is selected. A warning dialog is displayed if the component cannot be found.

Putting a component into context in the Components dialog

Use this procedure to put a component into context in the **Components** dialog of the GMDR Administration tool.

Putting a component into context is useful if you wish to work on the same component in another Preside Multiservice Data Manager tool, without having to retype the name of the component. For example, if you have selected a component in the Components dialog and wish to look at its alarm history with the Component Information Viewer (CIV), you can put a component you have selected in the Components list into context by clicking Put Context. When you start the CIV, the window automatically displays information about the component you put into context.

Procedure steps

1. Click **Show Components** in the **GMDR Administration** window.

   The **GMDR Components** dialog opens.

2. In the **Components** list, click on the name of a component that you wish to put into context.

3. Click **Put Context**.

Getting a component context in the Components dialog

Use this procedure to get the name of a component that has been put into context from another Preside Multiservice Data Manager tool and display its subcomponents in the **Components** dialog of the GMDR Administration tool.

Putting a component into context is useful if you wish to work on the same component in another tool, without having to retype the name of the component. For example, if you are looking at a component in the Component Information Viewer (CIV) and you wish to list its subcomponents in the **Components** dialog of the GMDR Administration tool, click **Get Context** in the **Components** dialog and the name of the component that was put into context in CIV appears in the **Component** field.

Procedure steps

1 Click **Show Components** in the **GMDR Administration** window.

The **GMDR Components** dialog opens.

2 Click **Get Context**.

The name of the component that you put into context in another tool appears in the **Component** text field, and the **Components** list scrolls to the component that is in context. The component name changes color to indicate that the component is selected.

Viewing a list of the surveillance servers connected to GMDR

Use this procedure to view a list of surveillance servers connected to GMDR.

Procedure steps

1 Click **Show Clients**.

The **GMDR Clients** dialog opens and displays a list of the surveillance servers that are connected to the GMDR server, the host names of the workstations on which the surveillance servers are running, and the time and date at which they were connected.

Closing the GMDR Administration tool

Use this procedure to close the GMDR Aministration tool.

Procedure steps

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

All windows close. A warning is displayed if the GMDR server configuration has been altered, but not saved. You can also use the shortcut Ctrl + E to close the GMDR Administration tool.

Administrative procedures

To perform the administrative procedures you must log in to the GMDR Administration tool as the administrator. When you access GMDR for the first time, no password is defined. A password must be set to limit future access to the GMDR administrative functions. The administrator can change the password by selecting **Set admin password** from the **Security** menu.

If you forget the administrator password, see "Forgotten password" (page 464).

Navigation

Setting up an administrator password

Use this procedure to set up an administrator password when no administrator password has been set. This is required when the GMDR Administration tool is started for the first time.

Procedure steps

1. From the **Security** menu, click **Login as admin**.

   The **GMDR Admin Login** dialog opens.

2. Click **OK**. Do not enter anything in the Password field.

   The Admin Login dialog closes.

3. From the **Security** menu select **Set admin password**.

   The **GMDR Admin Login** dialog reopens. The dialog prompts for the old admin password.

4. Click **OK**. Do not enter anything in the **Old password** field.

   The dialog prompts for a new password.

5. Enter the new password and re-enter it when prompted. The password must have a minimum of 5 characters and a maximum of 12.

   The password is displayed on the screen as a series of characters.

   If the passwords match, the password is updated and the dialog closes. Otherwise, you are prompted for the new password again.

   Click **Cancel** to abort setting up the new password and to close the dialog.

Logging in as the administrator

Use this procedure to log in as the administrator. Only one person can log in as the administrator at a time.

Procedure steps

1. From the **Security** menu, select **Login as admin**.

   The **GMDR Admin Login** dialog opens.

2. In the **Password** field, type the admin password and click **OK**.

   - If you enter the correct password, the administrative functions are enabled. Otherwise, the message `Invalid password` appears. After three invalid attempts, the dialog closes.
   - If an administrator is already logged in, the **GMDR Admin Login** dialog closes and a warning message appears.
   - If you forget what the password is, see “Forgotten password” (page 464).
   - Click **Cancel** to abort the login and close the dialog.

Changing the administrator password

Use this procedure to change administrator password.

Note: Only one person can be logged in as the administrator at a time.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. From the **Security** menu, click **Set admin password**.

   The **GMDR Admin Password** dialog opens.
3. In the **Password** field, type the old password and click **OK**.
4. At the prompt, enter the new password. Re-enter the password when prompted. The password must be between five and 12 characters long.

   The password is displayed on the screen as a series of characters.

   If the new passwords match, the password is updated and the dialog closes. Otherwise, you are prompted for the new password again.

   Click **Cancel** to abort the password change operation and close the dialog.

Connecting to a surveillance server

Use this procedure to connect to a surveillance server.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. In the list of servers, click on the name of the surveillance server you wish to connect.

   The server state changes to Connecting while the GMDR attempts to connect to the surveillance server. GMDR attempts to reconnect to a server once every 30 seconds until it is successful, or until you halt connection attempts by clicking Disconnect. The state changes to Connected once the connection is established.

   If the state does not change to Connected, see “Failed or lost connections” (page 465).

Disconnecting from a surveillance server

Use this procedure to disconnect from a surveillance server.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. In the list of servers, click on the name of the surveillance server to disconnect, then click **Disconnect**.

   The server’s state changes to Disconnected.

   Note: Disconnecting is temporary. The disconnection is not saved to the configuration file. When you restart the GMDR server, GMDR attempts to reconnect to the disconnected server.

Configuring GMDR to access the surveillance servers

Use this procedure to configure GMDR to collect surveillance information from the surveillance servers.

Before configuring the GMDR servers with this tool, the FMDR, NMDR, DMDR, DMASERVER, IMDR, NDAM, SMDR, and subordinate GMDR servers from which the GMDR server receives surveillance data must be configured and running. For information about these servers, see the following sections in server sections in 241-6001-310 *Preside MDM Server Reference Guide*:

- FMIP Management Data Router (FMDR)
- MPE 9500 Management Data Router (NMDR)
- DPN Management Data Router (DMDR)
- Data Manager Agent (DMA)
- Injected Management Data Router (IMDR)
- Network Data Access Mediator (NDAM)
- SNMP Management Data Router (SMDR)
- General Management Data Router (GMDR)

See the following sections in this document for information about the servers:

- “Configuring network access data mediation” (page 211)

- "Configuring servers for DPN switches" (page 93)
- "Configuring MDM servers for Passport switches" (page 123)

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See "Logging in as the administrator" (page 448).
2. Click **Add**.

   The **GMDR Add Server** dialog opens.
3. Click Find Available Server.

   The **Find available server** dialog opens.

   In the dialog, you can do one of the following:

   - Type in the name of a remote host in the **Selection** field. Click **Find Match** to display a list of servers that are available on that host. If you double-click a server entry in the list or select it and click **OK**, the dialog closes and the selected server's name and host are filled in the **GMDR Add Server** dialog.
   - Enter the server name in the **Server Name** field of the GMDR Add Server dialog using one of the following syntaxes:

   For an FMDR server providing surveillance data from Passport nodes, use

   FMDR_<group_name>

   For an NMDR server providing surveillance data from MPE 9500 nodes, use

   NMDR_<group_name>

   For a DMDR server providing surveillance data from DPN devices, use the following:

   DMDR_<group_name>

   For an IMDR server that accepts surveillance data injected from an inbound alarm API/EPI client or a DMA server (workstation surveillance) use one of the following:

   IMDR
   IMDR_<suffix>

   For an NDAM server providing component type and regional filtering, use

NDAM

or whatever service name has been specified on its command line.

For an SMDR server that collects fault management data from the SNMP Surveillance Adapter, use the following:

SMDR
SMDR_<suffix>

For a subordinate GMDR server that is to run on this workstation along with a superior GMDR server, use the following:

GMDR_<name>

For a subordinate GMDR server that is to run on a remote workstation, use one of the following:

GMDR
GMDR_<name>

For a DMA server that is to provide Global Alarm Clearing for DPN, use the following:

DMASERVER

where:

<group_name>

is the name of the group from which the server gathers surveillance information. For DPN switches, this is the name of the OA group from which a DMDR server gathers surveillance information, for Passport groups, this is the name of the group from which an FMDR server gathers surveillance information, and MPE groups, this is the name of the group from which an GMDR server gathers surveillance information.

For a description of DMDR, FMDR, and NMDR servers, see 241-6001-310 *Preside MDM Server Reference Guide*.

<name>

identifies the server's purpose and distinguishes it from the superior GMDR server on this workstation. For example, GMDR_East. For an explanation of what a subordinate server is and recommended naming conventions, see the GMDR section in 241-6001-310 *Preside MDM Server Reference Guide*.

Note: Specifying GMDR or GMDR_<name> to identify a subordinate GMDR server enables the Criticality field.

<suffix>

specifies a suffix to be added to the SMDR or IMDR server name. This option is required to uniquely identify an SMDR or IMDR server when more than one server of the same type is running on the same workstation. When this option is specified, the server name becomes SMDR or IMDR followed by an underscore, followed by the suffix. For example, SMDR_EAST.

4 Enter the host name or IP address of the workstation on which the server is running in the Host name field. This field is mandatory.

5 Enter the user ID and password, if required, as described in the following list:

- Enter the user ID for FMDR, NMDR, and DMDR servers.
- Leave the userid field empty for IMDR and DMA servers.
- For NDAM and GMDR servers, the userid field is optional.
- For an SMDR server, the userid field is optional, however, it is filled in as GMDR if one is not specified.

6 Enter the password for the server in the **Password** field, as follows:

For an FMDR or NMDR server, enter a valid password for the respective FMDR or NMDR group.

For a DMDR server, enter a valid password for the DMDR group. This password must already be set up in the NCS so that it is available on all OAs in the group.

For SMDR and IMDR servers, no password is required.

For a subordinate GMDR server, the password is usually not required. A password is required if NDAM is named as a GMDR server.

For NDAM, enter a password if NDAM is secure and enabled.

For a DMA server to provide global alarm clearing for DPN, leave the password field blank.

7 If the server is a subordinate GMDR or NDAM server and you wish to set a criticality threshold, specify the appropriate value in the Criticality Threshold field. You can only do this if the subordinate GMDR server was set up with10.6 or later software. If the subordinate GMDR was set up with 10.5 or lower software, you cannot set a threshold; leave this field empty.

See “GMDR Add Server and GMDR Edit Server dialogs” (page 430).

8 Click **OK** to add the server, and to save the changes.

The server appears in the servers list window.

Note: Click Cancel to close the dialog without adding a server.

9 Repeat step 2 through step 8 to add all of the DMDR, FMDR, NMDR, IMDR, SMDR, DMA, and subordinate GMDR servers that are to supply surveillance data to the superior GMDR server on this workstation.

10 Open a connection to each server by clicking on each server in the GMDR servers list and clicking **Connect**.

The server state changes to **Connecting** while GMDR attempts to connect to the server. GMDR attempts to reconnect to a server once every 30 seconds until it is successful, or until the user halts connection attempts by clicking **Disconnect**. The state changes to **Connected** once the connection is established.

If the state does not change to **Connected**, see “Failed or lost connections” (page 465).

Changing the GMDR configuration

You can change the GMDR configuration by adding new servers, disconnecting servers, editing a server's definition, or removing a server from the list of GMDR servers.

This section contains the procedures to disconnect a server, edit a server's definition, and to remove a server from the list of GMDR servers. For the instructions to add a new server, use procedure "Procedure steps" (page 451).

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See "Logging in as the administrator" (page 448).
2. In the GMDR servers list, click on the name of the surveillance server you wish to edit, then click **Disconnect**.

   The state of the server changes to **Disconnected**.
3. Click **Edit**.

   The **GMDR Edit Server** dialog opens, which is identical to the **GMDR Add Server** dialog.
4. Make the changes to the fields in the dialog. For a description of the fields in the dialog, see "GMDR Add Server and GMDR Edit Server dialogs" (page 430).
5. Click **OK** to confirm and save the changes, or click **Cancel** to close the dialog without changing the server definition.
6. Click **Connect** to reopen the connection with the new parameters.

Removing a server from the list of GMDR servers

Use this procedure to remove a GMDR server.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. In the GMDR servers list, click on the name of the surveillance server you wish to delete, then click **Disconnect**.

   The state of the server changes to **Disconnected**.
3. Click **Remove**.

   The server is deleted from the list of GMDR servers.

   Note: The changes are saved when you click **Remove**.

Triggering a resynchronization

Use this procedure to trigger two resynchronizations to obtain the states and alarms of Passport and MPE 9500 nodes that are being managed by an FMDR or NMDR server. You can only trigger a resynchronization if one is not already in progress.

> ***Note:*** Active alarms may be obtained from the node only if the Active Alarm List feature (Passport release PCR 5.1 or higher) is installed and provisioned on the node.

You may wish to trigger a resynchronization when the proxy alarms produced by the FMDR or the NMDR server get out of date. This condiiton may cause lost state change notifications.

There are two ways to trigger a state walk:

- manually at any time from the GMDR Administration tool. See the procedure in this section.
- automatically at the same time of day by setting up parameters in a configuration file. For information about how to configure file FMDRStateWalk_<group>.cfg or file NMDRStateWalk_<group>.cfg, see 241-6001-310 *Preside MDM Server Reference Guide*.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. Scroll down the servers list until you find the name of the server that manages the modules on which you wish to perform a state walk.
3. Click on the name of the server to select it.

   Note: To find the name of the modules that are managed by the FMDR or NMDR server, look at file /opt/MagellanNMS/cfg/HGDS.cfg.
4. Look in the GMDR server list to see if the state of the server is **Connected**. If it is not in the **Connected** state, you cannot perform a state walk. Connect it first.
5. From the **Subserver Actions** menu, select **Resynch selected ... with device(s)**.

   The **Resynch request** dialog opens.

6 Type the name of the module in the **Module Name** field, if you are performing a state walk for a single module. If you are performing a state walk for all modules, leave this field blank.

7 Click **OK**.

The software performs a state walk to obtain the latest component states.

Note: Active alarms may be obtained from the Passport node only if the Active Alarm List feature (Passport release PCR 5.1 or higher) is installed and provisioned on the node.

Resetting the state and alarm information in a GMDR database

Use this procedure to reset state and alarm information that is out of sync with the subservers. Information can become out of sync when:

- a workstation is rebooted,
- a subserver is reset, or
- a subserver is disconnected.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. Click **Reset Alarm/State.**

   The **Reset Alarm/State** dialog opens.
3. Click **OK**.

   All alarms are deleted from the GMDR database.

   All components are set to a state of UNKNOWN.

   The alarm and state information is repopulated from all connected subservers.

Resetting the GMDR database

Use this procedure to reset the GMDR database when information about components stored in the database becomes obsolete. This can occur when:

- components have been renamed
- the customer IDs for components have been changed so that the components can no longer be accessed by the GMDR server

The administrator can manually delete each component one at a time, or reset the entire database.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. Click **Reset DB**.

   The **Database Reset** dialog opens.
3. Click **OK**.

   All component, alarm and statistical information is deleted from the GMDR database.

   The GMDR database is repopulated by the connected subservers.

Deleting a component from the GMDR database

Use this procedure to delete a component from the GMDR database.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. Click **Show Components**.

   The **GMDR Components** dialog opens.
3. Enter the component name in the **Component** field using one of the following methods:

   - by entering the component name from the keyboard
   - by selecting a component in the Modules or Components for: list
   - by clicking **Get Context** to populate the field with the component that is currently in context
4. Click **Delete**.

   A warning dialog opens.
5. Click **OK**.
6. Click **Refresh**.

   The selected component as well as all of its subcomponents and alarms are deleted from the GMDR database and may be reflected in the network model depending on the SURNUP option selected.

   The display in the GMDR Components dialog reflects the deletion of the component.

Resetting the database for networks containing nodes of only one type

Use this procedure to reset a database that contains only one type of node.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. Click **Reset DB**.

   A warning dialog opens.
3. Click **OK** to reset the database.
4. Click **Cancel** to close the dialog without resetting the database.
5. Start the Server Administration tool and use it to stop and restart all FMDR servers for Passport, NMDR servers for MPE 9500, and DMDR servers for DPN on this workstation. For the instructions to stop and restart a server, see “Logging out as administrator and accessing view mode” (page 379).

Resetting a database

Use this procedure to delete a database when you want to repopulate it.

Procedure steps

1. Log on to the GMDR Administration tool as the administrator. See “Logging in as the administrator” (page 448).
2. Click on the server name in the **GMDR Subservers** area.
3. On the **Subserver Actions** menu, click **Reset selected subserver database**.

   A warning dialog displays.
4. Click **OK**.

   All component, alarm and statistical information is deleted from the database. Note the following:

   - FMDR database repopulates from state walks on all connected modules
   - NMDR database repopulates from state walks on all connected modules
   - DMDR database repopulates when OAs reconnect.
   - IMDR database does not automatically repopulate.
   - For the SMDR database, all component information is deleted from connected DCD servers and the seed files of all connected DCDs are recreated.

Resetting all of the databases in a fault stack

Use this procedure to reset all of the databases in a fault stack.

Procedure steps

1. Identify device-specific servers in the fault stack.
2. Reset each device-specific server using the applicable procedure.
3. Reset all GMDR servers starting at the bottom of the stack.

   All component, alarm and statistical information is deleted from the fault stack.

   The fault stack is repopulated with the results of:

   - restarted discovery from the recreated seed files of SNMP devices,
   - state walks for Passport devices,
   - resynchronization for DPN devices, and
   - custom resynchronization of injected management data through IMDR, where applicable.

Logging out as the administrator

Use this procedure to log out as the administrator and to disable the administrative functions of the GMDR Administration tool.

Procedure steps

1. From the **Security** menu, select **Logout from admin**.

Forgotten password

Use this procedure to reset the administrator password.

Prerequisites

You must be logged in as root.

Procedure steps

1. Delete file opt/Magellan/cfg/private/GMDR.passwd.
2. Set a new password using procedure **“Changing the administrator password” (page 449)**.

Failed or lost connections

If the connection to a surveillance server is lost while the GMDR Administration tool is running, all dialogs close and a warning dialog opens. All tool functionality is disabled, with the exception of the remote host connection capability and the tool exit capability. The GMDR server attempts to re-connect to the server every 30 seconds unless you click Disconnect. Upon reconnection, you must log in again as administrator.

If the GMDR server in context is changed by the Service Selection tool while the GMDR Administration tool is running, a warning dialog opens and you are asked if you want to connect to the new GMDR server.

If the initial attempt to connect to a surveillance server fails, a warning dialog opens, and the state of the server stays at Connecting. All tool functionality is disabled, with the exception of the remote host connection capability and the tool exit capability. The GMDR server attempts to connect to the server every 30 seconds unless you click Disconnect.

Procedure steps

1 Use the Server Administration tool to determine if the surveillance server is running.

- If the surveillance server is not running, start it with the Server Administration tool, then use the GMDR Administration tool to reconnect to the surveillance server.
- If the surveillance server is running, click **Disconnect** in the GMDR Administration window, click **Edit**, then examine the information in the **GMDR Edit Server** dialog, especially the **User/Capability ID** and **Password** fields.

For a description of what should be entered in these fields, see “GMDR Add Server and GMDR Edit Server dialogs” (page 430).

Chapter 24
Using the Service Selection tool

Service selection is used when Preside Multiservice Data Manager (MDM) workstations, interconnected by a LAN, are deployed as Server Sets and Client Sets. It is used to define which workstation is to be used to run the set of servers for selected MDM applications such as Surveillance and Network Model.

The Server Sets - Clients Sets deployment has several advantages:

- use of less-powerful workstations as Client Set workstations, and more-powerful workstations as Server Set workstations.
- specialized network management by creating a number of Server Set workstations responsible for different functions such as: surveillance and support of the Network Model.
- regionalized network management by creating a number of Server Set workstations that are responsible for different regions of the network.
- redundancy by using workstations as redundant Server Set workstations. A user can select a redundant Server Set workstation if the main Server Set workstation fails, or if tool response is poor when using the main Server Set workstation.

See “Sample Server Set/Client Set configuration for a large network” (page 497).

Navigation

- “Tool fundamentals” (page 468)

- "Service Selection - System Wide user interface" (page 472)
- "Service Selection - User Specific user interface" (page 476)
- "Service Selection - System Wide procedures" (page 482)
- "Service Selection User - Specific procedures" (page 488)
- "Troubleshooting procedures" (page 495)
- "Sample Server Set/Client Set configuration for a large network" (page 497)

Tool fundamentals

The Service Selection tool enables the selection of the workstations to be used as server hosts for specific Preside Multiservice Data Manager (MDM) service categories. See "Server sets for each service category" (page 468).

Table 8
Server sets for each service category

Category	Server sets
Surveillance	GMDR, GMDR Agent, RTAC Agent, VPN Monitor server
Network Model	Network Model server, Network Model Edit server, Network Model Agent
DPN Provisioning	DPN PM File Access Server, DPN PM File Access Software Download
DPN Network Access	DPN NCS Communications Manager
Network Access	Passport Communications Manager, MPE Communications Manager, Shelf View Agent, Data Viewer Agent
Provisioning	Configuration Manager, Data Synchronization server

In addition, the Service Selection tool enables the selection of the workstations to be used as server hosts for the on-product help provided with the MDM software.The software provides default values for the service selection host workstations. See "MDM default service selection settings" (page 469).

Table 9
MDM default service selection settings

Services	Toolset environment	Operator Client environment
Surveillance	local host name	admin server name
Network Model	local host name	admin server name
DPN Network Access (not supported at the Operator Client workstation)	local host name	admin server name
DPN Provisioning (not supported at the Operator Client workstation)	local host name	admin server name
Network Access	local host name	admin server name
Provisioning	local host name	admin server name
Help Server Host	local host name	admin server name
Help Server Port	8081	8081

Changing service selection settings

You may want to change the service selection settings for the following reasons:

- access to a service provided through the Server Set workstation fails for any or all of the following reasons:
  - — the servers that are required to support the service stop running
  - — the workstation is rebooted or fails
  - — the servers on the workstations on the LAN are configured in such a way that the data required to support a service that the user wishes to select is not available on the workstation you have selected
- response time using a Preside Multiservice Data Manager (MDM) tool increases to unacceptable levels. For example, because of high traffic to the network through a workstation.

The software default service selection settings can be changed at the system wide level and at the user specific level.

In the Toolset environment:

- System wide changes affect the software default service selection settings for the server host workstation. These changes are persistent but can be overridden temporarily for a specific user session.
- User-specific changes affect the server host workstation for the duration of the user session. The user session is delimited by the duration of time that the MDM context server is active at that workstation.The changes override the MDM software default service selection settings and the system wide changes to these defaults.

In the Operator Client environment:

- System wide changes in the Operator Client environment can only be performed through the Toolset. The Toolset must be launched by a root user at the administration server workstation. The changes affect the MDM software default service selection settings for all the Operator Client desktop sessions using this workstation as their administration server.
- User specific changes in the Operator Client environment affect the Operator Client desktop user session. The changes override the MDM software default service selection settings and the system wide changes to these defaults.

Access to Service Selection GUIs

A user can access the Service Selection- System Wide and Service Selection - System Wide for Operator Client user interfaces only from the Preside Multiservice Data Manager (MDM) Toolset, as follows:

- To change the default service selection settings for the MDM Toolset environment, launch the Toolset. Select System-> Administration -> Service Selection - System Wide. No login to Service Selection is required unless the Administrator has configured password access. See “Login dialog” (page 479).
- To change the default service selection settings for the Operator Client environment, you must launch the Toolset as a root user. From the Toolset, select System -> Administration -> Service Selection - System Wide for Operator Client. No login to Service Selection is required.

A user can access the Service Selection - User Specific user interface from the Toolset at the MDM local host workstation and from the Operator Client desktop, as follows:

- To override the existing service selection settings for the local host workstation, launch the Toolset and select System -> Administration -> Service Selection - User Specific. No login to Service Selection is required.
- To override the existing service selection settings for an Operator Client workstation, launch the Operator Client desktop and in the System menu, select Administration -> Service Selection - User Specific. The Service Selection - User Specific main window opens. No login to Service Selection is required.

Service Selection - System Wide user interface

The Service Selection - System Wide user interface is identical for the Preside Multiservice Data Manager (MDM) Toolset and the Operator Client environments. The main window consists of a menu bar at the top of the window, a status bar at the bottom, and two tabbed panes: MDM Services and Help Service.

Menu bar

The menu bar is at the top of the main window. It contains File and Help menus that are identical in the System Wide and User Specific graphical user interfaces (GUI). The System Wide GUI contains an additional Security menu:

File

The File menu contains two items:

- **Refresh**
  - — Select this item to update the currents selections data in the MDM Services and Help Service panels.
- **Exit**
  - — Select this item to close the Service Selection user interface.

Security

The Security menu is present only in the System Wide GUI for the Toolset environment. It contains one item:

- **Change Password**

— Select this item to launch the Password Change dialog to set up or change the administrator password for the Service Selection tool

Help

The Help menu contains two items:

- **Help on Context**
  - — Select this item to launch the Help on Context feature that enables you to access information about any field in the window.
- **Help on Window**
  - — Select this item to open the information that describes all fields in the window.

Status bar

The Status bar is located at the bottom of the System Wide and User Specific windows. It changes to show the status of the tool in response to your actions in windows and dialogs.

MDM Services tabbed pane

Select the MDM Services tabbed pane to view and modify the current service selections. The MDM Services pane consists of two panels:

- “Current Selections panel” (page 473)
- “Change Selections panel” (page 474)

Current Selections panel

The Current Selection panel lists the current service selection for the Preside Multiservice Data Manager (MDM) services with their respective server hosts. The values are the system administrator customized values or they are the MDM software defaults. See “MDM default service selection settings” (page 469).

The bottom of the Current Selection panel contains one command button:

- **Show Server Status**
  - — Click on this button to launch the Server Status for Current Selections dialog box.

ATTENTION	Showing the server status requires that the MDM mnsdagent process is running on all the hosts.

Change Selections panel

Use the Change Selections panel to change the service selection for Preside Multiservice Data Manager (MDM) services. There are two fields and two command button:

- **Server Host** field
  - — Enter the server host name or the IP address in the Server Host field.
- **MDM Service** field
  - — Select 'All' or one of the six service areas.
- **Show Service** button
  - — Optionally, click this button before you click the Set Service button to display the Server Status on <target host> dialog to see which of the servers are running.

ATTENTION	Showing the server status requires that the MDM mnsdagent process is running on all the target hosts.

- **Set Service** button
  - — Click this button once you have entered the Server Host and MDM Service fields. The data in the MDM Services Selection table and the Server Status for Current Selections dialog are updated with the modifications you entered.

Help Service tabbed pane

Select the Help Service tabbed pane to view and modify the current service selections for the Preside Multiservice Data Manager on-product help information. The Help Service pane consists of two panels:

- "Current Selections panel" (page 475)
- "Change Selections panel" (page 475)

Current Selections panel

The Current Selections panel lists the server host and port for the Preside Multiservice Data Manager (MDM) on-product help information with system values for the host and port.

The system values come from the administrator customized values or from the MDM software defaults. See “MDM default service selection settings” (page 469).

Change Selections panel

Use the Change Selections panel to set the service selection for Preside Multiservice Data Manager (MDM) services. There are two fields:

- **Server Host** field
  - — Enter the server host name or the IP address in the Server Host field.
- **Server Port** field
  - — Enter the server port number in the Server Port field.
- **Set Service** button
  - — Click this button once you have entered the Server Host and Server Port fields. The data in the MDM Help Service table is updated with the modifications you entered.

Service Selection - User Specific user interface

The Service Selection - User Specific main window consists of a menu bar at the top of the window, a status bar at the bottom, and two tabbed panes: MDM Services and Help Service.

- "Menu bar" (page 472)
- "Status bar" (page 473)
- "MDM Services tabbed pane" (page 476)
- "Help Service tabbed pane" (page 478)

MDM Services tabbed pane

Select the MDM Services tabbed pane to view and modify the current service selections. The MDM Services pane consists of two panels:

- "Current Selections panel" (page 476)
- "Change Selections panel" (page 477)

Current Selections panel

The Current Selection panel lists the system settings for all the Preside Multiservice Data Manager (MDM) services with the User Override and System Defaults values for each server.

The User Override column shows the settings that override the system wide settings. A blank cell in this column means the user has not overridden the system wide settings.

The System Default column is read-only and the values come from the administrator customized values or from the MDM software defaults. See "MDM default service selection settings" (page 469).

The bottom of the Current Selection panel contains two command buttons:

- **Show Server Status**
  - — Click on this button to launch the Server Status for Current Selections dialog box. If a service is not overridden by the operator, the server status of its corresponding System Default host is shown.
- **Unset User Override**

— Select one or more service in the MDM Service Column and click on this button to clear the user specific service selection. The cells in the User Override column will blank. The Server Status for Current Selections dialog is updated with the change.

Change Selections panel

Use the Change Selections panel to change the service selection for Preside Multiservice Data Manager (MDM) services. There are two fields and two command button:

- **Server Host** field
  - — Enter the server host name or the IP address in the Server Host field.
- **MDM Service** field
  - — Select 'All' or one of the six service areas.
- **Show Service** button
  - — Optionally, click this button before you click the Set Service button to display the Server Status on <target host> dialog to see which of the servers are running.

ATTENTION	Showing the server status requires that the MDM mnsdagent process is running on the target host.

- **Set Service** button
  - — Click this button once you have entered the Server Host and MDM Service fields. The data in the MDM Services Selection table and the Server Status for Current Selections dialog are updated with the modifications you entered.

ATTENTION	If you are in the Operator Client environment, the Set Service button is disabled.

Help Service tabbed pane

Select the Help Service tabbed pane to view and modify the current service selections for the Preside Multiservice Data Manager (MDM) on-product help information. The Help Service pane consists of two panels:

- "Current Selections panel" (page 478)
- "Change Selections panel" (page 478)

Current Selections panel

The Current Selection panel lists the servers for the Help service server host and server port with User Override and System Defaults values for the host and port.

The User Override column shows the operators's own settings. A blank cell in this column means the operator has not overridden the administrator's system default.

The System Default column is read-only and the values come from the administrator-customized values or from the Preside Multiservice Data Manager (MDM) software defaults. See "MDM default service selection settings" (page 469).

The bottom of the Current Selection panel contains one command button:

- U**nset User Override**
  - — Click on this button to unset the Help service. The cells in this column will blank.

Change Selections panel

Use the Change Selections panel to set the service selection for Preside Multiservice Data Manager (MDM) services. There are two fields:

- **Server Host** field
  - — Enter the server host name or the IP address in the Server Host field.
- **Server Port** field
  - — Enter the server port number in the Server Port field.
- **Set Service** button

— Click this button once you have entered the Server Host and Server Port fields. The data in the MDM Help Service table is updated with the modifications you entered.

Dialogs

ATTENTION	The hosts in the Server Status dialogs do not auto refresh. You must use the Refresh command button to update the current status.

For information about the dialogs of the Service Selection tool, see the following sections:

- "Login dialog" (page 479)
- "Change Password dialog" (page 479)
- "Server Status for Current selections dialog" (page 480)
- "Server Status on <target host> dialog" (page 480)

Login dialog

The login dialog displays only when Service Selection - System Wide is launched from the Toolset.

If password access has not be configured for the workstation, no password is required. Just click OK to close the dialog.

If password access has been configured for the workstation, you must login with the appropriate password and click OK. If the password entered is incorrect or invalid, login fails and you must try again. When you enter the correct password, the login dialog disappears and the main window opens.

You can click 'Cancel' at any time before you click OK to cancel the login and exit the tool.

Change Password dialog

The **Change Password** dialog lets the Administrator set a password if none exists, or change an existing password. Setting a password is optional.

If the **Current password** field is enabled, you need to enter the current password in that field.

You also need to enter a new password in the **New Password** and **Confirm New Password** fields. The password is masked as you type it. Once you have entered the password in both fields, click **OK** to register the password change or click **Cancel** to close the **Change Password** dialog without registering the new password.

Server Status for Current selections dialog

The Server Status for Current Selections dialog consists of four columns:

- Category - the Preside Multiservice Data Manager service category
- Host - the server host
- Server - the server name
- Status - the server status

You can sort on any column by clicking the column heading.

There are three command buttons at the bottom of the dialog:

- **Close**
  - — Click this button to close the dialog.
- **Refresh**
  - — Click this button to update the Status column.
- **Help**
  - — Click this button to launch context help for this dialog.

Server Status on <target host> dialog

The Server Status on <target host> dialog consists of three columns:

- Category - the Preside Multiservice Data Manager service category
- Server - the server name
- Status - the server status

You can sort on any column by clicking the column heading.

There are three command buttons at the bottom of the dialog:

- **Close**
  - Click this button to close the dialog.
- **Refresh**
  - Click this button to update the Status column.
- **Help**
  - Click this button to launch context help for this dialog.

Service Selection - System Wide procedures

Use Service Selection - System Wide to change the service selections for all the users at the client workstations.

Changes to the system wide settings affect all client workstations and are preserved over a restart. Users can temporarily override these settings.

Navigation

Prerequisites to using Service Selection - System Wide

- On the workstation on which you wish to run the Service Selection tool, ensure that file /etc/hosts contains the host names of all workstations in the domain, as described in "Configuring Multi-nodal Naming Service domains" (page 223).

Setting up an administrator password

Use this procedure to set up or change the administrator password. Using an administrator password is applicable only to changing the system wide service selections for the Preside Multiservice Data Manager (MDM) Toolset environment.

ATTENTION	If you do not set up the administrator password, any user will be able to access and use Service Selection - System Wide for the MDM Toolset environment.

Prerequisites

- MDM Toolset launched.

Procedure steps

1. From the Toolset under System -> Administration, select Service Selection - System Wide.

   The **Service Selection: Login** dialog opens.

2. If no administrator password has been configured, click **OK**. Otherwise, enter the existing password and click **OK**.

   The Service Selection - System Wide main window opens.

3. From the Security menu, select **Change password**.

   The **Password Change** dialog opens.

4. If you are changing an existing password, enter it in the **Old Password** field. Otherwise skip this step and go to step 5.

5. In the **New Password** field, enter the password to be used by the Service Selection Administrator.

6. In the **Confirm Password** field, enter the same password.

7. Click **OK**.

   The **Password Change** dialog closes and the new password is in effect.

Accessing Service Selection - System Wide

Use this procedure to access Service Selection - System Wide for the Preside Multiservice Data Manager (MDM) Toolset environment.

Prerequisites

- MDM Toolset launched.

Procedure steps

1. From the Toolset under System -> Administration, select Service Selection - System Wide.

   The **Service Selection: Login** dialog opens.

2. If no administrator password has been configured, click **OK**. Otherwise go to step 3.

   The **Service Selection - System Wide** main window opens.

3. Type your password in the **Password** field, then click **OK**.

   The **Service Selection - System Wide** main window opens.

Accessing Service Selection - System Wide for Operator Client

Use this procedure to access Preside Multiservice Data Manager (MDM) Service Selection - System Wide for the Operator Client environment.

Prerequisites

- MDM Toolset launched by the root user.

Procedure steps

1 From the Toolset under System -> Administration, select Service Selection - System Wide for Operator Client.

The **Service Selection - System Wide** main window opens.

Changing the system wide Services settings

Use this procedure to change the Preside Multiservice Data Manager (MDM) Services settings for all users in both the Toolset and Operator Client environments.

Prerequisites

- Service Selection - System Wide main window is open. See “Accessing Service Selection - System Wide” (page 484) or “Accessing Service Selection - System Wide for Operator Client” (page 485).
- MDM Services tabbed pane is selected.
- Optionally, use the Show Server Status command button to check the server status for the correct service selections. See “Server Status for Current selections dialog” (page 480).

Procedure steps

1. In the **Change Selections** panel, select a target server host from the **Server Host** picklist or type in the target server name or IP address.
2. Optionally, check the status of the target server host by clicking on the **Show Services** button. Otherwise, go to step 4.

   The **Server Status on <target server host name>** dialog opens.
3. Verify that the relevant server is running on the target server host.
4. In the **MDM Service** picklist, select All or select one of the services that you want to run on the server host.
5. Click on the **Set Service** button.

   The new server host name shows in the **Current Selections System Default** column beside the relevant MDM services.

Changing the system wide Help Service settings

Use this procedure to change the Help Service setting for all users in both the Preside Multiservice Data Manager (MDM) Toolset and Operator Client environments.

Prerequisites

- Service Selection - System Wide main window is open. See “Accessing Service Selection - System Wide” (page 484) or “Accessing Service Selection - System Wide for Operator Client” (page 485).
- Help Service tabbed pane is selected.

Procedure steps

1. In the **Change Selections** panel, select a target server host from the **Server Host** picklist or type in the target server name or IP address.
2. In the **Server Port** picklist, select or type a port number.
3. Click on the **Set Servic**e button.

   The new server host name and port number show in the **Current Selections System Default** column.

Service Selection User - Specific procedures

Use Preside Multiservice Data Manager (MDM) Service Selection - User Specific to override the system wide service selections for your user session at a client workstation.

Navigation

- "Accessing Service Selection - User Specific from the Toolset" (page 489)
- "Accessing Service Selection - User Specific from the Operator Client desktop" (page 490)
- "Changing the user specific Services settings" (page 491)
- "Unsetting Services user overrides" (page 493)

Accessing Service Selection - User Specific from the Toolset

Use this procedure to access Preside Multiservice Data Manager (MDM) Service Selection - System Wide in the Toolset environment.

Prerequisites

- MDM Toolset launched.

Procedure steps

1 From the Toolset under System -> Administration, select Service Selection - User Specific.

The **Service Selection - User Specific** main window opens.

Accessing Service Selection - User Specific from the Operator Client desktop

Use this procedure to access Preside Multiservice Data Manager (MDM) Service Selection - User Specific from an Operator Client workstation.

Prerequisites

- Operator Client desktop is launched.

Procedure steps

1 From the Operator Client desktop System menu, select Service Selection - User Specific

The **Service Selection - User Specific** main window opens.

Changing the user specific Services settings

Change the Preside Multiservice Data Manager(MDM) Services settings to override the system wide service selections. The procedure is applicable to a client workstation in the MDM Toolset and Operator Client environments.

Prerequisites

- Service Selection - User Specific main window is open. See “Accessing Service Selection - User Specific from the Toolset” (page 489) or “Accessing Service Selection - User Specific from the Operator Client desktop” (page 490).
- MDM Services tabbed pane is selected.
- Optionally, use the Show Server Status command button to check the server status for the correct service selections. See “Server Status for Current selections dialog” (page 480).

Procedure steps

1. In the **Change Selections** panel, select a target server host from the **Server Host** picklist or type in the target server name or IP address.
2. Optionally, check the status of the target server host by clicking on the **Show Services** button. Otherwise, go to step 4.

   The **Server Status on <target server host name>** dialog opens.
3. Verify that the relevant server is running on the target server host.
4. In the **MDM Service** picklist, select All or select one of the services that you want to run on the server host.
5. Click on the **Set Service** button.

   The new server host name shows in the **Current Selections System Default** column beside the relevant MDM services.

Changing the user specific Help Service settings

Change the Help Service settings to override the system wide service selections. The procedure is applicable to a client workstation in the Preside Multiservice Data Manager (MDM) Toolset and Operator Client environments.

Prerequisites

- Service Selection - User Specific main window is open. See “Accessing Service Selection - User Specific from the Toolset” (page 489) or “Accessing Service Selection - User Specific from the Operator Client desktop” (page 490).
- Help Service tabbed pane is selected.

Procedure steps

1. In the **Change Selections** panel, select a target server host from the **Server Host** picklist or type in the target server name or IP address.
2. In the **Server Port** picklist, select All or select one of the services that you want to run on the server host.
3. Click on the **Set Service** button.

   The new server host name and port number show in the **Current Selections System Default** column.

Unsetting Services user overrides

Use this procedure to unset any Preside Multiservice Data Manager (MDM) Services selections you have made.

Prerequisites

- one or more service selections is specific to your user session at the workstation
- Service Selection - User Specific main window is open. See “Accessing Service Selection - User Specific from the Toolset” (page 489) or “Accessing Service Selection - User Specific from the Operator Client desktop” (page 490).
- MDM Services tabbed pane is selected.
- Optionally, use the Show Server Status command button to check the server status for the correct service selections. See “Server Status for Current selections dialog” (page 480).

Procedure steps

1. In the **Current Selections** panel, select one or more of the MDM services that has an entry in the User Override column.
2. Click the **Unset User Override** button.

   The entry in the User Override column clears for each of the services you selected in step 1.

Unsetting Help Service user overrides

Use this procedure to unset the Help Service selection you have made.

Prerequisites

- one or more service selections is specific to your user session at the workstation
- Service Selection - User Specific main window is open. See “Accessing Service Selection - User Specific from the Toolset” (page 489) or “Accessing Service Selection - User Specific from the Operator Client desktop” (page 490).
- Help Service tabbed pane is selected.

Procedure steps

1. In the **Current Selections** panel, select the Help Service entry in the User Override column.
2. Click the **Unset User Override** button.

   The entry in the User Override column clears.

Troubleshooting procedures

This section contains instructions for coping with the most common difficulties that arise when using Preside Multiservice Data Manager (MDM) Service Selection tool. The troubleshooting procedures are described in the following sections:

- "Server status not available" (page 495)
- "Forgotten password" (page 495)

Server status not available

Use this procedure if one or more host names show 'status not available in the Server Status for Current Selections dialog.

1. Log in as root.
2. Enter the PING command once for each workstation that is missing from the list of host names to determine if the workstation is able to respond. The workstation(s) missing from the list may be shut down.

   ```
   /usr/bin/ping <hostname>
   ```

3. Using an editor, examine the contents of file /etc/hosts.The node names and IP addresses of all workstations in the domain to which this workstation belongs should be listed in this file.
   - If they do, continue at step 4.
   - If they do not, and this workstation belongs to a network that uses a Naming Information Service (NIS), use the Sun NIS Administration tool to add the missing host names and IP addresses.
   - If they do not, and this workstation does not belong to a network that uses NIS, add the missing host names and IP addresses to the file.
4. Verify that *mnsdagent* is running on the workstation.

Forgotten password

Use this procedure to delete the administrator password if you forget what the current password is.

Deleting the current password involves logging in as root and removing the administrator password file (/opt/MagellanNMS/cfg/private/ServSel.passwd). Once the current password is deleted, see "Setting up an administrator password" (page 483) to establish a new password.

1. Log in as root
2. Remove the administrator password file:

   ```
   rm /opt/MagellanNMS/cfg/private/ServSel.passwd
   ```

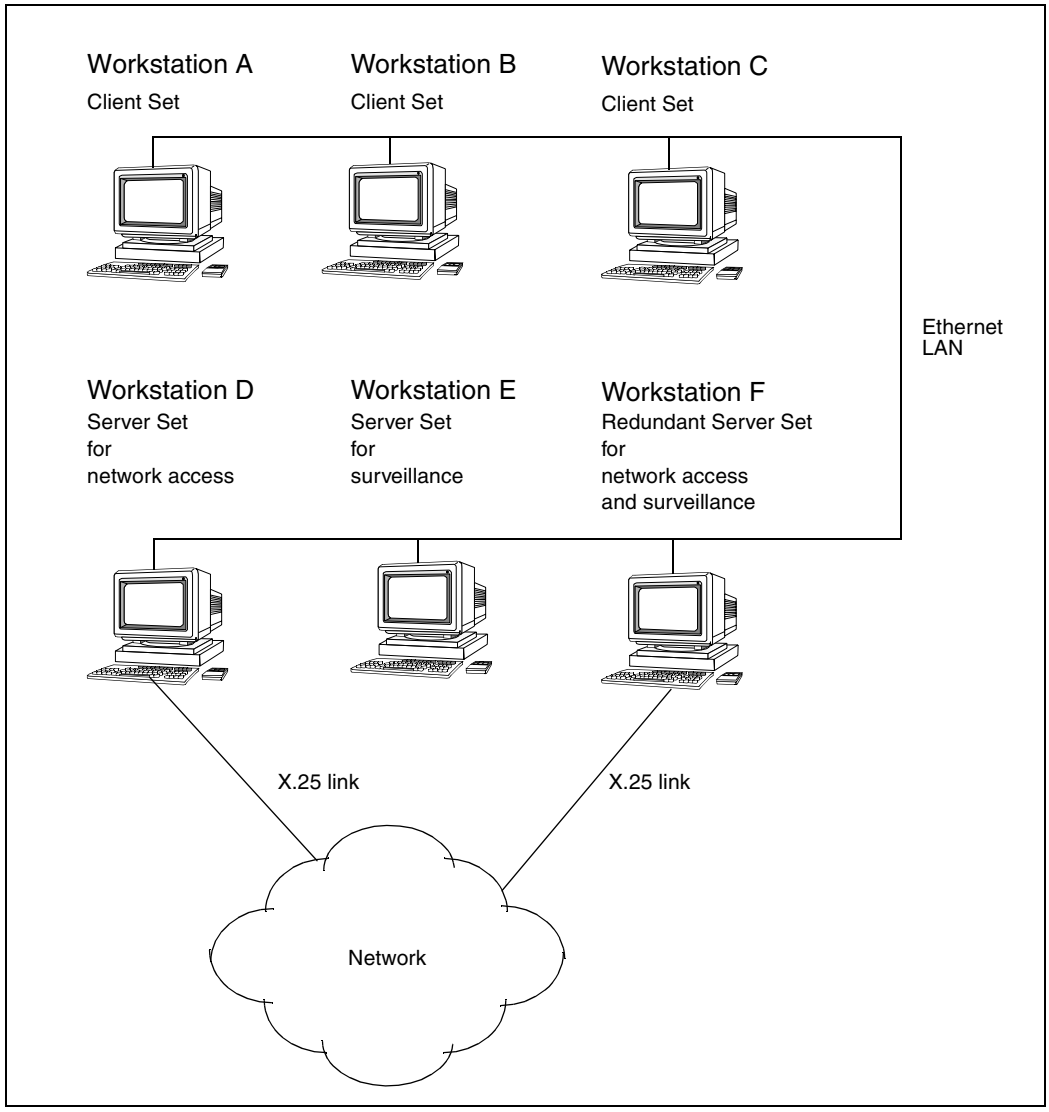
3. Create a new administrator password, as described in “Setting up an administrator password” (page 483).

Sample Server Set/Client Set configuration for a large network

For a sample configuration of Server Set and Client Sets in a large network, see the figure "Sample Server Set and Client Set configuration for a large network" (page 498). In this figure, the user at workstation B could select the Server Set on workstation D to obtain access to the network, or the Server Set on workstation F.

Similarly, the user on workstation A could select the Server Set on workstation E to obtain surveillance information for alarm-based surveillance, or the Server Set on workstation F.

Figure 48
Sample Server Set and Client Set configuration for a large network



Chapter 25
Using the System Log Display tool

This section explains the purpose of the System Log Display tool and provides instructions for using the tool. See the following sections for more information:

System Log Display tool

The System Log Display tool lets you display and print logs produced by the Preside Multiservice Data Manager (MDM) servers and by the action of the tools. With the tool you can also pause the displaying of new logs, and copy logs to the clipboard.

For information about the logs produced by the MDM servers, see 241-6001-310 *Preside MDM Server Reference Guide*. For information about the logs produced by the action of the tools, see "MDM log files" (page 539).

You cannot, however, use the System Log Display tool to route log information to a file. To do this, you must use the Server Administration tool to start the OAMC server with the command:

```
/opt/MagellanNMS/bin/oamc -f <log file name>
```

For instructions to use the Server Administration tool to start the OAMC server, see "Using the Server Administration tool" (page 359).

See the following information:

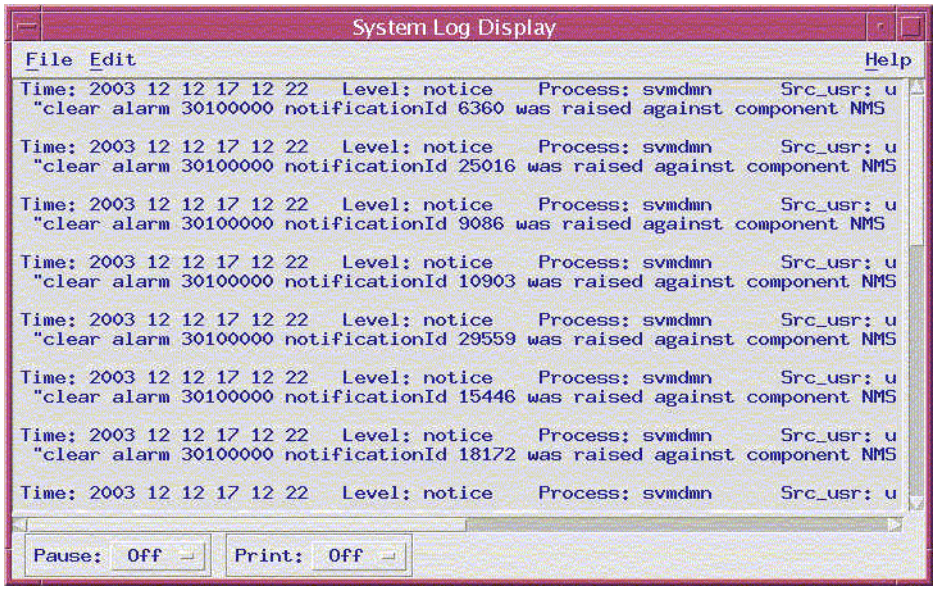
- “System Log Display main window” (page 500)
- “Keyboard shortcuts” (page 502)
- “Procedures” (page 503)

System Log Display main window

The main window contains the items described in the following sections:

- “File menu” (page 501)
- “Edit menu” (page 501)
- “Help menu” (page 501)
- “Log List” (page 501)
- “Pause menu button” (page 502)
- “Print menu button” (page 502)

Figure 49
System Log Display main window



File menu

The File menu contains the following command:

- Exit closes the System Log Display main window.

Edit menu

The Edit menu contains the following commands:

- Copy copies the current selection into the clipboard.
- Select All selects and highlights all of the log information displayed in the Log List.
- Deselect All cancels any selections that have been made in the Log List and removes any highlighting.

Help menu

The Help menu contains the following commands:

- On Context lets you choose any area of the window and receive help about that part of the window.
- On Help displays help about the help facility.
- On Window displays help about the application main window and its general contents.
- On Keys displays help about the keyboard accelerators.

Log List

The Log List displays log reports produced by the Preside Multiservice Data Manager (MDM) servers and by the action of the tools.

For information about the logs produced by the MDM servers, see 241-6001-310 *Preside MDM Server Reference Guide*. For information about the logs produced by the action of the tools, see “MDM log files” (page 539).

Edit pop-up menu

The Edit pop-up menu available in the Log List contains the following commands:

- Copy copies the current selection into the clipboard.

- Select All selects and highlights all of the log information displayed in the Log List.
- Deselect All cancels any selections that have been made in the Log List and removes any highlighting.

Pause menu button

The Pause menu button lets you halt the addition of new logs to the Log List, and provides the following two choices:

- Off displays any new logs at the bottom of the Log List and scrolls it down to the end. If the text already contains the maximum number of logs when a new log is received, the oldest log (the one at the top) is removed.
- On halts the display of incoming logs and places them in a buffer. If more than 100 logs are received while the Pause is On, Pause is automatically reset to Off.

Print menu button

The Print menu button lets you send incoming logs to a printer, and provides the following two choices:

- On prints logs in the log display to the default printer as defined by the environment variable LPDEST, or if a printer name is not defined for this variable, to the system-wide default printer.
- Off halts the printing of logs.

Keyboard shortcuts

The System Log Display provides the following command shortcuts:

- Ctrl + / selects all logs in the System Log Display.
- Ctrl + \ deselects all logs in the System Log Display.
- Ctrl +C copies the current selection to the clipboard.
- Ctrl +E closes the System Log Display window.
- Ctrl+P sets Print to On.
- Ctrl+O sets Print to Off.
- Ctrl+S sets Pause to On.

- Ctrl+Q sets Pause to Off.

Procedures

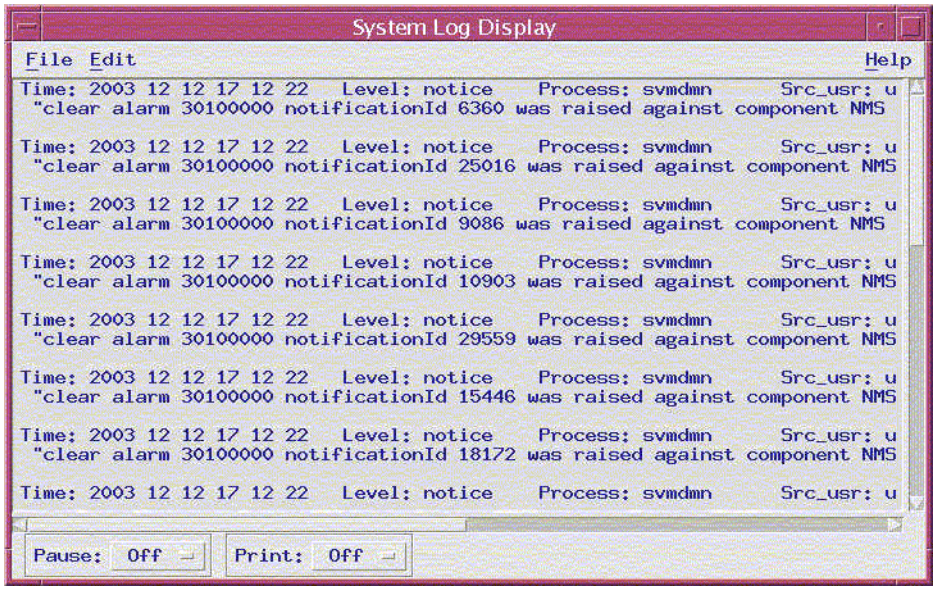
See the following sections for procedures you can perform with the System Log Display tool:

Starting the System Log Display tool

Use this procedure to start the System Log Display tool.

1 From the application main window select System -> Administration -> System Log Display.

The System Log Display main window opens.



Stopping and starting the display of new incoming logs

Use this procedure to halt the display of new incoming logs in the System Log Display main window or to start displaying them again. You may need to halt the display of new incoming logs while you copy, select, or print off log information, particularly if logs are being output frequently.

1 To halt the display of new incoming logs, select On from the Pause menu button.

No new logs are displayed in the Log List. All incoming logs are stored in a buffer until 100 logs have been accumulated. When more than 100 logs are in the buffer, Pause is automatically set to Off.

2 To resume the display of new incoming logs, select Off from the Pause menu button.

After you choose On or Off, the word On or Off is displayed on the Pause button to indicate whether new incoming logs are being added to the screen.

If you stop incoming logs from being displayed on the screen then turn them back on again, any logs that were buffered while incoming logs were shut off are added to the display.

Scrolling through logs in the System Log Display

The log list area of the System Log Display main window is equipped with vertical and horizontal scrollbars. Use this procedure to scroll up or down through the logs.

Scrolling through logs in the System Log Display

1 Stop incoming logs from being added to the Log List as described in “Stopping and starting the display of new incoming logs” (page 504).

This freezes the log display area and prevents new logs from being added to the area while you are attempting to scroll through them.

2 To scroll upwards or downwards, place the cursor on the elevator in the vertical scrollbar, then press the left mouse button while moving the mouse towards you or away from you.

3 To scroll left or right, do the same thing, except use the horizontal scrollbar and move the mouse left or right.

Selecting and copying logs

Use the following procedures to select one or more logs, or to select all logs, and copy them into the clipboard from where they can be pasted into another application for further use.

Selecting one or more logs

1 Stop incoming logs from being added to Log List as described in “Stopping and starting the display of new incoming logs” (page 504).

This freezes the log display area and prevents new logs from being added to the area while you are attempting to select them.

2 In the Log List, place the cursor at the beginning or end of the log or logs that you wish to print out.

3 Drag the mouse to select the log or logs you wish to copy.

The text is highlighted to indicate that it has been selected.

4 From the Edit menu, select Copy.

The text that is selected is copied to the clipboard and is ready to be pasted into another application.

Selecting all logs

1 From the Edit menu, select Select all.

All logs in the window are highlighted to indicate that they are selected.

2 From the Edit menu, select Copy.

The text that is selected is copied to the clipboard and is ready to be pasted into another application.

Deselecting all logs

Use this procedure to deselect all logs that have been selected in the System Log Display main window.

Deselecting all logs

1 From the Edit menu, select Deselect all.

Highlighting is removed from the log display area to indicate that text is no longer selected.

Printing all logs in the Log List

Use this procedure to stop and start printing logs that are displayed in the Log List. You can only print off all logs that are being displayed; you cannot select and print off individual logs. Also, the print command only prints off new incoming logs; it does not print of existing logs that are already displayed on the screen.

To print off logs, you must have set up the LPDEST environment variable in the user account's .login file to specify the workstation's default printer.

Printing all logs from the System Log Display

1 From the Print menu button, select On.

After you choose On or Off, the word On or Off is displayed on the Print button to indicate that printing is turned on or off.

Chapter 26
Managing Passport SDD files

This section describes Passport SDD files and contains procedures for generating, installing, and deleting them. See the following sections for more information:

- “About SDD files” (page 507)
- “Manually generating model files” (page 509)
- “Generating model files from a tar file on compact disk or one delivered electronically” (page 512)
- “Uploading a tar file and generating model files” (page 514)
- “Deleting old model files” (page 515)

About SDD files

Passport Software Data Definition (SDD) files define the structure and format of service data for Passport nodes. This information is needed as the framework for performing provisioning and surveillance operations on a node.

More than one SDD file is used to define the structure and format of the service data for a node. Together these files constitute a model that is identified by a version number, for example: AC0053C. Because SDD files constitute a model, they are also referred to as model files.

Model files can be obtained in the following ways:

- automatically by starting a provisioning session to a node

- manually by generating them from a tar file on compact disk, on tape, or that has been transferred electronically
- manually by generating them from a tar file uploaded from a node
- automatically by generating them from a tar file uploaded from a node when new software is detected

For more information, see the following:

- "SDD files and provisioning applications" (page 508)
- "SDD files and surveillance applications" (page 508)

SDD files and provisioning applications

When a provisioning application, such as the Component Provisioning tool, requires access to a model file, the provisioning stack (fps) does the following to provide access to the file:

- Fps determines if the model file is loaded into its local memory and if it is, provides access to it.
- If the model file is not loaded into memory, fps searches for it on the Preside Multiservice Data Manager (MDM) disk and uploads it into its own memory.
- If fps cannot find the model file on MDM disk, it automatically uploads the model file from the node, copies it onto MDM disk, and loads it into its own memory.

SDD files and surveillance applications

When a surveillance application, such as Network Viewer, requires access to a model file, the model file is loaded into shared memory, meaning that the SDD file is parsed and the corresponding model is created in shared memory. model files are updated dynamically in shared memory. Dynamic updating refers to the following behaviours:

- SDD files are automatically retrieved from the node when new software is detected.
- Applications in the middle of processing can cut over to new model files without causing any service interruption.

Dynamic updating of models occurs under the following conditions:

- Each time a login to a node occurs, the software versions on the node and the loaded model files are compared. If the software version on the node is higher than the software version of the loaded model for that family, a new model based on the software on the switch is dynamically loaded into shared memory.
- The script fdtm.newsdd.kick has been run. Run this script as part of an explicit management operation when you use the getsursdd script to retrieve an SDD file from a node. Fdtm.newsdd.kick signals FDTM to check each family's SDD files. If FDTM finds any updated SDD files, fdtm.newsdd.kick parses the SDD files and dynamically loads the new model into shared memory.

Once dynamic updating is complete, all applications are notified to synchronize to the new model files. When all applications respond that they have synchronized, the shared memory segment associated with the old model files is released.

Manually generating model files

Although fps uploads model files automatically for a provisioning application, it is sometimes necessary to generate model files manually from a tar file. For example, if you are only using a workstation for surveillance purposes, you will never launch a provisioning session and fps will not upload the required model files. When this is the case, you need to generate them manually from a tar file.

Generating the model files manually requires the use of the fmsgetmod or getsursdd utilities provided with the Preside Multiservice Data Manager (MDM) software.

For more information, see the following:

- "Fmsgetmod" (page 510)
- "Getsursdd" (page 511)

Fmsgetmod

This utility extracts source files from the tar file, generates output model files, and installs them in the /opt/MagellanNMS/cfg/PassportSchema directory on Preside Multiservice Data Manager (MDM) disk. The tar file can be on disk, in a directory, or on a node. If the file is on a node, the fmsgetmod utility can be used to upload the tar file first before doing the generate and install operations.

The fmsgetmod utility creates templates for the provisioning user interface. Since these templates are only needed for Passport provisioning applications, you can use the simpler getsursdd utility to retrieve an SDD file from a node for all other applications.

The fmsgetmod utility can also be used to delete old model files. You can delete the files with the rm command, but you need to manually determine the correct files to delete for a given version of the model. Because the fmsgetmod utility automatically determines the correct files to delete for a given version and deletes them, it is the recommended method.

> ***Note:*** If you used the getsursdd utility to retrieve an SDD file from a node, you can use the rm command to delete the SDD file. No other files are created by getsursdd.

Use the following command to run the fmsgetmod utility:

```
/opt/MagellanNMS/bin/fmsgetmod
-v <version>
[-u <host userid passwd> |-s <src_dir> |-t <tarfile>]
[-d]
[-f]
```

where:

`-v <version>` specifies the version of the model, for example, AC0323c

`-u <host userid passwd>` uploads a tar file from a node, generates model files from it, and installs them where:

`host` is the IP address or NIS name of the node

`id` is a valid user ID on the node

`passwd` is the valid password for the user ID

> ***Note:*** The PROV_TEMPDIR_PATH environment variable can be set to specify the directory on the MDM disk into which the tar file is uploaded. If this variable is not set, fmsgetmod uploads the tar file into directory /opt/MagellanNMS/data/architect_tmp. If this directory does not exist, fmsgetmod uploads the file into directory /tmp.

`-s <src_dir>` generates new model files from a directory containing existing model files. The value for `src_dir` is the path to the directory that contains the existing model files.

`-t <tarfile>` is the full pathname of the tar file on the MDM disk or on compact disk

`-d` removes all model files associated with the version except the file named sursdd<version>.act, for example, sursddAC0323c.act. This file is a master file from which all other models files can be generated. To remove all files including the master file, use the -f option.

`-f` removes all model files associated with the version, including the file named sursdd<version>.act, and then regenerates the model files

> ***Note 1:*** If you specify the -d option, the -u, -s, and -t options are ignored.
>
> ***Note 2:*** The -u, -t, and -s options are mutually exclusive. You can only specify one of them.

Getsursdd

The getsursdd utility restrieves a specified SDD file from a node if the SDD file does not already exist on the Preside Multiservice Data Manager (MDM) workstation. This utility does not create any other files, such as the templates for the provisioning user interfaces, that the fmsgetmod utility does.

Use the following command to run the getsursdd utility:

```
/opt/MagellanNMS/bin/getsursdd -v <version>\
-u <host userid passwd>
```

where:

`-v <version>` specifies the version of the model, for example, AC0323c

`-u <host userid passwd>` specifies the node and valid user ID and password from which to retrieve the SDD file

After you run the getsursdd utility, run the fdtm.newsdd.kick utility, which signals FDTM to check the software version of each family's model files. If FDTM finds any updated SDD files, fdtm.newsdd.kick parses the SDD files and dynamically loads the new model files into shared memory.

You must be logged on as root to run fdtm.newsdd.kick. Use the following command to run the utility:

```
/opt/MagellanNMS/bin/fdtm.newsdd.kick
```

Generating model files from a tar file on compact disk or one delivered electronically

Use the following procedure to generate and install model files from a tar file on compact disk, or one that is delivered to you electronically by using a file transfer protocol such as FTP.

1. Log in as root.
2. Display the subdirectories in /opt/MagellanNMS/cfg:

   ```
   ls /opt/MagellanNMS/cfg
   ```

3. Verify that PassportSchema is listed among the directories displayed on the screen. If this directory does not exist, create it by entering the following command:

   ```
   mkdir /opt/MagellanNMS/cfg/PassportSchema
   ```

4. If the tar file is on compact disk, go to step 5.

   If the tar file is delivered electronically, go to step 10.

5. Enter the following command to determine if the volume manager is running:

   ```
   ps -ef | grep vold
   ```

   The response indicates if it is running.

6. If the volume manager is running, go to step 10. If the volume manager is not running, go to step 7.

7 Display the contents of the root (/) directory:

```
ls /
```

The response should include the cdrom directory.

8 If the cdrom directory does not exist, create it:

```
mkdir /cdrom
```

9 Mount the CD-ROM drive:

```
mount -F hsfs /dev/sr0 /cdrom
```

Note: Substitute the name for your cdrom device, if it is different from sr0.

10 Generate the model files from the tar file and install them:

```
/opt/MagellanNMS/bin/fmsgetmod -v <version> \
-t <tarfile>
```

Examples:

For a tar file on compact disk:

```
/opt/MagellanNMS/bin/fmsgetmod -v AC0053C \
-t /cdrom/cdrom0/sdd/nmsSDDAC0053C.tar
```

For a tar file delivered electronically (see note):

```
/opt/MagellanNMS/bin/fmsgetmod -v AC0053C \
-t /tmp/nmsSDDAC0053C.tar
```

Note: Substitute the name of the directory in which the tar file is located, if it is different from /tmp.

The fmsgetmod utility extracts the source files from the tar file. generates output model files, and installs them in directory /opt/MagellanNMS/cfg/PassportSchema.

11 Access the PassportSchema directory:

```
cd /opt/MagellanNMS/cfg/PassportSchema
```

12 List information about the model files that have been generated and installed:

```
ls -l -d *<version>*
```

13 Verify that the file permissions are set to read/write by owner and group, and read only by others. That is: rw-rw-r--.

If they are not set correctly, enter the following command:

```
chmod -R 664 <version>
```

Uploading a tar file and generating model files

Use the following procedure to upload a tar file from a node, extract source files, generate output model files, and install them by means of the fmsgetmod utility.

Before beginning this procedure, an IP connection must be configured between the node and the workstation.

The PROV_TEMPDIR_PATH environment variable can be set to specify the directory on Preside Multiservice Data Manager (MDM) disk into which the tar file is uploaded. If this variable is not set, fmsgetmod uploads it into directory /opt/MagellanNMS/data/architect_tmp. If this directory does not exist, it uploads the file into directory /tmp. In this procedure it is assumed that environment variable PROV_TEMPDIR_PATH is not set and directory /opt/MagellanNMS/data/architect_tmp does not exist. Therefore, a copy of the tar file is uploaded into the /tmp directory.

1 Check to see if an IP connection exists to the node:

ping <ip_address)

where:

<ip_address>

is the IP address of the node on which the tar file resides

You should get the response: <ip_address> is alive. If you don't, check the configuration of the IP connection to the node.

2 Upload the tar file, generate and install the model files by entering one of the following commands:

/opt/MagellanNMS/bin/fmsgetmod -v <version>
-u <host userid passwd>

/opt/MagellanNMS/bin/getsursdd -v <version>
-u <host userid passwd>

Example:

/opt/MagellanNMS/bin/fmsgetmod -v AC0053C
-u 47.55.55.55 myuserid mypassword

The fmsgetmod utility automatically locates the tar file associated with version AC0053C on the node, uploads a copy into the /tmp directory,

extracts the source files, generates output model files, and installs them in directory /opt/MagellanNMS/cfg/PassportSchema.

The getsursdd utility automatically locates the tar file associated with version AC0053C on the node, generates output model files, and installs them in directory /opt/MagellanNMS/cfg/PassportSchema.

3 Access the PassportSchema directory:

```
cd /opt/MagellanNMS/cfg/PassportSchema
```

4 List information about the model files that have been generated and installed:

```
ls -l -d *<version>*
```

5 Verify that the file permissions are set to read/write by owner and group, and read only by others. That is: rw-rw-r--.

If they are not set correctly, enter the following command:

```
chmod -R 664 <version>
```

Deleting old model files

Use the following procedure to delete old model files associated with a version of a model.

Note: If you used the getsursdd utility to retrieve an SDD file from a node, you can use the rm command to delete the SDD file. No other files are created by getsursdd.

1 Log in as root.

2 Access the PassportSchema directory:

```
cd /opt/MagellanNMS/cfg/PassportSchema
```

3 List information about the model files that are installed:

```
ls -l -d *<version>*
```

4 Enter one of the following commands to remove the model files associated with the model version:

To remove all files, except the master file:

```
/opt/MagellanNMS/bin/fmsgetmod -v <version> -d
```

To remove all files including the master file

/opt/MagellanNMS/bin/fmsgetmod -v <version> -d -f

Examples:

/opt/MagellanNMS/bin/fmsgetmod -v AC0053C -d

/opt/MagellanNMS/bin/fmsgetmod -v AC0053C -d -f

The fmsgetmod utility determines the model files associated with version AC0053C, and deletes them.

5 Access the PassportSchema directory:

cd /opt/MagellanNMS/cfg/PassportSchema

6 List information about the model files that are installed:

ls -l -d *<version>*

The model files associated with the version should now be deleted.

Chapter 27
Configuring shared memory

This section contains instructions to re-configure the shared memory segment size in the kernel of the Solaris operating system. Also, this section describes how the following applications use shared memory:

- the Network Model
- Passport Communications Manager (FDTM)
- Passport Configuration Model Server (PCMS)

See the following sections for more information:

- "Determining the requirements for shared memory" (page 517)
- "Setting the amount of shared memory in the kernel" (page 518)

Determining the requirements for shared memory

You need to configure shared memory in the kernel of the Solaris operating system on the workstation. The amount of shared memory of the following applications should be less than the system default of 256 Mbyte:

- the amount of shared memory to support the size of the Network Model on your workstation
- the amount of shared memory required by the Passport Communication Manager (FDTM) to load models
- the amount of shared memory required by the Passport Configuration Model Server (PCMS)

Setting the amount of shared memory in the kernel

Setting the amount of shared memory in the kernel involves setting the value of variable shmysis:shminfo_shmax in the system kernel file /etc/system, then rebooting the workstation to make the changes effective. This variable specifies the amount of memory that an application can create as a shared memory segment. You can create multiple such segments. Because shared memory is swapped in and out just like the workstation's virtual memory, it can therefore can be larger than the workstation's physical memory size. By default the amount applications can create is 1 Mbyte.

If you need to increase the amount of shared memory, you can use an editor, such as vi, to change the value of the shared memory variable in kernel file /etc/system, but the Preside Multiservice Data Manager (MDM) software provides a convenient script for this purpose. This scripts are contained in the files /opt/MagellanNMS/system/config/config_sys_shmem <size> and /opt/MagellanNMS/system/config/config_sys_semaphores. These scripts have the following advantages:

- reads the amount of shared memory allocated in the kernel file, and increases the amount only if you specify an amount greater than the amount that is already allocated
- retains a copy of the existing kernel in file /etc/system.old

If you want to decrease the amount of shared memory, you cannot use script config_sys_shmem. You need to edit the file with a UNIX editor.

Use the procedure, "Using the config_sys_shmem script to configure shared memory" (page 518) to reconfigure the amount of shared memory using the config_sys_shem script.

Using the config_sys_shmem script to configure shared memory

1. Log in as root.
2. In a UNIX access window enter the following commands:

```
/opt/MagellanNMS/system/config/\
config_sys_shmem <size>

/opt/MagellanNMS/system/config/config_sys_semaphores
```

3 Enter the following commands to reboot the workstation, and make the new shared memory available.

```
sync
sync
init 6
```

Variable definitions

Variable	Definition
`size`	is the maximum amount of shared memory, in megabytes, to be allocated per segment. The suggested size is 256 Mbyte. This amount of shared memory will be sufficient for both surveillance and configuration tools.

Shared memory required by a Network Model

In the startup command for the Network Coordinator (DNMNMC) server, you can specify the amount of shared memory that the server uses for Network Models. You can make this specification by starting the server with the following command:

```
/opt/MagellanNMS/bin/dnmnmc [-s <shm size in MB>]
```

Note 1: If this option is not specified, the DNMNMC server reserves the largest possible shared memory segment allowed by the kernel. Therefore, it is important to specify a specific amount of shared memory for the DNMNMC server.

Note 2: For the shared memory to take effect, it must also be set in the startup command for the Network Model Coordinator (DNMNMC). See 241-6001-310 *Preside MDM Server Reference Guide*.

The amount of shared memory required by a Network Model is proportional to the number of components in the network. Use the following formula as a guide to calculate the shared memory requirements for each Network Model that runs on the workstation.

```
(270 + 20% x ( 25 x #PM + 60 x #EM + 8 x #other ))/1024
MB
```

The Preside Multiservice Data Manager (MDM) software provides a shared memory utilization tool that displays the amount of shared memory occupied by the current Network Model. To access this tool, from the MDM main window select System -> Utilities-> Network Model Shared Memory Utilization.

Variable definitions

Variable	Definition
`sh size in MB`	is the maximum amount of shared memory to reserve. This number must be less than or equal to the maximum shared memory segment size configured in the workstation's kernel. The default is 24 Mbyte.
`#PM`, `#EM`, and `#other`	are the number of DPN modules, the number of Passport modules, and the number of all other components (such as links) in the network.

Shared memory required by FDTM

In the startup command for the Passport Communications Manager (FDTM), you can specify the amount of shared memory that the server uses for each model that is loaded. Currently, the models for all the Passport releases supported by Preside Multiservice Data Manager are all smaller than the default size of 20 Mbyte used by FDTM. It is not necessary to provide a different value. However, if you decide to specify another value, use the following command line syntax:

```
/opt/MagellanNMS/bin/fdtm [-segSize <size>] (other
options...)
```

Variable definitions

Variable	Definition
`size`	is the size, in Mbyte, of each segment of shared memory segment. The default value is 20 Mbyte.

Shared memory required by PCMS

In the startup command for the Passport Configuration Model Server (PCMS), you can specify the amount of shared memory that the server uses for loading models. When the server starts, it allocates the shared memory up front using the following formula:

```
Number of models x model size
```

Variable definitions

Variable	Definition
`number of models`	is the number of different Passport software releases active in the network. The default for PCMS is 2.
`model size`	is the size, in Mbyte, of one Passport model. The default is 20 Mbyte. Currently, the model size of each of the Passport releases supported by Preside Multiservice Data Manager is smaller than 20 Mbyte. It is unnecessary to provide a different value.

If you need to use values other than the defaults, use the following command line syntax:

```
/opt/MagellanNMS/bin/pcms [-numOfModels <n>] [-
modelSize <s>] (other options...)
```

Chapter 28
Configuring maximum heap size for shared JVM

This section provides the instructions required to configure the maximum heap size for a shared Java virtual machine (JVM). Shared JVM is a single Java virtual machine that is shared by a number of applications.

See the following sections for more information:

About the maximum heap size

Heap size is the dynamic allocation of memory allowed for running Java processes. The following applications can be run simultaneously using one shared JVM process:

- Data Viewer
- Shelf View
- Nodal Provisioning
- Embedded Nodal Provisioning (ENP)

- Nodal Provisioning Template Editor
- Service Selection
- Operational Command
- Log Browser

The default /opt/MagellanNMS/lib/cfg/SharedJVM.cfg configuration file

The maximum heap size is defined in the default configuration file /opt/MagellanNMS/lib/cfg/SharedJVM.cfg. You can make a copy of this file in the directory /opt/MagellanNMS/cfg/ and use it as a template to create a new file with custom settings. See "Changing the maximum heap size for MDM toolset" (page 525).

The minimum heap size is 20M. The default for maximum heap size is 128M. The default of 128M allows a user to run the following:

- one instance of Nodal Provisioning
- one instance of Shelf View with ENP
- two instances of Data Viewer with default parameters, or one instance of Data Viewer replaying a BDF file of about 10M in size.

File format

The /opt/MagellanNMS/lib/cfg/SharedJVM.cfg file consist of the following syntax:

```
MAXHEAPSIZE <size in megabytes>
```

where:

MAXHEAPSIZE is the maximum allocation of dynamic memory (heap) for running simultaneous applications in a shared JVM.

<size in megabytes> is the maximum number of megabytes allocated for the heap.

Example

```
MAXHEAPSIZE 128
```

Monitoring the maximum heap size

The maximum heap size is monitored to ensure that the shared JVM does not run out of heap space. The heap size is monitored every 60 seconds. The criteria used to monitor the heap size is:

Maximum heap size minus Currently used heap size < 10M

Memory usage warning dialog

A pop-up dialog opens whenever the currently-used heap size reaches 10M less than the maximum heap size configured. The dialog informs the user that system resources (heap size) are running low, and some applications must be closed.

If the dialog is displayed frequently, it indicates that the shared JVM is not configured with the appropriate maximum heap size. It is recommend that the maximum heap size be increased. See “Changing the maximum heap size for MDM toolset” (page 525) or “Changing the maximum heap size for MDM Operator Client” (page 526).

Changing the maximum heap size for MDM toolset

The maximum heap size should be changed in situations when the user wants to run many instances of the following: Data Viewer, Shelf View, Nodal Provisioning, and Embedded Nodal Provisioning. Each user session requires up to the maximum heap size specified plus the memory required for the process. Heap size should be changed after carefully analyzing total workstation RAM, swap space and user session requirements. For more information, refer to 241-6001-102 *Preside MDM Planning Guide*.

Prerequisites

- You must be logged in as root to change the maximum heap size.

Procedure steps

1. Stop all the Preside Multiservice Data Manager (MDM) applications running in the shared JVM environment, for example, Data Viewer, Shelf View, and Nodal Provisioning.

2 Copy the default configuration file from the default directory /opt/MagellanNMS/lib/cfg/SharedJVM.cfg:

```
cp /opt/MagellanNMS/lib/cfg/SharedJVM.cfg /opt/
MagellanNMS/cfg/SharedJVM.cfg
```

3 Edit the new file.

```
vi /opt/MagellanNMS/cfg/SharedJVM.cfg
```

4 Set MAXHEAPSIZE to a new value.

Note: The maximum heap size cannot be less than 20M (the hard-coded minimum.)

5 Save the changes.

6 Launch any of the MDM applications in shared JVM. The new heap size is now in effect.

Changing the maximum heap size for MDM Operator Client

The maximum heap size may need to be changed in situations when the user wants to run many instances of specific applications. Each user session requires up to the maximum heap size specified plus the memory required for the process. Heap size should be changed after carefully analyzing total workstation or PC RAM, swap space and user session requirements. For more information, refer to 241-6001-102 *Preside MDM Planning Guide*.

Procedure steps

1 Edit the DesktopGUI.jnlp located in /opt/nortel/config/applications/desktop/jws/mft/resources/desktop

2 Locate the lines starting with:

j2se version=”1.4.2_02+” href=”http://Please install JRE 1.4.2_02 or higher.” initial-heap-size=”64m” max-heap-size=”xxxm” /

and

j2se version=”1.4.2_02+” href=”http://java.sun.com/products/autodl/j2se” initial-heap-size=”64m” max-heap-size=”xxxm” /

where:
xxx is the current max heap size and should be greater or equal to 64 (the initial heap size).

3 Click reload on the browser to load the changed jnlp file. Only new sessions will use the modified value.

Chapter 29
Using the Auto-Patch tool

The Preside Multiservice Data Manager (MDM) Auto-Patch tool simplifies the tasks you perform to download and apply non-service affecting (TAP) patches to Passport nodes. The tool enables you to schedule the application of TAP patches across multiple nodes simultaneously. This functionality is available only with PCR 6.1 on Passport 7400, 15000, and 20000 nodes.

Using the Auto-Patch tool ensures that all the nodes in your network have access to the complete set of TAP and Reset patches available at the SDS. The tool frees you from the day-to-day monitoring of the patch releases and guarantees that each node is running up-to-date patches.

ATTENTION	You cannot use the Auto-Patch tool to apply service-affecting patches.

Prerequisites to using the Auto-Patch tool

- PCR 6.1 loaded on the Passport 7400, 15000, and 20000 nodes
- Patch Auto-Application feature active in the nodes (reference to PP NTP to be added when available)
- HGDS populated
- you must have permission to edit the crontab if you want to use it to schedule the Auto-Patch process
- all non-service affecting patches loaded to the SDS
- Patch Av downloaded from the SDS site

Navigation

Tool fundamentals

The Auto-Patch tool lets you schedule the patch download and application on the Passport nodes. The applications should be set to run during off-peak times. You can configure the frequency and timing of the applications using the crontab utility or any similar scheduling method the you use in your network. You can specify the nodes and the tool operation for each node to download patches or apply patches, or both.

You can schedule and control the patching from any Preside Multiservice Data Manager (MDM) workstation.You can run the Auto-Patch operations on a daily basis, or more or less frequently. This lets you to schedule redundant MDM hosts for patching purposes.

There are two MDM on-switch commands that are part of the Auto-Patch tool: *ppautopatch -download* and *ppautopatch -apply*. See "Configuring the auto-patch process" (page 532)

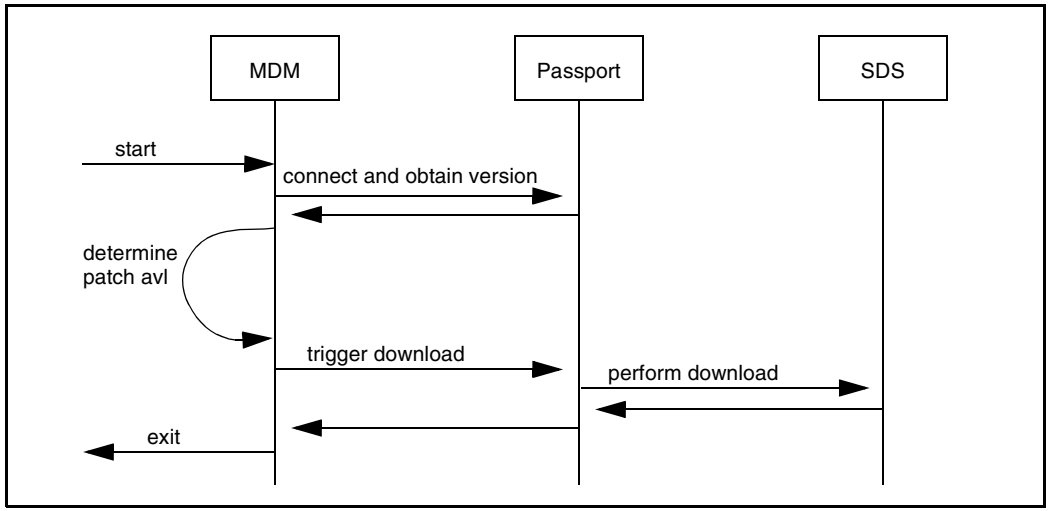
Patch download

The Auto-Patch tool triggers a software download to each node, based on the patch download schedule you have configured. If new patches are available, they are downloaded to the node file system. If all of the available patches have already been downloaded to the file system, then no transfer occurs.

The patch version information on-switch is obtained during the login confirmation and is used in setting the *download avl* component. Then the node is instructed to retrieve the patches from the SDS. The address and authentication for the SDS host is obtained from the associated run-time parameter.

See "Auto-patch download process flow" (page 531).

Figure 50
Auto-patch download process flow



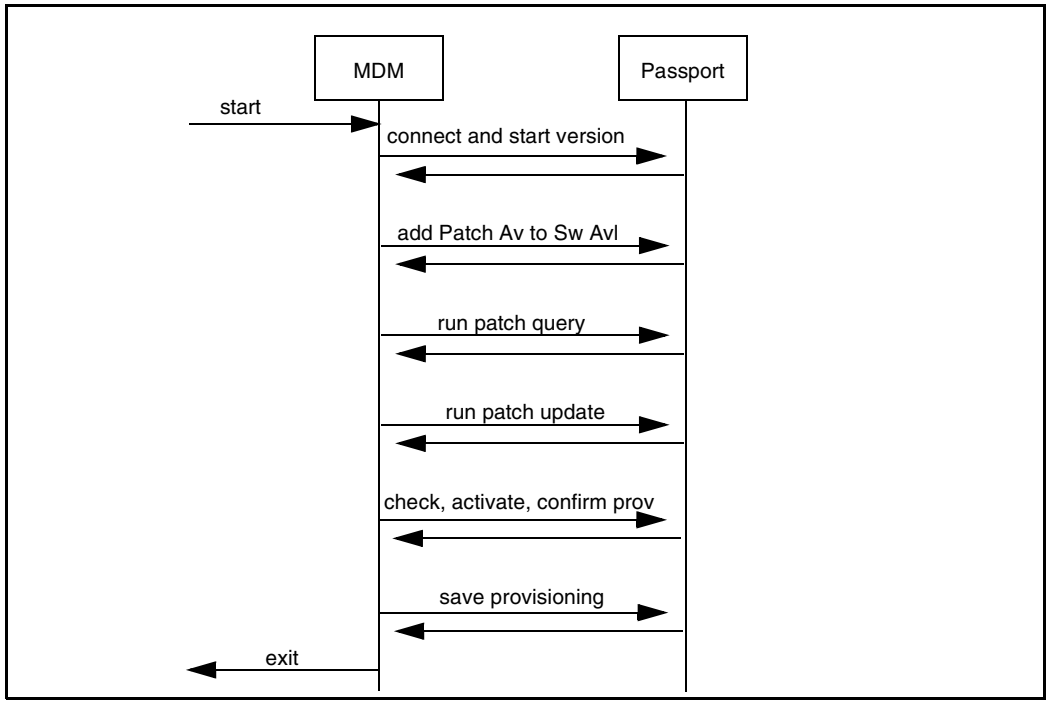
Patch application

The Auto-Patch tool initiates a provisioning session on each node, based on the patch application schedule you have configured. The provisioning session updates the Sw patchList on each node. If the Sw patchList update is successful, it activates the new patch. If the Sw patchList update is not successful, the Auto-Patch tool does not retry.

Auto-Patch failures that require user intervention are logged. You can apply the failed patches manually.

See “Auto-patch application process flow” (page 532).

Figure 51
Auto-patch application process flow



Configuring the auto-patch process

The command to configure the auto-patch process has the following syntax:

```
ppautopatch (-download -host <sds host name> -huser
<sds host userid> <sds host password>)
```

and, or

```
(-apply [-log_verbose])

-nodes <group> | <node> | <filename>

-nuser <node userid> <node password>

[-max_duration <n> h | m]

[-successfile <filename>]

[-failedfile < filename]
```

where:

-download selects the patch download operation **-apply** selects the patch apply operation. You must select at least one operation or both.

-host is the IP address of the SDS

-huser is the authentication user ID and password required to connect to the SDS

-nodes is one or more Passport nodes. You can enter a node name, a group of nodes, or a list of nodes that is stored in a file. Any node or group name must be configured in HGDS. The list of names must be carriage return delimited. The filename can be either the name of an actual file or the default keyword filename, LATEST_<SUCCESS | FAILED_<DL | PATCH>. If you use the keyword filename, then the -successfile filename must be in /opt/MagellanNMS/data/ppautopatch.

-nuser is the authentication user ID and password required to connect to the node(s). The user ID permissions must have a user scope of network and a user impact of debug, administration, or configuration.The password may either be stored in the clear or be the name for a file that contains an encrypted password.

-max_duration defines the maximum time for the Auto-Patch tool to complete the patch download and, or application operations on each node. You can enter the time in hours from 1 - 23 or in minutes from 1 - 1439.

-successfile is an option that lets you identify a file other than the default file to store the names of all of the nodes where the Auto-Patch tool successfully performed the download and, or apply operations. You can use this option with the -nodes parameter to record successful downloaded and applied patches or for customer auditing purposes. If you do not use this option, the names of the nodes will be stored in /opt/

MagellanNMS/data/ppautopatch/<filename>. The filename will include the date, operation requested, nodes variable, and an incrementing index <N> to ensure the filename remains unique, as follows:

<YYYYMMDD>_SUCCESS_<DL | APPLY>.<NODES>.<N>.hosts

-failedfile is an option that lets you identify a file other than the default file to store the names of all of the nodes where the Auto-Patch tool unsuccessfully performed the download and, or apply operations. You can use this option with the -nodes parameter to record successful downloaded and applied patches or for customer auditing purposes. If you do not use this option, the names of the nodes will be stored in /opt/MagellanNMS/data/ppautopatch/<filename>. The filename will include the date, operation requested, nodes variable, and an incrementing index <N> to ensure the filename remains unique, as follows:

<YYYYMMDD>_FAILED_<DL | APPLY>.<NODES>.<N>.hosts

-log_verbose is an optional operation that you can select to include the output of the patch query that is run by the Auto-Patch tool. The output includes the state of all patches and the software patchlist for every node. The operation will run before the download and apply operations. If you do not select this operation, the patches that require manual intervention are output by default. This includes patches that have been declared obsolete, patches with an emergency removal notice or defect, and patches which are service affecting.

ATTENTION	The -log_verbose operation output is large and can quickly fill disk space. You must monitor disk utilization carefully and perform the appropriate disk management procedures. See “Disk management” (page 535).

Auto-patching process control

You can prevent the scheduled auto-patching operations or halt an operation in progress using the following command:

```
touch /opt/MagellanNMS/cfg/private/noppautopatchrun
```

Once the command is executed, you must delete the *noppautopatchrun* file before the next scheduled auto-patch operation(s).

ATTENTION	If the *noppautopatch* file is present when the next scheduled operation begins, the operation will abort with an alarm and a log.

Disk management

A process called *mdmlogclean* can be used to clean up the temporary successful and failed files as well as the optional verbose logfiles. The cleanup is controlled by a configuration file called MDMClean.cfg which contains records that define which directory the *mdmlogclean* process examines and the length of time the files can accumulate in the directory.

To use the *mdmlogclean* process to manage the disks which accumulate the auto-patching log files, you must populate the MDMClean.cfg file in the opt/MagellanNMS/cfg directory with the following:

```
Directory: /opt/MagellanNMS/data/ppautopatch

RetentionDays: <number of days>

Directory: opt/MagellanNMS/data/log/ppautopatch

RetentionDays: <number of days>
```

You can then run the *mdmlogclean* process with the -file option, as follows:

```
/opt/MagellanNMS/bin/mdmlogclean -file /opt/
MagellanNMS/cfg/MDMClean.cfg
```

Error logs

The auto-patching process can result in errors that require user intervention. In these cases, the Auto-Patching tool issues an alarm and log to the OAM Collector. In a large network, only summary alarms are issued to prevent operator overload.

Some of the error conditions are as follows:

- noppautopatchrun file exists
- node specified in -nodes does not exist in HGDS
- incorrect authentication

- HGDS server unavailable
- unreadable nodelist input files

If a scheduled patch download or activation fails on any node, an error alarm will be issued with a detailed log file for troubleshooting. Errors that are logged include:

- process starting and stopping
- connection errors
- process exit status
- write errors to output nodelist file
- corrupt nodelist entries
- insufficient user scope or impact

The error are logged in the following location:

```
/opt/MagellanNMS/data/log/ppautopatch/
ppautopatch_YYYYMMDD>.nlog
```

See “Log record attributes” (page 536).

Table 10
Log record attributes

Attribute	Description
Date	The time the event is recorded, in ISO format.
Source	The source address of the event in fully qualified domain name (FQDN) format.
Process	The name of the software process running on the workstation that triggered the log. The format is *ppautopatch:<pid>* where pid is the process ID.
SRC_USR	The user ID logged into the workstation when the log is generated or another software process.
STAT	The status of the event shown as one of the values: {start, end, success, failure}

(Sheet 1 of 2)

Table 10
Log record attributes

Attribute	Description
MSG_TXT	A text message that describes the event.
LEVEL	The severity level of the event. (Fatal, Alert, Critical, Error, Warning, Cleared, Notice, Info, Debug, or Trace.)
LOGGER	The logger instance that generated the log message within the process.
LOG_TYPE	The type of log generated. For the auto-patch processes, the value is always *application*.
(Sheet 2 of 2)	

Optional verbose logs

If you have selected the -log_verbose operation, the logs containing the output from the *run -q sw* command are stored in /opt/MagellanNMS/data/log/ppautopatch. For each log instance a new file is created. The filename format is:

```
ppautopatch_<YYYYMMDD>T<HHMMSS.ss>.status
```

Each entry in the file will have a header indicating the time and node name.

Appendix A
MDM log files

This appendix describes the log files generated by the Preside Multiservice Data Manager (MDM) tools and the logs stored in them.

Information about logs produced by the MDM servers is not contained in this appendix. For information about the logs produced by each server, see information about each of the servers in 241-6001-310 *Preside MDM Server Reference Guide*.

See the following section for information on how this appendix is organized:

- "How log information is arranged in this appendix" (page 540)

This appendix contains information about logs from the following sets of tools:

- "DPN Component Provisioning" (page 541)
- "DPN Data Collector" (page 542)
- "DPN Global Data Manager" (page 542)
- "DPN MCF Management" (page 543)
- "DPN NRS Populator" (page 545)
- "DPN NRS Automatic Populator" (page 545)
- "DPN NRS PM Lister" (page 545)
- "DPN NRS/NCD Population Manager" (page 546)
- "DPN Service Data Conversion" (page 547)

How log information is arranged in this appendix

For each log file, this appendix provides the following information:

- Log file name: the name of the file in which log information is written. This information also indicates whether the file name is fixed, is settable, and if a default filename exists.
- Generated by: the name of the process that generates the logs
- Activation method: the method by which the logs are generated; automatic or selectable. Automatic means that the log file is always generated automatically by the server or tool that creates it. Selectable means that you can turn on or turn off generation of the log, if you choose to do so. If generation of the log file is selectable, this information explains how log generation can be activated.
- Contents: the purpose of the logs in the log file

- Mandatory or optional: the requirement to keep the log file. Mandatory means that the log file should not be erased because removing it may have an effect on the operation of a tool. Optional means that you can delete the file. This information also includes hints about when to delete the file and whether the system software is to delete them automatically.

  If disk space is an issue, the optional log files can be erased. If you plan to erase the log files, we suggest that you consider backing them up on tape before erasing them.

  Note: If a tool is not listed in this appendix, this means that there are no log files associated with the tool.

DPN Component Provisioning

Component Provisioning logs are saved in the following file:

- Log file name: any user-defined name in any directory. The name of the log file is specified from File Upload Preferences Dialog. If a filename is entered, and not a full pathname the user's home directory is used as the default directory for the file.
- Generated by: the pui process
- Activation method: selectable. Log file generation is activated by selecting Propagation Logging in the File Upload Preferences Dialog
- Contents: a history of a component provisioning session. The contents of this log file can be modified and used in a Provisioning API session.
- Mandatory or optional: optional

DPN Data Collector

DPN Data Collector logs are saved in the following file:

- Log file: /opt/MagellanNMS/data/model/cdf/<collection name>/<filename>

  where:

  <collection_name> specifies the type of data collection entered when using the Data Collection tool.

  <filename> is one of files comp.nidf, link.nidf, or module.nidf that are generated automatically while data collection is taking place, or one of files mcdf.log or instance.nidf that exist after the data collection is completed

- Generated by: the dpnmcdf process
- Activation method: automatic, by the dpnmcdf and autocollect utilities. You can run these utilities manually from the command line or from the Network Viewer Editor.
- Contents: a record of the modules and subcomponents that are being queried by the DPN Data Collector and errors encountered during the data collection.
- Mandatory or optional: optional. Files comp.nidf, link.nidf, or module.nidf are removed automatically, unless the mcdf process is killed or terminates abnormally. Files mcdf.log or instance.nidf are not removed automatically unless the data collection is tagged to be removed upon completion by means of the Network Viewer Editor. It is recommended that you periodically remove the entire set of files from the /opt/MagellanNMS/data/model/cdf/<collection name>/<filename>.

DPN Global Data Manager

DPN Global Data Manager graphical user interface logs are saved in the following file:

- Default log file name: $HOME/MagellanNMS/gdm.log
- Generated by: the rdpui process

- Activation method: selectable. Logs can be activated from the main window of the tool.
- Contents: error, warning, and information messages
- Mandatory or optional: optional

DPN Global Data Manager command line interface logs are saved in the following file:

- Default log file name: ./gdm.log
- Generated by: the gdm process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error warning and information messages
- Mandatory or optional: optional

DPN MCF Management

Logs from the deletion of specific MCFs on the PM disk are saved in the following file:

- Default log file name: ./pmdeletemcf.log
- Generated by: the pmdeletemcf process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning, and information messages
- Mandatory or optional: optional

Logs from tidying the PM disk by deleting MCFs are saved in the following file:

- Default log file name: ./pmtidymcf.log

- Generated by: the pmtidymcf process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning, and information messages
- Mandatory or optional: optional

Logs from the deletion of backup MCFs are saved in the following file:

- Default log file name: ./bddeletemcf.log
- Generated by: the bddeletemcf process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning and information messages
- Mandatory or optional: optional

Logs from the tidying of backup MCFs are saved in the following file:

- Default log file name: ./bdtidymcf.log
- Generated by: the bdtidymcf process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning and information messages
- Mandatory or optional: optional

DPN NRS Populator

DPN NRS Populator command line interface logs are saved in the following file:

- Default log file name: ./nrspop.log
- Generated by: the nsrpop process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning, and information messages
- Mandatory or optional: optional

DPN NRS Automatic Populator

DPN NRS automatic populator command line interface logs are saved in the following file:

- Default log file name: ./nrsauto.log
- Generated by: the nrsauto process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning, and information messages, and information about the files are uploaded, a timestamp associated with the upload, success or failure of each upload, and errors encountered
- Mandatory or optional: optional

DPN NRS PM Lister

DPN NRS PM Lister command line interface logs are saved in the following file:

- Default log file name: ./nrspmlist.log

- Generated by: the nrspmlist process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter, no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning, and information messages
- Mandatory or optional: optional

DPN NRS/NCD Population Manager

A number of log files are generated by the DPN NRS Population Manager. The tool starts the popmgr process.

When the popmgr process runs, it creates a master log file in the data directory specified in the population manager configuration file by variable POP_MGR_DATA_DIR.

The name of this master log file is defined by entering the -log <logfilename> on the command line of the tool. If you do not specify the <logfilename> parameter, the name popmgr.log is used by default.

The tool also calls a number of other processes (mcflist, nrspop, nrslist, ncdpop) each of which creates its own instance files in the working directory specified in the population manager configuration file by variable POP_MGR_WORK_DIR. These instance files are:

- mcflist.log.<number of instance>
- nrslist.log.<number of instance>
- ncdpop.log.<number of instance>
- nrspop.log.<number of instance>

These files are cleaned out from the working directory if the popmgr process runs successfully.

If the popmgr process fails, all of the instances files are merged into the master log file (default popmgr.log).

If either or both nrspop or ncdpop fail while running under the control of the popmgr process, log files popmgr.nrspop.<time>.log and/or popmgr.ncdop.<time>.log respectively are created in the directory specified by variable POP_MGR_WORK_DIR.

DPN Service Data Conversion

DPN Service Data Conversion graphical user interface logs are saved in the following file:

- Default log file name: $HOME/MagellanNMS/sdconv.log
- Generated by: the sdcui process
- Activation method: selectable. Logs can be activated from the main window of the tool.
- Contents: error, warning, and information messages
- Mandatory or optional: optional

DPN Service Data Conversion command line interface logs are saved in the following file:

- Default log file name: ./sdconv.log
- Generated by: the sdconv process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning, and information messages
- Mandatory or optional: optional

DPN Software Distribution

DPN Software Distribution graphical user interface logs are saved in the following file:

- Default log file name: $HOME/MagellanNMS/getimg.log
- Generated by: the swdui process

- Activation method: selectable. Logs can be activated from the main window of the tool.
- Contents: error, warning, and information messages
- Mandatory or optional: optional

DPN Software Distribution command line interface logs are saved in the following file:

- Default log file name: ./getimg.log
- Generated by: the getimg process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning and information messages
- Mandatory or optional: optional

DPN Software Substitution

DPN Software Substitution graphical user interface logs are saved in the following file:

- Default log file name: $HOME/MagellanNMS/upgradeimg.log
- Generated by: the swsui process
- Activation method: automatic
- Contents: error, warning, and information messages
- Mandatory or optional: optional

DPN Software Substitution command line interface logs are saved in the following file:

- Default log file name:. /upgradeimg.log
- Generated by: the upgradimg process
- Activation method: automatic

- Contents: error, warning, and information messages
- Mandatory or optional: optional

Shared Java Virtual Machine

Shared Java virtual machine (JVM) logs are saved in the following file:

- Default log file: /opt/MagellanNMS/data/log/mft/Desktop/GUI_1<some_ID>log

  where:

  <some_ID> is the actual timestamp; it is the difference, measured in milliseconds, between the current time and midnight, January 1, 1979 UTC.

- Generated by: every time a shared JVM is started
- Activation method: automatic
- Contents: information message on whether the launch was successful, and if not what caused the exception
- Mandatory or optional: mandatory

Network Configuration Database

Network Configuration Database (NCD) Server logs are saved in the following file:

- Default log file: ./ncdsvr.<target_NCD>.log

  where:

  <target_NCD> is the name of the database for the NCD Server to be started.

- Generated by: the ncdsvr server daemon
- Activation method: selectable. Logs can be activated by entering the NCD server startup command with the-log [<logfilename>] parameter. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.

- Contents: error, warning and information messages
- Mandatory or optional: optional

Network Configuration Database Populator logs are as follows:

- Default log file: ./ncdpop.<target_ncd>.<YYMMDDhhmmss>.log

  where:

  <target_NCD> is the name of the database for the NCD Server to be started.

  <YYMMDDhhmmss> is a timestamp that indicates when the log file was created

- Generated by: the ncdpop process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning and information messages
- Mandatory or optional: optional

Network Viewer

Network Viewer logs are saved in the following file:

- Default log file: /opt/MagellanNMS/data/nvs/views
- Generated by: the nv process
- Activation method: optional, by selecting Save view or Save View as... from the Network Viewer
- Contents: information about the organizational structure of the network that is currently open with the Network Viewer
- Mandatory or optional: optional

Workstation Surveillance

Preside Multiservice Data Manager (MDM) workstation surveillance provides a runtime log in the following file:

/opt/MagellanNMS/data/log/sfm.log

This log is created after running the sfm_config script, which is found in /opt/MagellanNMS/bin.

- Default log file: /opt/MagellanNMS/data/wfs.run.log
- Generated by: sfm process
- Activation method: automatic
- Contents: alarms generated through the sfm process
- Mandatory or optional: mandatory

You can check this log to identify runtime errors that are generated by the workstation surveillance process (sfm). If the MDM process is dead, all alarms generated by the sfm process appear in this runtime log file.

NRS

See also, "Passport NRS Populator" and all headings beginning with DPN NRS. The first of these is "DPN NRS Populator" (page 545).

NRS Differences Report

NRS Differences Report command line interface logs are saved in the following file:

- Default log file name: ./nrsdiff.log
- Generated by: the nrsdiff process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: a trace for a run of the nrsdiff program
- Mandatory or optional: optional

Passport NRS Populator

Passport NRS Populator command line interface logs are saved in the following file:

- Default log file name: ./pnrspop.log
- Generated by: the pnrspop process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error, warning, and information messages
- Mandatory or optional: optional

Passport Software Distribution

Passport Software Distribution command line interface logs are saved in the following file:

- Default log file name: ./fsdl.log
- Generated by: the fsdl process
- Activation method: selectable. Logs can be activated by entering the -log [<logfilename>] parameter at the command line interface. If you do not enter the -log parameter no log file is produced. If you enter the -log parameter without the <logfilename> argument, the default log file name is used.
- Contents: error warning an information messages
- Mandatory or optional: optional

DPN Performance Viewer

DPN Performance Viewer logs are saved in the following file:

- Log file: The log file for the DPN Performance Viewer can be any user-defined name in any directory. The name of the log file is set by selecting Log to File from the DPN Performance Viewer and specifying a filename or a full pathname. If a just the filename is entered (not the full pathname), the user's home directory is used as the default.
- Generated by: the pv process
- Activation method: optional, by selecting Log to file from the DPN Performance Viewer
- Contents: statistics for the components that re currently displayed with the DPN Performance Viewer
- Mandatory or optional: optional

Server Administration

Error logs are saved in the following file:

- Log file: /opt/MagellanNMS/data/SVM/SVM.errors
- Generated by: the svmdmn process
- Activation method: automatic
- Contents: a timestamped list of messages resulting from system errors
- Mandatory or optional: optional.

  Use the Server Administration tool to verify that there is no start, stop, or restart activity occurring before deleting this log file.

Activity logs are as follows:

- Log file: /opt/MagellanNMS/data/SVM/SVM.log
- Generated by: the svmdmn process
- Activation method: automatic
- Contents: a timestamped list of Server ADministration daemon activity. All starts, stops, changes, additions, and deletions are recorded in this file.

- Mandatory or optional: optional

  Use the Server Administration tool to verify that there is no start, stop, or restart activity occurring before deleting this log file.

Service Integrity Audit

Service Integrity Audit command line interface logs are saved in the following file:

- Log file name: sisauto.<date>.log

  where:

  <date> is in the format <yyymmddhhmmss>.

  This log file is stored in the directory specified by variable SIS_DATA_DIR as set in file SIS.cfg.

- Generated by: the sisauto process and processes called by sisauto
- Activation method: automatic
- Contents: error, warning and information messages
- Mandatory or optional: optional. This file is cleaned up automatically at the interval specified by variable SIS_OUTPUT_FILES_KEEP_COUNT in file SIS.cfg. You can however, delete the file at any time.

SunLink Frame Relay

SunLink Frame Relay maintains tracking information in the following log file:

- Log file name: /var/opt/SUNWconn/fr.log

  This log file is created at boot time when the Frame Relay service is started (by /etc/init.d/fr.control).

- Activation method: automatic
- Contents: tracking information for Frame Relay circuits and processes
- Mandatory or optional: mandatory

- Clean up: As root, enter the following command to truncate the file:

  ```
  cp /dev/null /var/opt/SUNWconn/fr.log
  ```

For more information about cleanup of SunLink Frame Relay and this command, refer to the SunLink Frame Relay documentation.

Start Logs for CDE

Starting a user session in CDE creates the following log file:

- Log file name:

  /$HOME/.dt/startlog

  If there is startlog file from the previous session, it is renamed to startlog.old. before new startlog file is opened. Similarly, if there is already a startlog.old file, it is renamed to startlog.older. Log files for a maximum of three sessions are kept: startlog, startlog.old, and startlog.older. Whenever you start a tool during a session, information is written to the current startlog file.

- Activation method: remove the # symbol in the .dtprofile file in your home directory.
- Contents: lists of the tools that were started and error messages.
- Mandatory or optional: Optional
- Clean up: Have user log in, delete the current files, then modify file $HOME/.dtprofile to elminate generation and population of log files.

Appendix B
Configuring the OA groups with the oa.config program

This appendix describes how to create a new OA member and to add an existing OA member to a new group.

> ***Note:*** Nortel Networks recommends that the Host Group Administration tool be used to update the Host Group Directory Server configuration file /opt/MagellanNMS/cfg/HGDS.cfg. For more information, see "You are now ready to create OA groups. See "Defining the OA groups and OA members" (page 108)." (page 107).

You must create a new OA member at least once before you can add an existing OA member to a new group. You only need to add an existing OA member to a new group for an OA that needs to belong to more than one group.

Both procedures run script /opt/MagellanNMS/bin/oa.config to define an OA group and its members for DPN network access or for DPN surveillance. The script writes the information into file /opt/MagellanNMS/cfg/HGDS.cfg. Running the script in prompt mode gives you prompts for each parameter. You can run the script in no-prompt mode, and enter all the parameters in one line. The following procedures run the script in no-prompt mode.

Creating an OA member with the oa.config script

Use the following procedure to create a new OA member and add it to a group. Because the script only defines one member of a group at a time, you must run the script for each OA that is to be a member of the group.

1 Read “Planning OA groups” (page 94).

2 Log in as root.

Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in “Setting up the root account to run MDM software” (page 62).

3 Run the oa.config script in no-prompt mode to define the first OA in the group:

```
/opt/MagellanNMS/bin/oa.config \
[<group name> <WS-MDI name> [<OA name> \
[<WS-MDI DNA> <CUG> <Pkt Size> \
[<X75:Y or N> [<RPOA>]]]]]
```

Note: To run the script in prompt mode, enter: /opt/MagellanNMS/bin/oa.config

where:

`<group name>`

is the name of the group of OAs to which the OA belongs. The group name is an uppercase string of 1 to 12 characters.

If the group does not already exist a new group is created. The group name must be unique on this workstation. If the group name consists of more than one word, join the words by underscore characters; for example SURV_G1.

If you wish to gather alarms and surveillance information automatically from your network, you must create at least one special OA group called a surveillance group whose OAs are dedicated to gathering surveillance information.

Examples:

name of an OA group for network access: ALLOAS

name of a surveillance group: SURV_G1

`<WS-MDI name>`

is the name used to identify the connection to the Workstation Management Data Interface (WS_MDI) on the Operations Agent (OA) to which the workstation is connected. An OA can have multiple connections; the WS-MDI name identifies which one of the connections is involved. The WS-MDI name is also known as the OA member name.

If no other parameters are specified after this parameter, the command adds an existing OA to another group.

The WS-MDI name is a combination of up to 12 alphanumeric characters that begins with a letter.The WS-MDI name must be unique on this workstation.

<OA name>

is the name of the Operations Agent (OA) on which the WS-MDI is located.

The OA name is a mnemonic consisting of up to 12 alpahnumeric characters. Obtain this OA name from the DPN system administrator.

<WS-MDI DNA>

is the Data Network Address (DNA) used to access the WS-MDI. The WS-MDI DNA is a valid DNA for the WS-MDI consisting of up to 15 digits. Obtain this DNA from the DPN system administrator.

<CUG>

is the index number of the Closed User Group (CUG) to which the WS-MDI belongs. The CUGs a valid two-digit CUG index. Obtain the CUG index from your DPN system administrator.

<Pkt Size>

is the default size of data packets transmitted between the Preside Multiservice Data Manager (MDM) workstation and the WS-MDI. The Pkt Size is one of: 128, 256, or 512. The default is 256.

<X75:Y or N>

indicates whether the connection between the workstation and the OA passes through an X.75 link. X.75 links are used to interconnect two packet network, either public or private.

Valid entries are Y or N. If you omit this parameter, a default of N is assumed.

<RPOA>

is used to identify the Recognized Private Operating Agency (RPOA) that owns the X.75 link to the WS-MDI. Enter this parameter only if you specify Y for parameter <X75: Y or N>.The RPOA number is a four-digit number that is unique for all network and is often used for reverse charging purposes.

The script displays a response indicating that the group has been created.

4 Repeat step 3 once for each other member of the group using the same group name. Do this until you have added all OAs to the group.

5 Using the Server Administration tool, restart the NCSMGR server and the DMDR servers for any surveillance groups that you created, or modified.

See "Adding a new server" (page 367).

If you have an OA that belongs to more than one OA group, add the existing OA to the new group, as described in "Adding an existing OA to a new group with the oa.config script" (page 561). If not, configure and start the servers, as described in "Example" (page 562).

Example

The following example describes how to create an OA group called SURV_G1, which is dedicated to gathering surveillance information. This group contains two members whose WS-MDI names are OAM_1 and OAM_2. OAM_1 and OAM_2 feed into OAs called WEST_OA and EAST_OA, with DNAs 123456 and 123457, CUG indexes of 02, and a default packet size of 256 bytes for transmission purposes. The connection between the workstation and the OAs does not pass through an X.75 link.

1 Create the first member of the group:

```
/opt/MagellanNMS/bin/oa.config SURV_G1 OAM_1 WEST_OA \
123456 02 256
```

The script responds with

```
Configuring OA MDI "OAM_1" for OA "WEST_OA" in group
"SURV_G1" using DNA 123456 (CUG02), Packet Size 256,
disallowing X.75 calls.
```

2 Create the second member of the group:

```
/opt/MagellanNMS/bin/oa.config SURV_G1 OAM_2 \
EAST_OA 123457 02 256
```

The script responds with

```
Configuring OA MDI "OAM_2" for OA "EAST_OA" in group
"SURV_G1" using DNA 123457 (CUG02), Packet Size 256,
disallowing X.75 calls.
```

Group SURV_G1 is created with the two members OAM_1 and OAM_2.

Adding an existing OA to a new group with the oa.config script

Use the following procedure to add an existing OA to a new group. Before performing this procedure you must have already created the new member according to the instructions in "Adding an existing OA to a new group with the oa.config script" (page 561).

1 Log in as root.

Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in "Setting up the root account to run MDM software" (page 62).

2 Run the oa.config script in no-prompt mode to add the existing OA to the new group:

```
/opt/MagellanNMS/bin/oa.config \
<group name> <WS-MDI name>
```

where:

`<group name>`

is the name of the group of OAs to which the OA belongs. If the group does not exist, the script creates it for you.

`<WS-MDI name>`

is the name used to identify the connection on the Workstation Management Data Interface (WS_MDI) on the Operations Agent (OA) to which the workstation is connected.

The script response indicates that the group is created.

3 Repeat step 3 for each other member of the group using the same group name. Do this until you have added all existing OAs to the group.

4 Using the Server Administration tool, restart the NCSMGR server and the DMDR servers for any surveillance groups that you have created, or modified.

See "Adding a new server" (page 367).

You are now ready to configure and start the servers. See "Example" (page 562).

Example

The following is an example of adding an existing OA member to a surveillance group called SURV_G2. The WS-MDI name is OAM_1, and the OA name is WEST_OA. Because the group does not exist, the *oa.config* script creates the group.

Enter the following command:

```
/opt/MagellanNMS/bin/oa.config SURV_G2 OAM_1
```

The script responds with

```
Configuring OA MDI "OAM_1" for OA "WEST_OA" in group
"SURV_G2".Using DNA 123456 (CUG 02), Packet Size
256,disallowing X.75 calls.
```

Group SURV_G2 is created and includes existing OA member, OAM_1.

Appendix C
Defining Passport hosts and groups with the passport.config script

Note: Nortel Networks recommends that the Host Group Administration tool be used to update the Host Group Directory Server configuration file /opt/MagellanNMS/cfg/HGDS.cfg. For more information, see "Defining the groups and hosts" (page 141).

Use the procedures in this section to configure Passport hosts and groups in networks that

- contain a mix of DPN and Passport nodes, and the Preside Multiservice Data Manager workstation connects to the network by an IP connecting running on an X.25 switches virtual circuit to a DPN node that acts as a gateway to Passport nodes in the network
- contain Passport nodes only that are set up in an Integrated LAN Switching (ILS) configuration

You must be logged in as root to run the passport.config script.

You can use the passport.config script to perform the following functions:

- add a new node to an existing Passport group or to a new group
- add an existing node to an existing group or to a new group

You cannot use passport.config by itself to perform the following functions:

- specify the X.121 address and the CUG for an IP over SVC on an X.25 connection. You must do this using Sun's SunLink X.25 configuration tool.

- delete a node from an existing group
- move node to another group
- modify the IP address of a node

There are two ways to run the passport.config script: in prompt mode and in no-prompt mode.

In prompt mode, the script prompts for the parameters that define a node as a member of a group and prompts you for permission to run the passport.kick script. The passport.kick script updates the HGDS, FDTM, and FMDR servers with information about the new node without having to restart the servers with the Server Administration tool.

In no-prompt mode, the script lets you enter all of the parameters on one line, but only reminds you to run the passport.kick script to update the servers using the passport.kick script. It does not provide the ability to run the script.

The passport.config script requires the following information as inputs which it uses to populate file /opt/MagellanNMS/cfg/HGDS.cfg:

- the name of the group which the node belongs
- the host name of the node
- the IP address of the node

This section contains the following procedures:

- "Adding nodes to a group using passport.config in no-prompt mode" (page 565)
- "Example: Adding nodes to a group using passport.config in no-prompt mode" (page 566)
- "Adding nodes to a group using passport.config in no-prompt mode" (page 565)
- "Example: Adding nodes to a group using passport.config in prompt mode" (page 568)

Adding nodes to a group using passport.config in no-prompt mode

Use this procedure to add Passport nodes to a new group or to an existing group using passport.config in no-prompt mode.

1 Log on as root.

Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in “Setting up the root account to run MDM software” (page 62).

2 Run the passport.config script in no-prompt mode using the following command syntax:

```
/opt/MagellanNMS/bin/passport.config <group_name>\
<host_name> [<IP_address>]
```

where:

`group name` is the name of the group to which the node belongs consisting of an uppercase string of from 1 to 12 characters.If the group does not already exist, the script creates a new group for you.

The group name must be unique on the workstation. If the group name consists of more than one word, join the words by underscore characters; for example SURV_G1.

If you wish to gather alarms and surveillance information automatically from your network, you should create at least one special group called a surveillance group that is dedicated to gathering surveillance information.

Examples:

name of a group used for provisioning and troubleshooting: FMGROUP

name of a surveillance group: FG_1

Note: Do not use the name of a node as the name of a surveillance group. Doing so may cause confusion in identifying what you are logged in to when using the Command Console.

`host name` is the name of the node. The host name is an uppercase character string consisting of from 1 to 12 characters, as stored in the service data of node. Example: host1

`IP address` is the IP address of the node. The IP address must be a valid node address consisting of four numbers from 1 to 3 digits, separated by periods. Omit this parameter if you are adding an existing node to an existing group or to a new group. Example: 10.0.0.3

The script displays responses indicating that the group has been created and reminds you to run the passport.kick script.

3 Repeat step 2 once for each node that you are adding to the group.

4 Update the HGDS, FDTM, and FDTR servers with the new information by running the passport.kick script.

/opt/MagellanNMS/bin/passport.kick

Messages appear indicating that the servers are being updated with the modified group information.

5 Watch the System Log Display tool for possible warnings about syntax errors and failures of the HGDS, FDTM, and FDTR servers. Alternatively, launch the Server Administration tool and examine information displayed about the HGDS, FDTM, and FDTR servers to ensure that they are still running.

Example: Adding nodes to a group using passport.config in no-prompt mode

The following example shows the use of the passport.config script in no-prompt mode to add two new Passport nodes called OAK and MAPLE to a new group called TREES_1. The IP addresses of OAK and MAPLE are 1.2.3.4 and 1.2.3.5 respectively.

1 Add node OAK to group TREES_1:

/opt/MagellanNMS/bin/passport.config TREES_1 OAK \ 1.2.3.4

The script responds with the following:

```
Configuring Passport host "OAK" in group "TREES_1" with
IP address 1.2.3.4.

The Host Group Server configuration file has been
modified. Please signal the related servers with the
passport.kick script or restart them from the SVM
Administration tool

All appropriate files have been modified.
```

2 Add MAPLE to the same group:

/opt/MagellanNMS/bin/passport.config TREES MAPLE \ 1.2.3.5

The script responds with:

```
Configuring Passport host "MAPLE" in group "TREES_1"
with IP address 1.2.3.5.

The Host Group Server configuration file has been
modified. Please signal the related servers with the
passport.kick script or restart them from the Server
Administration tool

All appropriate files have been modified.
```

3 Run the passport.kick script:

/opt/MagellaNMS.bin/passport.kick

The script displays responses indicating that the HGDS, FDTM, and FMDR servers are being updated.

Adding nodes to a group using passport.config in prompt mode

Use this procedure to add Passport nodes to a new group or to an existing group using passport.config in prompt mode.

1 Log in as root.

Note: The root account must be set up to run Preside Multiservice Data Manager (MDM) software as described in "Setting up the root account to run MDM software" (page 62).

2 Start the passport.config script in prompt mode using the following command syntax:

The passport.config script displays the following prompt.

```
/opt/MagellanNMS/bin/passport.config

Please specify a group name for the new host:
```

3 Enter the group name. The group name is the name of the group to which the node belongs.

```
Please specify a name for the new host:
```

4 Enter the host name for the node.

```
Please specify an IP address for the new host
(or just return for none):
```

5 If you are adding a new node to a new group or to an existing group, enter the IP address.

If you are adding an existing node to an existing group or to a new group, press the return key to omit this parameter.

The script displays a response indicating that the group has been created, then displays the following prompt:

```
The Host Group server configuration file has been
modified. Please signal the related servers with the
passport.kick script or restart them from the Server
Administration tool

Do you want to run passport.kick and signal the
related MDM servers to reload the HGDS configuration
now (y/n)?
```

6 If you have finished adding nodes to the group, go to step 7.

If you have more nodes to add, go back to step 2.

7 Run passport.kick by entering Y.

Messages are displayed indicating that the servers are being updated with the modified group information, followed by the response: Done

8 Watch the System Log Display tool for possible warnings about syntax errors and failures of the HGDS, FDTM, and FDTR servers. Alternatively, launch the Server Administration tool and examine information displayed about the HGDS, FDTM, and FDTR servers to ensure that they are still running.

Example: Adding nodes to a group using passport.config in prompt mode

The following example shows the use of the passport.config script in prompt mode to add two new Passport nodes called PINE and SPRUCE to a new group called TREES_2. Nodes PINE and SPRUCE have IP addresses 1.2.3.6 and 1.2.3.7 respectively.

1 Add member PINE to group TREES_2:

`/opt/MagellanNMS/bin/passport.config`

The script responds with:

```
Please specify a group name for the new host: TREES_2

Please specify a name of the new host: PINE

Please specify an IP address for the new host
or just return for none): 1.2.3.6
```

```
Configuring Passport host "PINE" in group "TREES_2"
with IP address 1.2.3.6.

The Host Group Server configuration file has been
modified. Please signal the related servers with the
passport.kick script or restart them from the Server
Administration tool.

Do you want to run passport.kick and signal the related
MDM servers to reload the HGDS configuration now (y/
n)?: N

All appropriate files have been modified.
```

2 Add group:

/opt/MagellanNMS/bin/passport.config

The script responds with:

```
Please specify a group name for the new host: TREES_2

Please specify a name of the new host: SPRUCE

Please specify an IP address for the new host
or just return for none): 1.2.3.7

Configuring Passport host "SPRUCE" in group "TREES_2"
with IP address 1.2.3.7.

The Host Group Server configuration file has been
modified. Please signal the related servers with the
passport.kick script or restart them from the Server
Administration tool.

Do you want to run passport.kick and signal the related
MDM servers to reload the HGDS configuration now (y/
n)?: Y
```

The script displays responses indicating that the HGDS, FDTM, and FMDR servers are being updated, followed by the responses:

```
Done
All appropriate files have been modified.
```

Index

G

L

M

N

O

P

R

S

T

U

V

W

X

Preside Multiservice Data Manager
Administrator Guide

R15.1

Publication: 241-6001-303
Document status: Standard
Document version: 15.1RSUP
Document date: August 2004
Printed in Canada

NORTEL NETWORKS