NORTEL NETWORKS

Preside Multiservice Data Manager

Device Adapter Installation and Administration

User Guide

241-6001-121

Preside Multiservice Data Manager

Device Adapter Installation and Administration

User Guide

Publication: 241-6001-121
Document status: Standard
Document version: 14.3RSUP
Document date: December 2003

Printed in Canada

Publication history

December 2003

14.3RSUP Standard
Commercial availability.

Contents

About this document

This document contains instructions to plan, install, and administer the Preside Multiservice Data Manager (MDM) Device Adapter software. The MDM Device Adapter software provides Preside Applications Platform tools with fault information from devices managed by MDM software. The following topics are discussed in this section:

Who should read this document and why

This document is intended for experienced network operators who require fault information for Preside Applications Platforms. Personnel responsible for installing and maintaining MDM Device Adapter software will require this information.

What you need to know

To use this document, you need the following skills and training:

- working experience or training in the administration of SUN workstations and the Solaris operating system
- experience or training with the Preside Multiservice Data Manager (MDM)
- training courses for Passport and DPN-100

How this document is organized

This document contains the following sections:

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.

- `[optional_parameter]`

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

- `<general_term>`

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

- UPPERCASE, lowercase

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

- |

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

- ...

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

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

Related documents

This document references the following Nortel Networks technical publications (NTP) and other documentation:

- Preside Applications Platform, 9.1 Installation and Administration Guide, 450-3101-201
- 241-6001-011 *Preside MDM Fault Management User Guide*
- 241-6001-100 *Preside MDM Installer Guide*
- 241-6001-109 *Preside MDM Passport 4400 Integration Guide*
- 241-6001-303 *Preside MDM Administrator Guide*
- 241-6001-310 *Preside MDM Server Reference Guide*
- 241-7001-150 *Passport Operations and Maintenance Guide*

Chapter 1
MDM Device adapter

This section contains information about the following topics:

Understanding the Preside MDM Device Adapter

The Preside Multiservice Data Manager (MDM) Device Adapter software provides Preside Applications Platform tools, such as the graphical network browser (GNB), with fault information from devices that are managed with Preside MDM software. You can use the MDM Device Adapter software to obtain fault information from the following devices:

- Passport 4120, 4400, 6420, 6440, 6480,7480, 8780, and 15000
- DPN-100

You need three bundles of software to obtain fault information from these devices:

- the MDM software, which provides an element manager for the devices
- the MDM Device Adapter software, which provides an interface between the MDM software and the Preside applications

- the Preside Applications Platform software, which has an interface to the MDM Device Adapter software, and provides a set of applications and tools for correlating and displaying the fault information

MDM software

The following sections explain the functions of server processes in the Preside Multiservice Data Manager (MDM) software that collect fault information from devices in the network and make it available to the MDM Device Adapter software. Nortel Networks provides MDM software on CD-ROM.

The installed and configured MDM software can include more software servers than are listed in this section. The servers listed are for data collection and mediation purposes.

"Items associated with the MDM Device adapter" (page 19) shows MDM components associated with MDM Device adapter software.

Data collectors

Data collectors are software server processes that collect alarm and state change information from devices in the network and provide this information to the mediation servers in a common format. MDM software uses different sets of data collectors according to the device type. The data collectors are as follows:

- For DPN-100 and Passport 4120, the data collectors consist of the following server processes.

  The data collectors communicate with DPN-100s and Passport 4120s using a protocol called management data interface (MDI), which runs on an X.25 network connection.

  — network control system manager (NCSMGR)

  — DPN management data router (DMDR)

  — host group directory server (HGDS)

- For Passport 6420, 6440, 6480, 7480, 8780 and 15000, the data collectors consist of the following server processes.

  The data collectors communicate with Passport 6420, 6440, 6480, 7480, 8780, and 15000 using a protocol called fast management interface protocol (FMIP). This protocol runs on an IP over frame relay (IPIFR) connection, on an IP over ATM connection (ATM MPE), or on an IP over Ethernet connection when the Passport switches are arranged in an integrated local area network switching (ILS) configuration.

  — FMIP management data router (FMDR)

  — Passport communications manager (FDTM)

  — host group directory server (HGDS)

- For Passport 4400, the data collectors consist of the following software server processes that are provided on the Preside MDM CD-ROM.

  The data collectors communicate with the Passport 4400s using the simple network management protocol (SNMP) protocol that runs on IP connections between the data collectors and the Passport 4400s.

  Note: These server processes run on HP OpenView Network Node Manager software, not supplied with MDM.

  — Passport 4400 data collection daemon (OMSMPADCD)

  — OpenView management data router (OVMDR)

Mediation servers

Mediation servers are software server processes that perform the following functions.

- receive alarm and state information in a common format from the data collectors
- perform state calculations on the state change information
- maintain a current view of the states of devices and components in the network

- make the alarms and the calculated state information available to client applications such as the network management system Adapter (nmsAdapter) by means of the Network Access Data Manager (NDAM) server

The mediation servers are

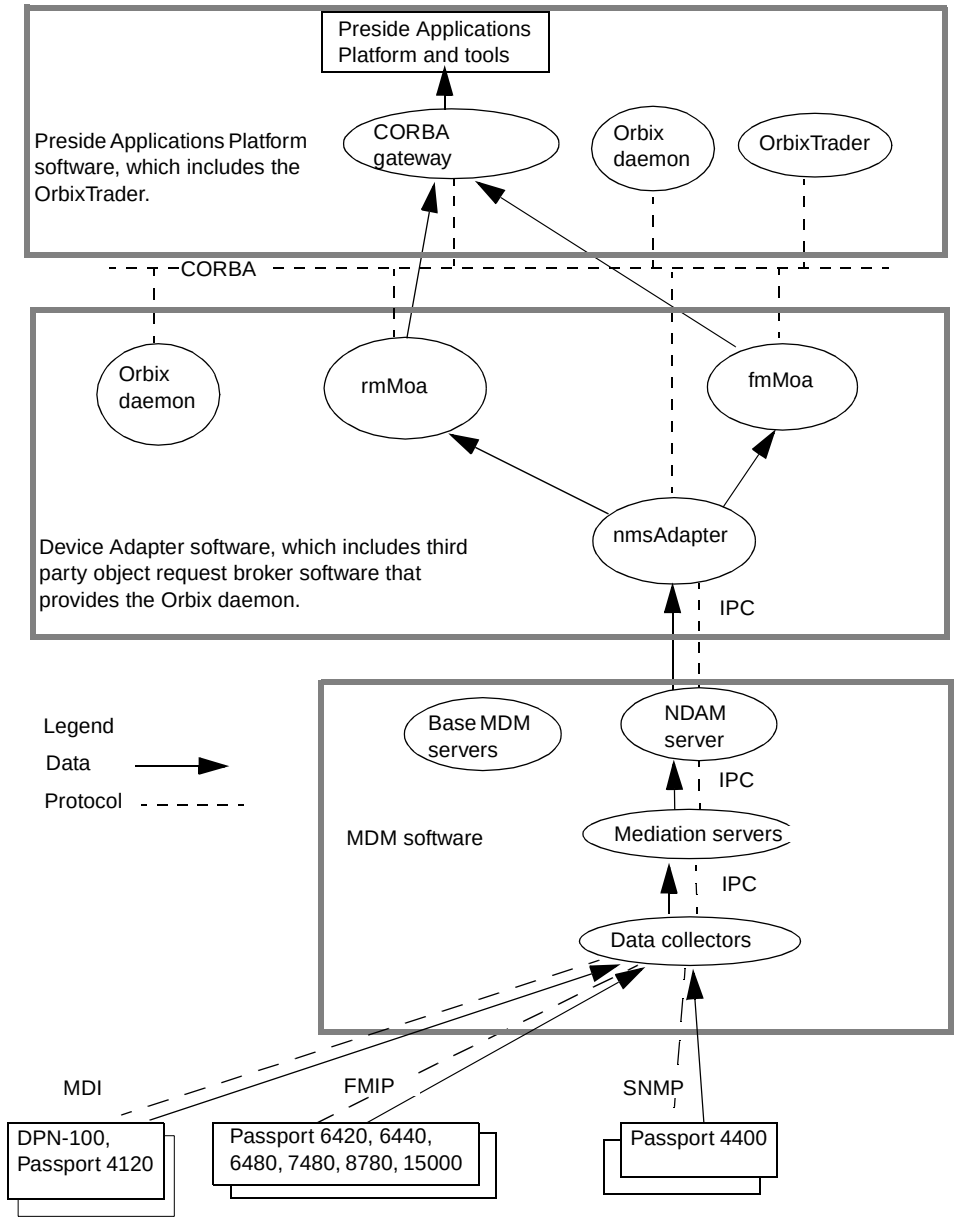
- general management data router (GMDR)
- network model data coordinator (DNMNMC)
- surveillance network model updater (SURNUP)
- network model server (NMSERVER)

Base MDM servers

The base MDM servers start automatically when a user starts an MDM session. These servers let MDM software server processes locate each other to communicate, and to provide MDM logs. The base servers are

- context server (CTXSVR)
- multi-nodal naming server (MNSD)
- MDM log display (OAMC)

Figure 1
Items associated with the MDM Device adapter



NDAM server

The Network Access Data Manager (NDAM) server provides alarms and calculated node and subcomponent states to client applications that register with the NDAM server. These client applications include the network management system Adapter (nmsAdapter).

By default, the NDAM server provides the nmsAdapter with fault information from all of the devices it monitors. You can create one or more typeset files and deviceset files to limit the amount of information NDAM supplies to an nmsAdapter.

When the nmsAdapter registers with the NDAM server, the registration request can include the names of one or more typeset files and deviceset files that the NDAM server uses for filtering fault information that it provides to the nmsAdapter.

Preside MDM Device Adapter software

The interface between the Preside Multiservice Data Manager (MDM) software and applications that make up the Preside Applications Platform is based on common object request broker architecture (CORBA). CORBA is the open management group (OMG) standard protocol that lets customers develop distributed software applications that work across hardware platforms and across programming languages. The interface to the MDM software server processes is based on the inter-process communications (IPC) protocol. One of the functions of the MDM Device Adapter software is to convert fault information delivered in IPC format into CORBA format for the Preside software.

The CORBA applications that make up MDM Device Adapter are

- network management system Application (nmsAdapter)
- resource management managed object agent (rmMoa)
- fault management managed object agent (fmMoa)

“Items associated with the MDM Device adapter” (page 19) shows the applications that make up the MDM Device Adapter software. The following sections explain the purpose of each item in the figure and their relationships.

Fault management MOA (FM MOA)

The Fault Management Managed Object Agent (FM MOA) collects alarms that it obtains from the network management system adapter (nmsAdapter) and makes them available to the MDM Device Adapter applications through the CORBA gateway adapter.

nmsAdapter

The network management system adapter (nmsAdapter) registers with the network data access mediator NDAM server to obtain alarms and calculated device and component states from managed devices through MDM. nmsAdapter communicates with the other MDM Device Adapter applications by a common object request broker (CORBA) protocol and with the NDAM server by inter-process communications (IPC) protocol.

You can create an optional deviceTypeSet filters configuration file to cause the nmsAdapter to include the name of an NDAM device set and/or type set configuration file in nmsAdapter's registration to NDAM. The NDAM server uses the specified file to filter fault information supplied to the nmsAdapter. You can also add exclusions to the deviceType Set filter file to further restrict information that NDAM supplies.

Resource management MOA (RM MOA)

The Resource Management Managed Object Agent (RM MOA) performs the following functions:

- maintains an inventory of network elements and their current states
- provides inventory and state information to Preside Applications Platform applications through the CORBA gateway adapter

Preside Applications Platform software

The following section describes the functions of the Preside Applications Platform software.

CORBA gateway adapter

The CORBA gateway adapter provides a CORBA interface for the Preside Applications Platform tools, such as a desktop or a graphical network browser (GNB).

Preside Applications Platform tools

The Preside Applications Platform tools provide a means to correlate the fault information and to display it on a graphical user interfaces such as the desktop or the graphical network browser (GNB).

OrbixTrader

The OrbixTrader provides a place for all CORBA applications to register so that they can locate each other in order to communicate. The CORBA applications that make use of the OrbixTrader are:

- network management system application (nmsAdapter)
- resource management managed object agent (rmMoa)
- fault management managed object agent (fmMoa)
- CORBA gateway adapter

The OrbixTrader software is included with the Preside Applications Platform software.

Orbix daemon

The Orbix daemon provides a means for all CORBA applications to communicate. Every workstation that runs a CORBA application must run an Orbix daemon. The Orbix daemon is contained in third party Orbix Object Request Broker software produced by IONA Technologies. This software is included with the MDM Device Adapter software.

MDM Device Adapter Network configurations

The figures “Small network configuration for running MDM Server Adapter software” (page 24) and “Medium network configuration for running MDM Server Adapter software” (page 25) show the most common configurations for running the Preside Multiservice Data Manager (MDM) Device Adapter software.

The OrbixTrader, the Preside Applications Platform, and the CORBA gateway adapter run on Hewlett-Packard (HP) workstations. In the most common configuration, the OrbixTrader and the CORBA gateway run on one HP workstation and the Preside Applications Platform and tools run on a second HP workstation.

The MDM Device Adapter software and the MDM software run on Sun workstations.

In small networks, the MDM Device Adapter software can run on the same workstation as the MDM software.

In medium and large networks, the MDM Device Adapter software and the MDM software need to run on separate workstations. To communicate with the network data access mediator (NDAM) server on the workstation that runs the MDM software, the workstation that runs the MDM Device Adapter software needs access to the MDM software libraries. To access the libraries, you must install the MDM software on the workstation that runs the MDM Device Adapter software. You only need to install the MDM software; you do not need to start and configure any of the MDM software server processes.

The Ethernet ports on the workstations that run the software must be connected by the same local area network (LAN) or wide area network (WAN).

Figure 2
Small network configuration for running MDM Server Adapter software

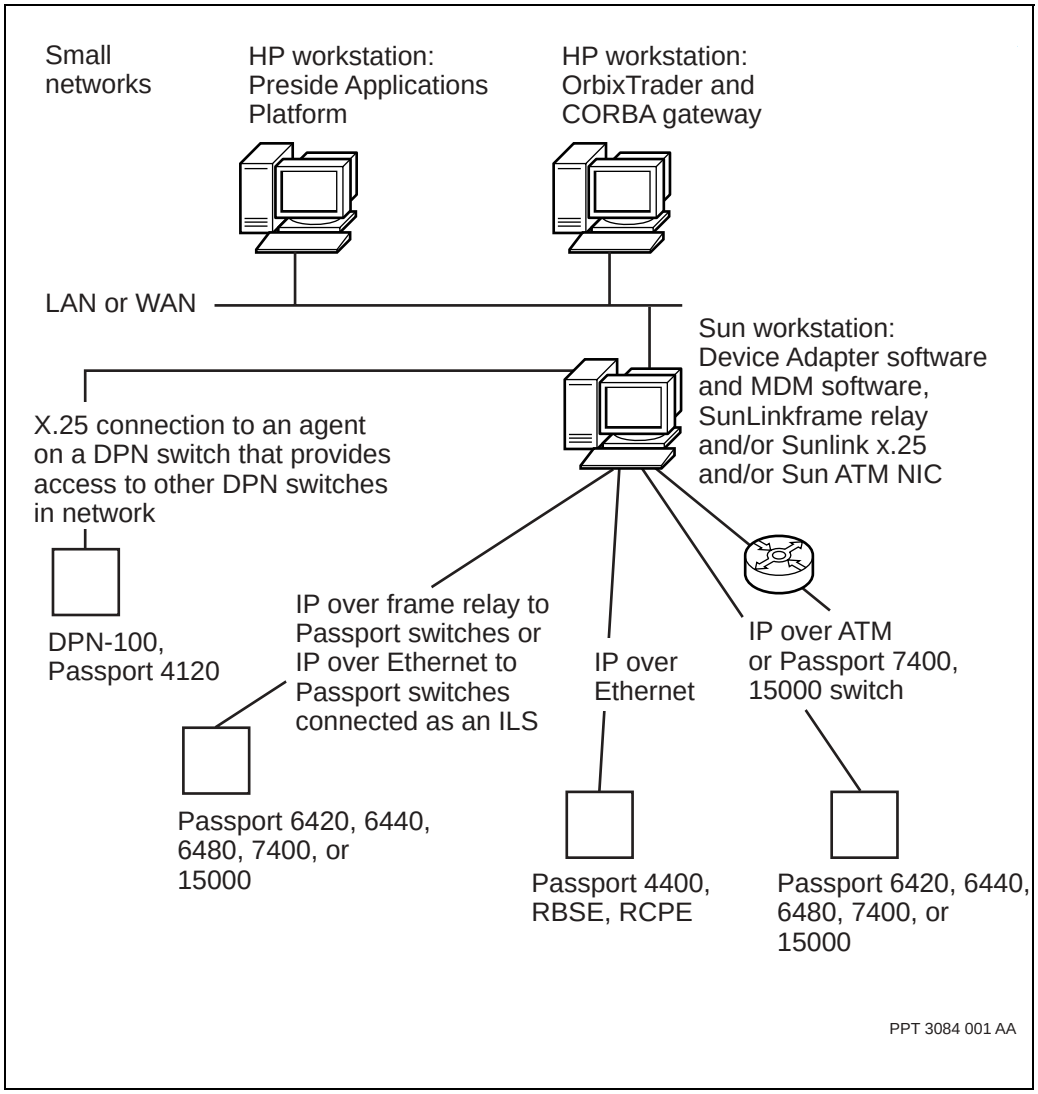
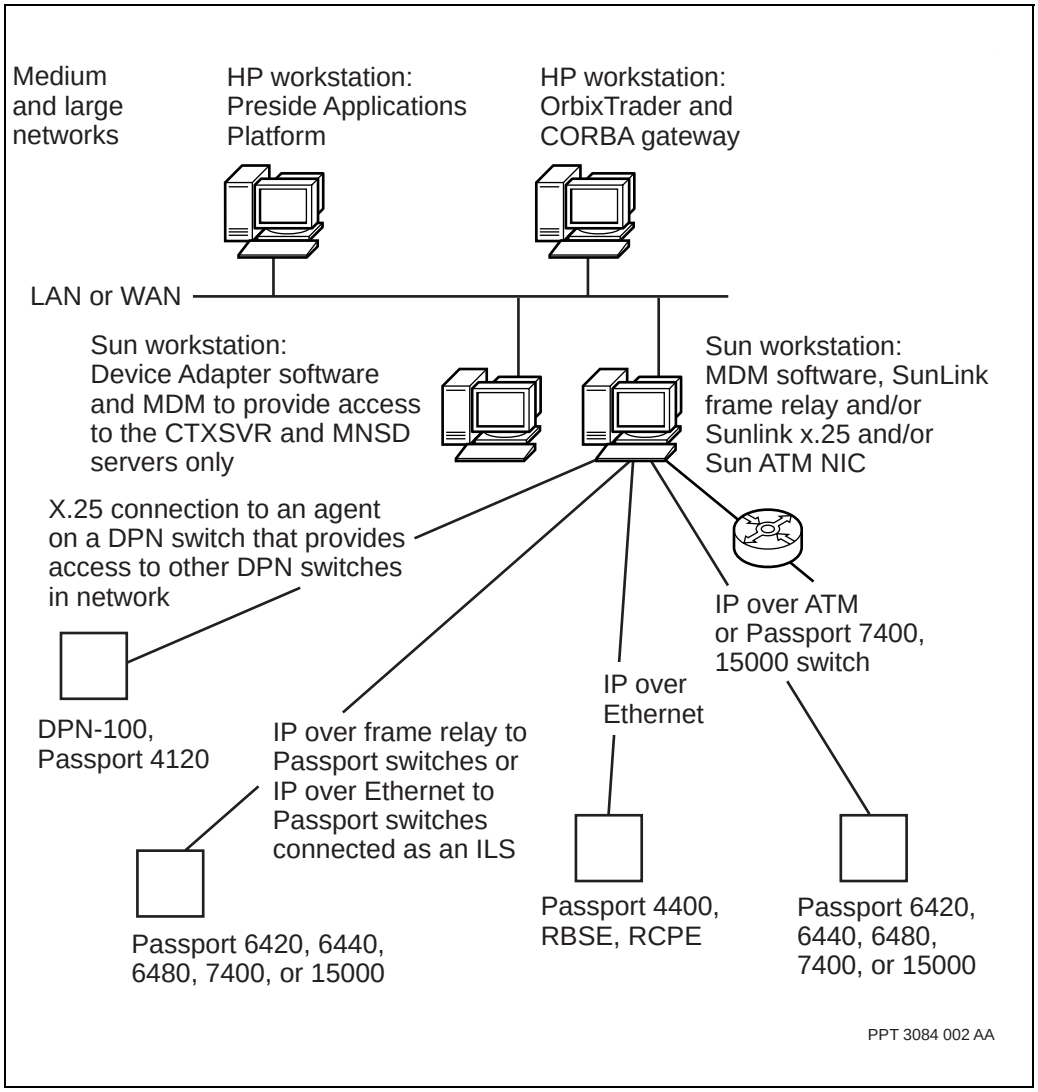


Figure 3
Medium network configuration for running MDM Server Adapter software



The workstation that runs MDM communicates

- with Passport 6420, 6440, 6480, 7480, 8780, and 15000 by means of point-to-point IP over frame relay (IPIFR) connections, or by means of IP over Ethernet when the Passport switches are arranged in an integrated local area network switching (ILS) configuration. When the workstation communicates with the Passport switches by means of IPIFR connections, SunLink frame relay software needs to be installed on the workstation that runs MDM. When the workstation communicates with Passport switches by means of IP over Ethernet, the software provided with the workstation provides IP access to the network.
- with Passport 7480 and 15000 by means of IP over ATM. This requires that you install a SunATM network interface card on the workstation along with the supporting software or connect the MDM workstation to a router, and then connect the router to the Passport 7480 and 15000 by means of IP over ATM.
- with DPN-100 and Passport 4120 by means of an X.25 connection to a DPN-100 switch or a Passport 4120 that runs an agent called the top operations agent (Top OA). The Top OA provides access to other DPN-100 switches in the network and to Passport 4120s in the network. To communicate with the DPN-100s and Passport 4120s in the network, SunLink X.25 software must be installed on the workstation that runs the MDM software.
- with Passport 4400 devices using IP over Ethernet connections provided through a LAN or WAN

Installation overview

This section contains information about the following topics:

- Prerequisites for the installation and configuration
- Installation tasks

Prerequisites for the installation and configuration

Before you install and configure the Preside Multiservice Data Manager (MDM) Device Adapter ensure that

- an OrbixTrader is installed on a workstation on the same local area network (LAN) as the workstation to run the Preside Application Platform tools
- the /etc/hosts file on the OrbixTrader workstation contains information that maps the MDM Device Adapter workstation's nodename to its IP address and identifies two administration userIDs
- the /etc/hosts file on the MDM Device Adaptor workstation contains information that maps the OrbixTrader workstation's nodename to its IP address and identifies two administration userIDs
- all devices (DPN-100s, Passport switches from which you want to obtain fault information are commissioned
- the MDM software is installed and configured to monitor all types of devices.
- the MDM servers listed in "MDM servers that start automatically when a user logs in" (page 28) and "MDM servers that you must start to manage different devices" (page 28) are configured and running. The tables contain two categories of servers:
  - — servers that start automatically when a user logs in to MDM
  - — servers that you must configure and start with the server manager administration tool

  Note: In addition to the servers listed in "MDM servers that start automatically when a user logs in" (page 28) and "MDM servers that you must start to manage different devices" (page 28), other servers may be running on a fully configured MDM workstation, but they are not essential for MDM Device Adapter. For example, the network model editor server (EDSERVER) can also be running. See 241-6001-303 *Preside MDM Administrator Guide* for information about these servers and the ways to start them.

MDM servers that start automatically when a user logs in

Abbreviation	Full name
CTXSVR	context server
MNSD	multi-nodal naming server
OAMC	MDM log collector

MDM servers that you must start to manage different devices

Required for	Abbreviation	Full name
Passport 6420, 6440, 6480, 7480, 8780, and 15000	FMDR	FMIP management data router (one server for each Passport group)
	FDTM	Passport communications manager
	HGDS	host group directory server (also needed for DPN-100 and PP 4120)
DPN-100 and PP4120	DMDR	DPN management data router (One server for each OA group)
	HGDS	host group directory server (also needed for Passport 6420, 6440, 6480, 7480, 8780, and 15000)
Passport 4400	OMSMPADCD	Passport 4400 data collection daemon
	OVMDR	OpenView management data router
		Note: To collect surveillance data from Passport 4400 devices also requires HP OpenView Network Node Manager software which must be purchased from Hewlett-Packard
All devices	GMDR	general management data router
	SURNUP	surveillance network model updater
	NMSERVER	network model server

Installation tasks

Perform the following tasks to install and configure the Preside Multiservice Data Manager (MDM) Device Adapter software:

1 Ensure that the workstation meets engineering requirements, see “Engineering” (page 31).

2 Plan domains and subdomains to support redundancy, see “Planning domains and subdomains with redundancy” (page 37).

3 Ensure that the MDM is set up to provide fault information to the MDM Device Adapter applications, see “Preparing MDM” (page 47).

4 Configure the MDM as a trusted workstations, see “Configuring trusted workstations” (page 58).

5 Create the necessary UNIX group and userIDs on the MDM, see “Creating an AP group and userIDs on the MDM host” (page 61).

6 Load the MDM Device Adapter software from the MDM CD-ROM and configure the object request broker (ORB), see “Installing Device Adapter software” (page 57).

7 Set up the ndam.hosts configuration file, then start the network management system Adapter (nmsAdapter), the fmMoa, and the rmMoa, see “Starting MDM Device adapter applications” (page 85).

8 Set up filtering to limit the amount of information supplied to the nmsAdapter (optional), see “Filtering fault information” (page 69).

Documentation roadmap

For instructions to install and configure the Preside Multiservice Data Manager (MDM) software so it provides fault information from DPN-100, Passport 4120, Passport 6420, Passport 6440, Passport 6480, Passport 7480, Passport 8780, and Passport 15000, see

- 241-6001-100 *Preside MDM Installer Guide*
- 241-6001-303 *Preside MDM Administrator Guide*
- 241-6001-310 *Preside MDM Server Reference Guide*

For instructions to configure the MDM software to provide fault information from Passport 4400 see

- 241-6001-109 *Preside MDM Passport 4400 Integration Guide*

For instructions to install and configure the CORBA gateway and the Preside Network Management applications, see

- Preside Applications Platform, 7.0.0 Installation and Administration Guide, 450-3101-201

Chapter 2
Engineering

This section contains information about the following topics:

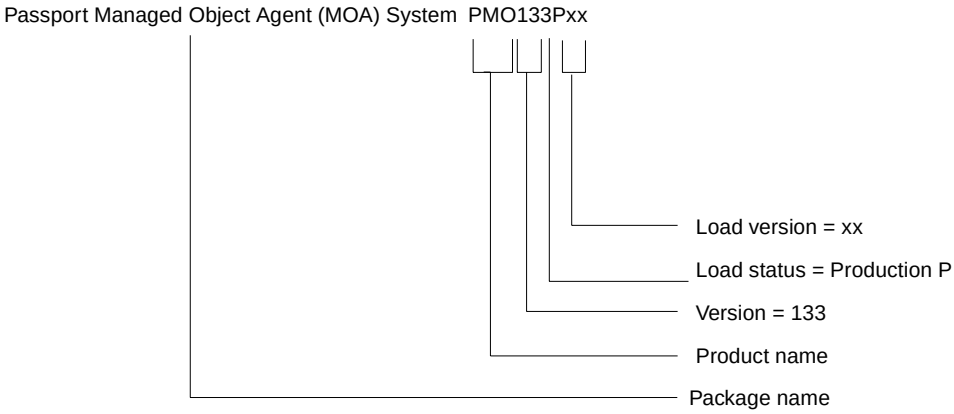
How the software is supplied

The Preside Multiservice Data Manager (MDM) Device Adapter software is supplied on the Preside MDM CD-ROMs. The software consists of a single software package that is created with the Solaris packaging tools. The package on the compact disk has a name similar to the following example:

Passport Managed Object Agent (MOA) System - PMO133Pxx

An explanation of the CD ROM package in the example is as follows:

Figure 4
Example of package naming



Licensing

Although you do not need a license to run the Preside Multiservice Data Manager (MDM) Device Adapter software, you do need licenses to run the MDM software.

The license for the MDM software must allow you to run the MDM Entry software package and the optional network data access mediator (NDAM) server package.

Software compatibility

The Preside Multiservice Data Manager (MDM) Device Adapter release 13.3 software

- runs on the Solaris 2.8 (and up) operating system
- is compatible with MDM release 13.3 software and up
- is compatible with Preside Applications Platform release 9.1 software and above
- requires access to an OrbixTrader, version 2000 1.2.1

- supports Passport switches that are running release 5.0 software and above
- supports DPN-100 and Passport 4120 that run release generic 36 and above

Minimum hardware requirements

The minimum requirements to run the Preside Multiservice Data Manager (MDM) Device Adapter software on a workstation are as follows:

- minimum workstation hardware platform: SPARC Ultra 5
- RAM: 128 Mbyte
- disk space: 4 Gbyte

Maximum number of nodes that you can monitor

The maximum number of nodes that you can monitor with a single installation of the Preside Multiservice Data Manager (MDM) Device Adapter software depends on the configuration of the network and factors, such as:

- the number of alarms set and cleared per minute
- whether the network is in a steady state
- the types of nodes you are monitoring

Contact Nortel Networks to determine the number of nodes you can support before deploying the MDM Device Adapter software.

We ran central processing unit (CPU) capacity tests which show that under specific conditions, the MDM Device Adapter software can support up to 200 nodes. The following sections describe the conditions and results of the capacity tests we performed.

Conditions

Conditions were as follows:

- workstation: SPARCstation Ultra 10 with 512 Mbyte of RAM
- number of network nodes: 200
- each node brought to a state of four alarms

Results

When injecting 1150 alarms per minute to hold the network at a steady state (that is alarm clearing and setting rates match) the following central processing unit (CPU) usage was noted:

- fault management managed object agent (fmMoa): 4 percent
- resource management managed object agent (rmMoa): 16 percent
- network management system Application (nmsAdapter): 16 percent

Connectivity requirements

Internet Protocol connectivity through a local area network (LAN) or a wide area network (WAN) is required:

- between the workstations that run the Preside Multiservice Data Manager (MDM) Device Adapter applications, the OrbixTrader, the Preside Applications Platform software, and the MDM software
- from the workstations to Passport 4400 and iBWA 5100 devices in the network

The workstation that runs the MDM software communicates with devices in the network in the following ways:

- with Passport 6420, 6440, 6480, 7480, 8780, and 15000 by means of point-to-point IP over frame relay (IPIFR) connections, or by means of IP over ethernet connections when the Passport switches are arranged in an integrated local area network switching (ILS) configuration. If you use IPIFR, you must install SunLink frame relay on the workstation that has the IPIFR connections to the network.
- with Passport 7480 and 1500 by means of IP over ATM. This requires that you install an ATM network interface card on the workstation along with the supporting software.
- with DPN and Passport 4120 by means of an X.25 connection to a DPN switch that runs an agent called the top operations agent (Top OA). The Top OA provides access to other DPN switches in the network and to Passport 4120s in the network. When X.25 is used, you must install SunLink X.25 on the workstation that has the connection to the network.

- with Passport 4400 and iBWA 5100 devices by means of IP over ethernet through a LAN or WAN

In small networks, the MDM software runs on the same workstation as the MDM Device Adapter software. In medium and large networks the MDM software and the MDM Device Adapter software must run on separate workstations. When the MDM and MDM Device Adapter software run on separate workstations, you must provide IP connectivity between the two workstations.

Chapter 3
Planning domains and subdomains with redundancy

This section contains information about the following topics:

- Domains and subdomains
- Resiliency and redundancy

This section also contains a procedure for planning domains and subdomains in a way that provides resiliency and redundancy, see “Planning domains and subdomains with redundancy” (page 44).

Domains and subdomains

The following sections define domains and subdomains, explain how they are used, and provide guidelines for choosing them.

Domain

For the Preside Multiservice Data Manager (MDM) Device Adapter, a domain is a set of Passport switches that belong to a geographic region or to a business organization for fault management purposes. For an example of a domain, see “Representation of a domain and a subdomain” (page 39). Guidelines for setting up domains are as follows:

- A domain can contain a maximum of 100 Passport switches.
- A domain must contain one instance of each of the following MDM Device Adapter applications:
  - a resource management managed object agent (rmMoa)

— a fault management managed object agent (fmMoa)

- You must assign the same domain name to the fmMoa and the rmMoa in a domain.
- You do not need to assign a domain name to the CORBA gateway adapter. The CORBA gateway adapter only requires the assignment of subdomain names. See “Subdomain” (page 38).

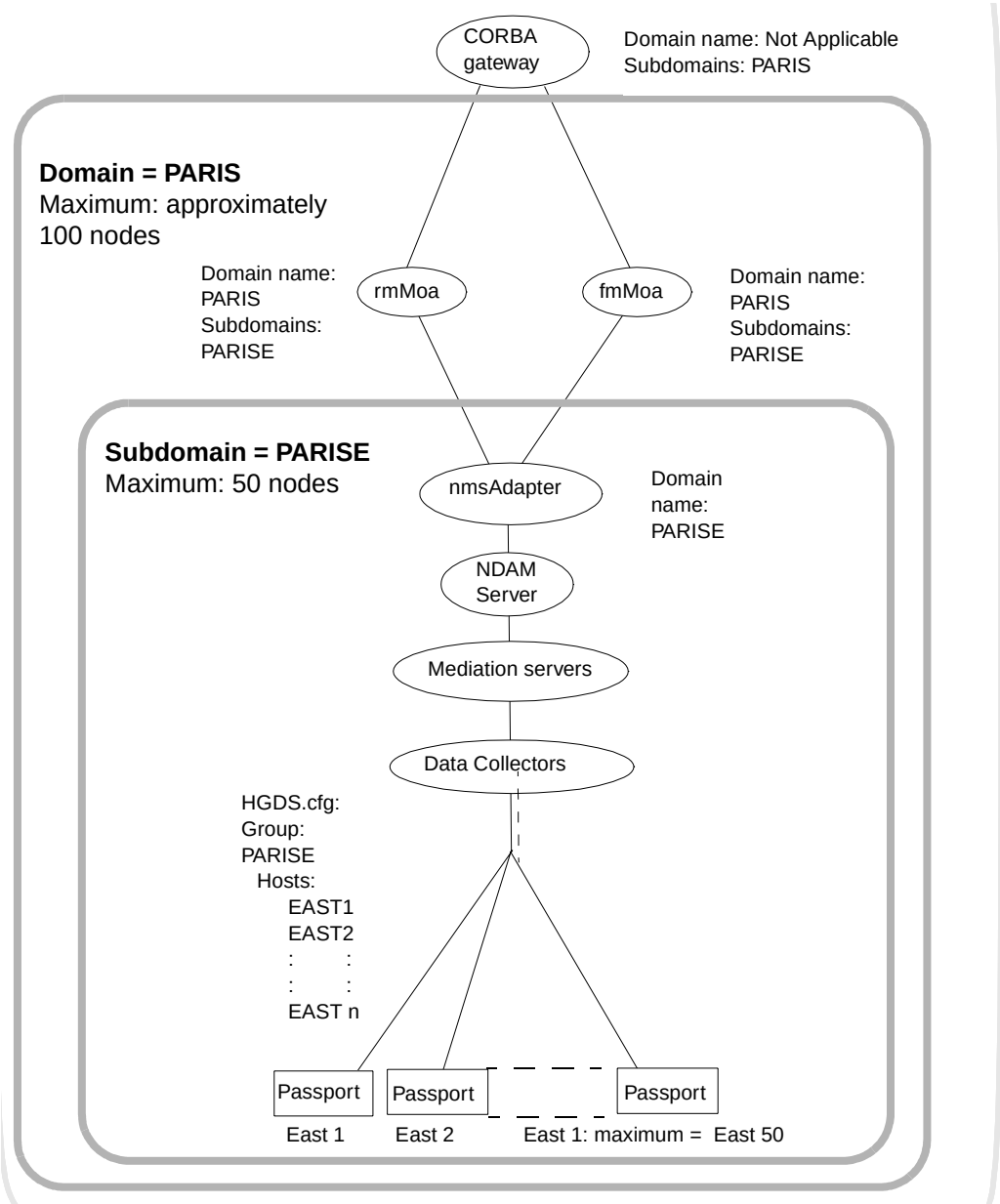
Subdomain

For the Preside Multiservice Data Manager (MDM) Device Adapter, a subdomain is a set of Passport switches within a domain that are managed with the MDM software. Guidelines for setting up subdomains are as follows:

- A subdomain can contain a maximum of 100 Passport switches.
- A subdomain must contain at least one instance of a network management system Application (nmsAdapter).
- The domain name you assign to an nmsAdapter must be the subdomain of a rmMoa and the fmMoa in the same domain.
- There must be one nmsAdapter for each network data access mediator (NDAM) server (part of the MDM software).
- The domain name you assign to an rmMoa and the fmMoa must appear as a subdomain in the startup command of the CORBA gateway adapter.

For a sample scheme for assigning subdomain names, see “Representation of a domain and a subdomain” (page 39).

Figure 5
Representation of a domain and a subdomain



Resiliency and redundancy

Resiliency is the ability of a system to recover from a fault condition such as software, link, or workstation failure. Although there are many ways to ensure resiliency and redundancy for the Preside Multiservice Data Manager (MDM) Device Adapter, the recommended way is to create redundant instances of

- MDM Device Adapter applications (network management system Adapter (nmsAdapter), fault management managed object agent (fmMoa), and resource management managed object agent (rmMoa))
- the network data access mediator (NDAM) servers (part of the MDM software)

Redundancy and the nmsAdapter, the fmMoa, and the rmMoa

Redundant Preside Multiservice Data Manager (MDM) Device Adapter applications [network management system Application (nmsAdapter), fault management managed object agent (fmMoa), and resource management managed object agent (rmMoa)] run in standby. If a client application, such as an fmMoa, loses contact with the server application that it relies on, such as an nmsAdapter, the client application contacts the OrbixTrader. The OrbixTrader provides the location of a redundant application that has the same domain name as the client application. The client application and server applications can be located on the same workstation or on different workstations. The client application then makes use of the new server application.

Redundancy and NDAM servers

Redundant NDAM servers also run in standby. The network management system Application (nmsAdapter) has a configuration file called ndam.hosts. This file specifies the location of at least one NDAM server (part of the Preside Multiservice Data Manager (MDM) software) that provides the nmsAdapter with Passport fault data.

You can also specify the location of one or more redundant NDAM servers in the ndam.hosts file. At startup, the nmsAdapter registers with the NDAM server that is specified in the first record of the file and begins to obtain fault information from it. If the nmsAdapter is unable to access this server, the system software tries to register with the next NDAM server in the file and so on, until it reaches the last NDAM server in the file. If it is still unable to

register, the system software starts back at the top of the file, and keeps attempting to register with each NDAM server listed in the file until it is successful. After it tries every entry in file, the nmsAdapter exits.

Provided that the MDM software is configured to provide duplicate streams to the main NDAM server and all backup NDAM servers, no data is lost in the switchover from one NDAM server to a backup NDAM server.

Recommended scheme for setting up redundancy

Although there are many ways to set up instances of the Preside Multiservice Data Manager (MDM) Device Adapter applications and NDAM servers to ensure redundancy, we recommend that you:

- create redundant instances of each Preside Multiservice Data Manager (MDM) Device Adapter application on separate workstations in your network
- configure the MDM software so that redundant NDAM servers run on separate workstations

We recommend that you use separate workstations because redundant instances of an application on the same workstation can counteract failure of an individual application, but not total workstation failure. For a sample of the recommended scheme using two Sun workstations, see “Example of a redundant configuration using two workstations” (page 43).

How redundancy operates with the recommended scheme

There are several types of failure to consider:

- failure of a single Preside Multiservice Data Manager (MDM) Device Adapter application [network management system Adapter (nmsAdapter), fault management managed object agent (fmMoa), and resource management managed object agent (rmMoa)]
- failure of a workstation that runs an MDM Device Adapter application
- failure of an NDAM server, or the connection between an nmsAdapter and the NDAM server

Failure of an MDM Device Adapter application

"Example of a redundant configuration using two workstations" (page 43) shows a sample configuration of redundant applications. Assume that the fault management managed object agent (fmMoa) on workstation Host 1 is using a network management system Application (nmsAdapter) which is also running on workstation Host 1, and the nmsAdapter application fails. If the fmMoa is unable to contact the nmsAdapter, the fmMoa contacts the OrbixTrader to obtain the location of an nmsAdapter that has the same domain name as the nmsAdapter that failed. In this case, the alternate nmsAdapter is on workstation Host 2. The fmMoa on workstation Host 1 then uses the new nmsAdapter on workstation Host 2. Because the resource management managed object agent (rmMoa) is also unable to contact the nmsAdapter, it also contacts the OrbixTrader and switches over to the nmsAdapter on Host 2.

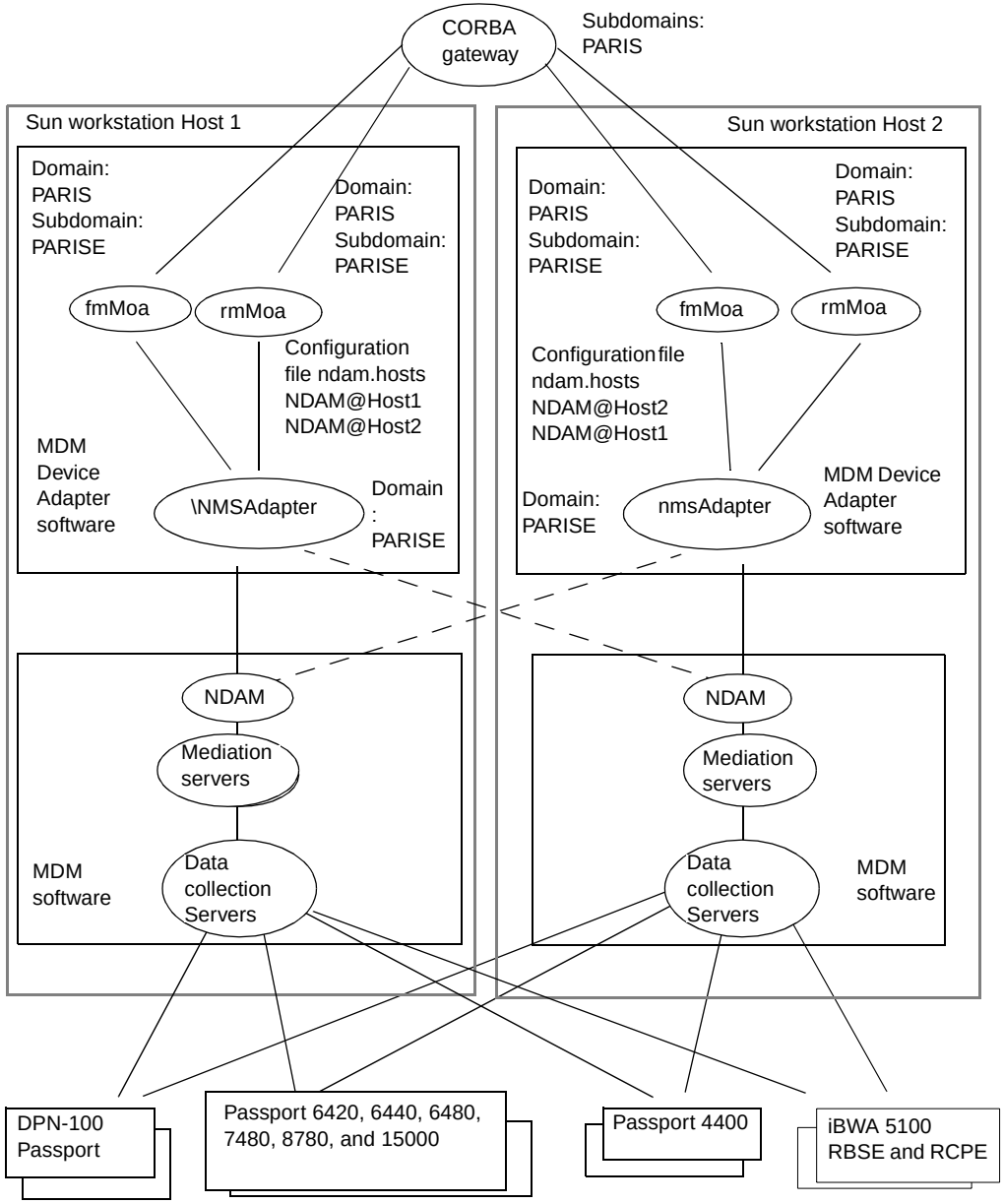
Failure of a workstation that runs MDM Device Adapter applications

Assume that workstation Host 1 fails entirely and all applications with it. The CORBA gateway that is using the fault management managed object agent (fmMoa), and resource management managed object agent (rmMoa) on Host 1 uses the OrbixTrader to locate an alternate fmMoa and rmMoa that have the domain name that the CORBA gateway requires. These are the fmMoa and rmMoa on Host 2.

Failure of an NDAM server

Assume that the configuration file of the network management system Adapter (nmsAdapter) on workstation Host 1 contains two records. The first record specifies the location of the NDAM server on Host 1 and the second record specifies the location of the NDAM server on Host 2. Assume that the nmsAdapter on Host 1 loses contact with the NDAM server on Host 1. The nmsAdapter reads the next record in its configuration file, determines that the record specifies the NDAM server on Host 2, and attempts to register with it. If the registration request succeeds, the nmsAdapter obtains fault information from the NDAM server on Host 2.

Figure 6
Example of a redundant configuration using two workstations



Planning domains and subdomains with redundancy

Use this procedure to plan domains and subdomains with redundancy. While using this procedure, capture the planning information on the worksheet “Planning worksheet” (page 45). You need this information to start the Preside Multiservice Data Manager (MDM) Device Adapter applications and to keep track of them for operations and administration purposes.

Prerequisites

If you are not familiar with the concepts of domains, subdomains, and how resiliency and redundancy can be provided for the Preside Multiservice Data Manager (MDM) Device Adapter, read:

- “Domains and subdomains” (page 37)
- “Resiliency and redundancy” (page 40)

1. Write the host name and IP address of the workstation on which you are going to install the Preside Multiservice Data Manager (MDM) Device Adapter software on the planning worksheet “Planning worksheet” (page 45).
2. Determine if you wish to manage your Passport switches on a regional or functional basis and choose the domain names for the fault management managed object agent (fmMoa), and resource management managed object agent (rmMoa) accordingly.

   Note: You can assign the same domain name or different domain names to the fmMoa and the rmMoa. If they are both using the same network management system Adapter (nmsAdapter), use the same domain name for simplicity.
3. Write the domain names on the planning worksheet “Planning worksheet” (page 45).
4. Choose a domain name for the nmsAdapter and write this information on the worksheet.

   Note: The domain name of the nmsAdapter must be different from the domain name of the fmMoa and rmMoa.
5. Assign the domain name of the nmsAdapter as the subdomain of the fmMoa and of the rmMoa.
6. Write the subdomain name on the worksheet.
7. Write the host name and IP address of the workstation that is running the primary NDAM server on the worksheet. If the MDM software and the

MDM Device Adapter software are running on the same workstation, the host name is localhost.

8 Optionally, if there is another workstation running the MDM software and a backup NDAM server, add the location of the NDAM server to the planning worksheet.

9 If you plan on using redundant workstations, add information about the workstation that is running the redundant fmMoa, rmMoa and the nmsAdapter to the planning worksheet.

10 Set up MDM to provide fault information to the MDM Device Adapter applications. See “Preparing MDM” (page 47).

Planning worksheet

Item	Information
Workstation running MDM Device Adapter software	
	Host name:
	IP Address:
fmMoa	
	Domain name:
	Subdomain names:
nmsAdapter	
	Domain name:
	Name of host that runs NDAM server:
	Name of host that runs backup NDAM server:
Workstation running redundant MDM Device Adapter applications	
	Host name:
	IP Address:

Chapter 4
Preparing MDM

Perform the tasks in this section to verify that the Preside Multiservice Data Manager (MDM) software is configured to obtain fault information from devices in the network and provide it to the MDM Device Adapter applications. This section includes the following topics:

Requirements

Before you begin

- There must be at least one workstation running the Preside Multiservice Data Manager (MDM) software in your network, and preferably a second backup workstation.
- The MDM software must be configured to obtain fault information from the devices you want to manage in your network.

If there is no Preside MDM workstation configured to obtain fault information, see the following documents:

- to install the MDM software and to configure Preside MDM software to provide fault information from DPN-100, Passport 4120, Passport 6420, Passport 6440, Passport 6480, Passport 7480, Passport 8780, and Passport 15000 devices, see:
  - 241-6001-100 *Preside MDM Installer Guide*
  - 241-6001-303 *Preside MDM Administrator Guide*

- to configure the MDM software to obtain fault information from Passport 4400 and iBWA 5100, see:
  - — 241-6001-109 *Preside MDM Passport 4400 Integration Guide*
  - — 241-6001-113 *Preside MDM iBWA 5100 Integration Guide*

Procedures for preparing MDM

You can verify that the Preside Multiservice Data Manager (MDM) software is configured to obtain fault information from devices in the network and you can confirm that the MDM software is configured to provide fault information to the MDM Device Adapter applications using the procedures in this section.

Checking the MDM software licenses

Use this procedure to ensure that the Preside Multiservice Data Manager (MDM) is equipped with a license to obtain fault information from devices in the network.

1 Log in as the root user on the workstation that runs the MDM software.

2 Display a list of the valid licenses on the workstation and the software sets you are entitled to run. Type the following:

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

Information about expiry dates and the software sets your licenses permits you to run is displayed. For example,

```
Product: MDM   Release: R12.5 Customer name: TelcoB

ACTIVE LICENSES:

_________________

MDM R12.5 MDMDEV ANY 19990510 20300101 FFFF 111111111FF

    Start Date:      1999/05/10
    End Date:           2030/01/01

    Options enabled:

MDM Base
Network Activation Tool
NDAM
```

If Fault and NDAM do not appear in this list, you need a new license. Contact your Nortel Networks Corporation representative.

3 Perform one, or more, of the following procedures according to the devices that you have in your network:

- "Verifying fault collection from Passport 6420, 6440, 6480, 7480, 8780, or 15000 devices" (page 49)
- "Verifying fault collection from DPN-100 or Passport 4120 devices" (page 51)
- "Verifying fault collection from Passport 4400 devices" (page 52)
- "Verifying fault collection from iBWA 5100 devices" (page 55)
- none of these, "Starting the NDAM server" (page 56)

Verifying fault collection from Passport 6420, 6440, 6480, 7480, 8780, or 15000 devices

Use this procedure to ensure that the Preside Multiservice Data Manager (MDM) software is configured to obtain fault information from Passport 6420, 6440, 6480, 7480, 8780 or 15000 devices in the network.

1 Ensure that every Passport switch that you want to manage is equipped with a common userID and password that provides read access to information. See 241-7001-150 *Passport Operations and Maintenance Guide* for information about setting and verifying userIDs and passwords.

2 Use an editor, such as the text editor that is provided with the Solaris operating system, to look at file /opt/MagellanNMS/cfg/HGDS.cfg and ensure that this file contains Passport groups that specify all of the Passport switches you want to manage. For information about this file, see 241-6001-303 *Preside MDM Administrator Guide*.

3 Use the MDM Server Administration tool to verify that the following base servers are running. The base server start automatically when a user logs in to the MDM software. If the servers do not start and remain running, ensure that an MDM user account is set up as described in 241-6001-303 *Preside MDM Administrator Guide*.

Server	Full name
CTXSVR	context server
OAMC	MDM log server
MNSD	multi-nodal naming server

4 Use the MDM Server Administration tool to verify that the following data collection and mediation servers are configured to start automatically after a reboot and that the servers are running.

Server	Start-up command
FDTM	/opt/MagellanNMS/bin/fdtm -offset <offset>
HGDS	/opt/MagellanNMS/bin/HGDS
FMDR (one for each group of Passport switches)	/opt/MagellanNMS/bin/fmdr -u <user ID> -p <password> -g group -I AL
GMDR	/opt/MagellanNMS/bin/gmdr
DMNNMC	/opt/MagellanNMS/bin/dmnnmc
SURNUP	/opt/MagellanNMS/bin/surnup
NMSERVER	/opt/MagellanNMS/bin/nmserver -c 5000

For information about the MDM Server Administration tool, see 241-6001-303 *Preside MDM Administrator Guide*.

Note 1: Be sure to click the Save and Start button to start each server and preserve the server's configuration after a system reboot.

Note 2: In addition to these servers, other Preside Multiservice Data Manager (MDM) servers can run on a fully configured MDM workstation, but they are not essential for the MDM Device Adapter, for example, the network model editing server (EDSERVER).

5 Display the size of the shared segment of memory in the system kernel:

```
more /etc/system
```

6 Verify that the following parameter has a value equal to or greater than the value in the following example:

```
shmsys:shminfo_shmmax=16777216
```

If the value of the parameter is lower than 16777216, run the /opt/MagellanNMS/system/config/config_sys_shem script to reset the value to 16, then reboot the workstation. For the instructions to do this, see 241-6001-303 *Preside MDM Administrator Guide*.

7 Use the GMDR Administration tool to ensure that the GMDR server is set up to obtain surveillance information from one FMDR server for each

group of Passport switches you want to manage. For information about Passport groups and the GMDR administration tool, see 241-6001-303 *Preside MDM Administrator Guide*.

8 Perform one or more of the following procedures according to the types of devices in your network

- "Verifying fault collection from DPN-100 or Passport 4120 devices" (page 51)
- "Verifying fault collection from Passport 4400 devices" (page 52)
- "Verifying fault collection from iBWA 5100 devices" (page 55)
- none of these, "Starting the NDAM server" (page 56)

Verifying fault collection from DPN-100 or Passport 4120 devices

Use this procedure to ensure that the Preside Multiservice Data Manager (MDM) software is set up to obtain fault information from DPN-100 and Passport 4120 devices in the network.

1 Using an editor, such as the text editor that is provided with the Solaris operating system, open the /opt/MagellanNMS/cfg/HGDS.cfg file.

2 Ensure that the file specifies groups of operations agents (OA) that include all DPN switches and Passport 4120 devices you wish to manage. For information about the syntax of this file, see 241-6001-303 *Preside MDM Administrator Guide*.

3 Using the MDM Server Administration tool, verify that the following servers are configured to start automatically after a reboot, and that these servers are running:

Server	**Start-up command**
NCSMGR	/opt/MagellanNMS/bin/ncsmgr
HGDS	/opt/MagellanNMS/bin/HGDS
DMDR (one for each group of OAs	/opt/MagellanNMS/bin/dmdr -g <group> -c <NCS capabillity> -p <password>
GMDR	/opt/MagellanNMS/bin/gmdr

Server	Start-up command
DMNNMC	/opt/MagellanNMs/bin/dmnnmc
SURNUP	/opt/MagellanNMS/bin/surnup
NMSERVER	/opt/MagellanNMS/bin/nmserver -c 5000

For information about the MDM Server Administration tool, see 241-6001-303 *Preside MDM Administrator Guide*.

Note 1: Be sure to click on the Save and Start button to start each server and preserve the configuration after a system reboot.

Note 2: In addition to these servers, other Preside Multiservice Data Manager (MDM) servers can run on a fully configured MDM workstation, but they are not essential for the MDM Device Adapter, for example the network model editing server (EDSERVER).

4 Using the GMDR Administration tool, ensure that the GMDR server is set up to obtain surveillance information from a DMDR server for each group of OAs for the DPN switches and Passport 4120s you want to manage. For information about the GMDR Administration tool, see 241-6001-303 *Preside MDM Administrator Guide*.

5 Perform one or more of the following procedures according to the types of devices in your network

- “Verifying fault collection from Passport 4400 devices” (page 52)
- “Verifying fault collection from iBWA 5100 devices” (page 55)
- none of these, “Starting the NDAM server” (page 56)

Verifying fault collection from Passport 4400 devices

Use this procedure to ensure that the Preside Multiservice Data Manager (MDM) software is set up to obtain fault information from Passport 4400 devices in the network.

1 Ensure that HP OpenView Network Node Manager release 5.1 software is installed on the workstation that collects data from Passport 4400. In small networks the HP OpenView software can be installed on the same workstation as the Preside Multiservice Data Manager (MDM) software. In large networks you require a separate workstation. See 241-6001-109 *Preside MDM Passport 4400 Integration Guide* for details.

2 On the workstation that is running HP OpenView, ensure that the system kernel (file /etc/system) contains the following parameters and values:

```
set maxusers=64
set max_nprocs-1000
set semsys:seminfo_semmap=10
```

If the values are not correct, edit the /etc/system file to correct the values, then reboot the workstation.

3 On the workstation that is running HP OpenView, enter the following command for each Passport 4400 to ensure that there is IP connectivity between the workstation and the Passport 4400:

`ping <ip-address of 4400>`

4 If the MDM software runs on a different workstation from HP OpenView, enter the following command to ensure that there is connectivity to the workstation that is running the MDM software:

`ping <ip-address of MDM workstation>`

5 At the workstation that is running HP OpenView, enter the following command to ensure that the MDM-Passport 4400 application is loaded on the workstation:

`/opt/OV/nortel/oms/install/tools/omsverify`

A table containing a list of the installed packages appears on the screen. This table must contain the following packages:

- gmb
- omshelp
- omsbase
- ovmdr
- nmsmpa
- omsmpacfg

6 Are all of the packages present?

If	Then
Yes	Go to step step 7
No	Load the MDM-Passport 4400 application from the MDM CD-ROM by entering the following commands, then go to step step 7. cd /cdrom/cdrom0 cd oms/solaris/ov/mpa ./nmsmpainstall

7 At the workstation that is running the MDM software, start the command console, set the route to @, and enter the following command to determine if trap subscription is set up on the Passport 4400. For information about the command console and the instructions for using it, see 241-6001-804 *Preside MDM Workstation Utilities User Guide*.

`MPA <mpa_name> QUERYSUBSCRIBE`

If the response indicates that trap subscription is not set up, use Telnet to log in to the Passport 4400, then enter the following command to set up trap subscription:

`add system trap new <ip-address-HPOpenViewWorkstation> “public”`

8 Make sure that the OVMDR server is running:

`/opt/OV/bin/ovstart ovmdr`

9 On the workstation that is running the MDM software, use the Server Administration tool to verify that the following servers are configured to start automatically after a reboot and that these servers are running.

Server	Start-up command
GMDR	/opt/MagellanNMS/bin/gmdr
DMNNMC	/opt/MagellanNMS/bin/dmnnmc
SURNUP	/opt/MagellanNMS/bin/surnup
NMSERVER	/opt/MagellanNMS/bin/nmserver -c 5000

10 On the workstation that is running the MDM software, log in to the GMDR Administration tool as administrator and ensure that the GMDR server is

set up to obtain information from the OpenView management data reporter (OVMDR) server. For the instructions to do this, see 241-6001-303 *Preside MDM Administrator Guide*.

11 Perform one or more of the following procedures according to the types of devices in your network:

- "Verifying fault collection from iBWA 5100 devices" (page 55)
- none of these, "Starting the NDAM server" (page 56)

Verifying fault collection from iBWA 5100 devices

Use this procedure to ensure that the Preside Multiservice Data Manager (MDM) software is set up to obtain fault information from iBWA 5100 family of devices, namely Radio base station equipment or Radio customer premises equipment in the network.

1 On the workstation that is running the Preside Multiservice Data Manager (MDM) software, enter the following command for each iBWA 5100 device to ensure that there is IP connectivity between the workstation and the device:

```
ping <ip-address of iBWA 5100 device>
```

2 On the workstation that is running the MDM software, ensure that file /opt/MagellanNMS/cfg/gendcd_ibwa5k.sed exists and that it contains information about all of the iBWA 5100 devices managed through the MDM software. If it does not exist or it is missing the devices you wish to manage, create and populate the file as described in 241-6001-113 *Preside MDM iBWA 5100 Integration Guide*.

3 On the workstation that is running the MDM software, use the Server Administration tool to verify that the required servers are configured to start automatically after a reboot and are currently running. See 241-6001-113 *Preside MDM iBWA 5100 Integration Guide* for a list of the required servers.

4 On the workstation that is running the MDM software, log in to the GMDR Administration tool as administrator and ensure that the GMDR server is set up to obtain information from the SMDR server. For the instructions to do this, see 241-6001-303 *Preside MDM Administrator Guide*.

5 Go to "Starting the NDAM server" (page 56).

Starting the NDAM server

Use this procedure to start a network data access mediator (NDAM) server to provide fault information to a network management system Adapter (nmsAdapter).

Note: Never use an existing NDAM server that is configured as a subserver of the GMDR server to provide fault information to an nmsAdapter. The NDAM server will provide inconsistent fault information to the nmsAdapter.

1 Use the MDM Server Administration tool to configure a new NDAM server to restart automatically when the workstation reboots, and to start the NDAM server. For instructions to use the MDM Server Administration tool, see 241-6001-303 *Preside MDM Administrator Guide*.

The startup command for the NDAM server to enter in the tool is

`/opt/MagellanNMS/bin/ndam -n <ndam server name>`↵

where

<ndam server name> is NDAM if this is the first NDAM server to be started on the workstation, or NDAM_ followed by a name of your choice if this is the second NDAM server started on the workstation, for example NDAM_EastRegion

2 Load the Preside Multiservice Data Manager (MDM) Device Adapter software from the compact disk. See “Installing Device Adapter software” (page 57).

Chapter 5
Installing Device Adapter software

Perform these procedures to install and configure software associated with the MDM Device Adapter:

- “Installing and configuring the Preside Applications Platform software” (page 57)
- “Configuring trusted workstations” (page 58)
- “Configuring and starting the CORBA gateway” (page 60)

Perform the following procedures to load the Preside Multiservice Data Manager (MDM) Device Adapter software from CD-ROM and to configure the object request broker (ORB) software. The ORB software is included with the MDM Device Adapter software.

- “Creating an AP group and userIDs on the MDM host” (page 61)
- “Loading the MDM Device Adapter software from CD-ROM” (page 63)
- “Configuring the object request broker software” (page 66)

Installing and configuring the Preside Applications Platform software

Use this procedure to install and configure the Preside Applications Platform software.

1 Use the procedures in Preside Applications Platform, Installation and Administration Guide, 450-3101-201 to install and configure the Preside Applications Platform software. Ensure that you select the following menu items when installing the software:

Menu item	Title
2.	Install the graphical user Interface and gateway components
3.	Install the trouble ticketing adapter
6.	Install the application management agent (AMA)
7.	Install the application management building block (AMBB)
8.	Install the application management graphical user Interface (AMGUI)
9.	Install the fault management building block (FMBB)
11	Install the resource management building block (RMBB)

Note: If you do not need the historical fault browser, you do not need to install the FMBB and RMBB.

2 Perform “Configuring trusted workstations” (page 58).

Configuring trusted workstations

Use these procedures to configure the workstations that run the Graphical Network Browser (GNB) and the Preside Multiservice Data Manager (MDM) server workstation as trusted workstations.

- “Configuring the CORBA gateway host as a trusted workstation” (page 59)
- “Configuring the MDM host as a trusted workstation” (page 59)

Note: Use both of these procedures to configure trusted workstations.

You can set configuration files on a workstation to allow one user, some users, or all users on a remote workstation to log in without having to enter a a password. When all users at a remote workstation can log in without a password, the remote workstation is said to be a trusted workstation. When one user or some users can log in without a userID and password from the remote workstation, those users are said to be trusted users.

To allow autologin to start the MDM tools from a workstation that runs the GNB, the MDM workstation and the workstation that runs the GNB need to be set up as trusted workstations. These procedures tells you how to configure workstations as trusted workstations, and ensures that the /etc/hosts file on both workstations contains mappings between the hostname and IP address of the trusted workstations. This mapping is also required for autologin.

Configuring the CORBA gateway host as a trusted workstation

1. Access the workstation that runs the MDM server using the userID root.
2. Use a UNIX editor, such as vi, to open the file /etc/hosts for editing.
3. Ensure that the file /etc/hosts contains an entry that maps the IP address of the CORBA gateway workstation to its hostname.

   ```
   <IP_address> <CORBA_gateway_workstation_hostname>
   ```

   Note: The entry containing the word localhost is the MDM server workstation.
4. Save the file and exit from it.
5. Open the file /etc/hosts.equiv for editing.
6. Add the following to entries to identify the hostname of the CORBA gateway workstation and the associated GNB userIDs.

   ```
   <CORBA_gateway_workstation_hostname> admin
   <CORBA_gateway_workstation_hostname> netmgr
   ```
7. Save the file /etc/hosts.equiv and exit from the file.

Configuring the MDM host as a trusted workstation

1. Log in to the workstation that runs the CORBA gateway.
2. Using a UNIX editor, such as vi, open the file /etc/hosts for editing.
3. Ensure that the file /etc hosts contains an entry that maps the IP address of the MDM server to its hostname.

   ```
   <IP_address> <MDM_server_hostname>
   ```
4. Save the file /etc/hosts and exit from it.
5. Open the file /etc/hosts.equiv for editing.
6. Add the following entries to identify the hostname of the MDM server and the associated GNB userIDs.

   ```
   <MDM_server_hostname> admin
   <MDM_server_hostname> netmgr
   ```
7. Save the file /etc/hosts.equiv and exit from it.
8. Perform “Configuring and starting the CORBA gateway” (page 60).

Configuring and starting the CORBA gateway

Use this procedure to configure and start the CORBA gateway.

1. Login as root at the Integrated Network Management (INM) workstation.
2. Start the application management graphical user interface (AMGUI):

   `cd /opt/nortel/Preside AP07/amgui`

   `./appman`

   The Application Management Graphical User Interface window opens.
3. In the AMGUI, select Add from the Instances menu.

   The Add GUI opens.
4. In the Process Type panel, select corbagwy (CORBA gateway).
5. In the Interface field, type in the name of the interface. For example, PFI.
6. In the Hosts panel, select the name of the host on which the CORBA Gateway is to run.
7. Click on the Add button.

   The name of the new instance of the CORBA gateway appears in the AMGUI.
8. In the AMGUI window, click on the name of the new instance you just created.
9. Click on the Start button.

   The state of the CORBA gateway changes from starting to started.
10. In the AMGUI window, select the Configuration tab.
11. From the Attribute menu, select subdomain.
12. In the Value for subdomain field, type in the domain name of the resource management managed object agent (rmMoa) and the fault management managed object agent (fmMoa). Use the same subdomains for the rmMoa and the fmMoa.
13. Click on the Submit button.

    The status of in CORBA gateway changes from Configuring to Configured, then the Messages window opens.
14. Verify that the date, time, and the correct subdomain name appear in the Messages window along with the words <domain name of the rmMoa and the fmMoa> accepted.

15 Close all windows by clicking on the appropriate Close and Exit buttons.

16 On the HP workstation, log in as admin and start the gnconfig script:

```
gnconfig
```

The View Management window opens.

17 Click the on New button.

The Enter the name of the New View window opens.

18 Enter the name of the new view. This can be anything, provided it is unique.

19 Click the OK button.

The Enter the Name of New View Window closes.

20 In the View Management window, select the name of the new view and click the OK button.

The Preside Graphical Network Editor (View Name) window opens.

21 From the Controllers menu, select Add CORBA Gateway to top level.

The Controller Details window opens.

22 In the IP address field, enter the IP address of IP address of the CORBA gateway workstation.

23 Click on the Validate button.

The software validates the IP address.

The Preside Applications Platform software and the CORBA gateway are now installed and configured.

Creating an AP group and userIDs on the MDM host

Access to the GNB (AP) is restricted to specified users. Use the procedures in this section to create a UNIX group and two UNIX userIDs to access the GNB host.

The following procedures describe using the Solaris Admintool to create the the userIDs and groups. Other methods can be used to create these UNIX accounts.

Note: The passwords used for the new userIDs on the MDM host must be the same passwords used by these userIDs on the GNB host.

Creating the GNB group

1. On the MDM host, as userID root, open a UNIX xterm.
2. Launch the Solaris Admintool. Type

   `/usr/bin/admintool &`

   The Admintool window opens.
3. From the **Browse** menu, select **Groups**.

   The current window displays the existing groups.
4. From the **Edit** menu, select **Add**.

   The Admintool: Add Group window opens.
5. Type the Group Name **nocadm**.
6. Type the **Group ID** (for example, 015).
7. Type the userIDs **admin** and **netmgr**.

   This profile can be editted at a later time to add additional users.
8. Click **OK**.

   The Admintool: Add Group window closes.

   The new group is displayed with the list of existing groups.

Creating the GNB users

After using the procedure “Creating the GNB group” (page 62)

1. From the **Browse** menu of the Admintool, select **Users**.

   The current window displays the existing users.
2. From the **Edit** menu, select **Add**.

   The Admintool: Add User window opens.
3. Type the User Name **admin**.
4. Type the **Primary Group** (for example, 015).
5. Set the **Login Shell** to **C**.
6. Set the **Password** to **Normal Password**.
7. Set the **expiration date** to **None, None, and None**.
8. Set the **Path** to **/localdisk/<userID>**

where
<userID> is the new userID **admin**

9 Click the **Apply** button.

The Admintool: Add User window entries are erased.

10 Return to step 3 and create another userID named **netmgr**.

11 Click **OK**.

The Admintool: Add User window closes.

The new users are displayed with the list of existing users.

12 From the **File** menu of the Admintool, select **Exit**.

Loading the MDM Device Adapter software from CD-ROM

Use this procedure to load the MDM Device Adapter from the Preside MDM CD-ROM.

Ensure that

- a CD-ROM drive is connected to your workstation and is powered up.
- the Solaris operating system is installed and configured. Refer to the MDM Release Supplement for information about the version of Solaris required.
- the Preside MDM CD-ROMs are available.

1 Log in as the root user.

2 Start the C-shell:

```
csh
```

3 Insert the compact disk into the CD ROM drive, pattern side up. If your drive uses a disk caddy, insert the disk into the disk caddy with the pattern up, then slide the disk caddy into the CD ROM drive.

4 From the desktop, open a terminal window.

5 Start up the Sun Admintool as a background process:

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

The Admintool window opens.

6 From the Browse menu, select Software.

The Admintool window lists all software installed on the workstation.

7 From the Edit menu, select Add.

The Set Source Media window opens.

8 From Software Locations, select CD with Volume Management.

9 Type in the path name of the source media:

`/cdrom/cdrom0`

10 Click the OK button.

The Admintool:Add Software window opens and displays a list of the software on the CD.

11 Click on the package labelled:

`Passport Managed Object Agent (MOA) system - <load name>`

where:

<loadname> is the abbreviation for the MDM Device Adapter software package. For example: PM0133Pxx.

12 In the Admintool Add Software window, click the Add button.

Another Admintool: Add Software window opens. A copyright banner appears in the new window, followed by a prompt similar to the following:

```
The selected base directory </opt/MagellanMOA/loads/
PMO133Pxx must exist before installation is attempted.

Do you want this directory created now [y,n,?,q]
```

13 Enter y.

A message as follows appears:

```
This package contains scripts which will be executed
with super user permission during the installation of
this package.

Do you want to continue with the installation of
<PM0133Pxx> [y,n,?q]
```

14 Enter y.

The software begins to load. Loading can take up to eight minutes.

When loading is complete, the window displays the message:

```
Installation of <PMO133Pxx> was successful.
press <Return> to continue
```

Note: Do not press the enter key yet! You need to create a log file first.

15 Create a log file:

a. Place the cursor in the window, press and hold the right mouse button.

b. Choose History then select Store log as new file from the Term Pane menu.

c. Release the right mouse button.

A Text Save As window opens that requests information about the log file.

d. In the Save As field, type the full path name of the log file. Do not touch anything else in the Save As window.

We suggest typing in a name consisting of: /var/<load>.log.
For example: /var/PMO133Pxx.log.

e. Click on the Save button.

The software creates the specified log file and the Test Save As window closes.

f. Click in the second Admintool: Add Software window and press the return key.

The first and second Admintool: Add Software windows close.

16 From the File menu, choose Exit.

The Admintool: Software window closes.

17 Start up Sun's Admintool as a background process:

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

The Admintool window opens.

18 From the Browse menu, select Software.

The Admintool window lists all software installed on the workstation.

19 Scroll down the list of installed software and verify that the MDM Device Adapter- <load name> appears in the list of installed packages.

20 From the File menu, choose Exit

The Admintool: Software window closes.

Loading launchUI

The MDM-DA tool **launchUI** provides an interface between the GNB host and the MDM host.

1. Ensure that previously loaded device cartridge software has not already loaded this tool. Using the userID root on the MDM host, type the following at a UNIX command line:

   ```
   cd /usr/local/bin
   ```

   ```
   ls
   ```

   If the list of files includes **launchUI**, go to step 3.

2. Copy the tool **launchUI** from the CD-ROM to the MDM host.

   ```
   cd /cdrom/cdrom0/opt/MagellanMOA/bin/launchUI
   /usr/local/bin/.
   ```

3. Eject the compact disk. Type the following at a UNIX command line:

   ```
   eject cdrom
   ```

Configuring the object request broker software

Use this procedure to configure the object request broker (ORB) software that is included with the MDM Device Adapter software. Configure the ORB by adding the location of the workstation that runs the OrbixTrader to the common.cfg configuration file, and ensure that the Orbix daemon is running.

1. Log in as the root user.
2. Access the directory that contains the /etc/hosts file:

   ```
   cd/etc
   ```

3. Use a UNIX editor, such as vi, to open the hosts file for editing.
4. Ensure that the host name and IP address of the workstation that is running the OrbixTrader appears in the /etc/hosts file. If not, add them.
5. Save the file and exit from it.
6. Log in to HP running the OrbixTrader as the admin user.
7. Go to the config directory:

   ```
   cd /opt/iona/config
   ```

8. Edit the file comon.cfg on an HP workstation. Locate the following line:

```
Services{
TradingService=”IOR:000...020”;
};
```

Note: If the line is not present, ensure that Preside Application Platform installation is complete. If the installation is complete, contact Nortel Networks.

9 On the Preside MDM Device Adapter machine, enter the following command, using a UNIX editor, such as vi:

`vi /opt/MagellanMOA/3rdparty/Orbix_3.3.1MT/config/common.cfg`

10 Locate the following entry:

```
Services
      {
            TradingService= "";
      };
```

11 Copy the section in quotes (IOR:000...020) from step 8 in the empty section:

```
TradingService="";
```

The entry should look like the following:

```
Services{

TradingService="IOR:000000000000002249444c3a6f6d672e6
f72672f436f7354726164696e672f4c6f6f6b75703a312e300000
0000000010000000000000008a0001010000000009776b706b683
0336400003a99000000303a3e0233311b776b706b683033640054
726164696e675365727696365504f41000e54726164696e67536
5727669636500000003000000000000000800000000049545f4100
0000010000001800000000000010001000000010501000100010010
900000000000000060000006000000000020";
 };
```

Note: If the editor splits the IOR into multiple lines, you will need to join them into one line. In vi, this can be done using shift-j, and then deleting the space used to replace the line feeds.

12 Display the status of the Orbix daemon:

`ps -ef | grep orbixd`

Responses similar to the following example mean that the Orbix daemon is running. A blank line means that the Orbix daemon is not running.

```
root 3079 3076 0 09:50:45 ? 0:00 orbixd -u
root 3076 1 0 09:50:44 /bin/csh /opt/MagellanMOA/bin/
moaLaunch orbixd -u
```

13 Does the response show that the Orbix daemon is running?

If the Orbix daemon	Then
is running	Stop the orbixd by issuing the process ID (pid)returned in step 12. In this step, the command is kill -15 3079. Then continue with step 15.
is not running	Go to step 14.

14 Start the Orbix daemon:

```
addToInittab 0 orbixd -u
```

15 Wait for approximately 10 seconds, then return to step 12 and display the status of the Orbix daemon again. If the Orbix daemon is not running after a second attempt, contact Nortel Networks support.

Chapter 6
Filtering fault information

This section contains optional procedures to set up filtering of fault information that the Network Data Access Mediator (NDAM) server supplies to the network management system Adapter (nmsAdapter). To set up filtering you must configure the following files:

- typeset files and deviceset files for the NDAM server
- the deviceTypeSetFilters file for the nmsAdapter

If you do not perform any of the procedures in this chapter, then by default, the nmsAdapter receives fault information from all of the devices monitored by the NDAM server.

Perform the following tasks to set up filtering:

- "Understanding filtering" (page 69)
- "Creating configuration files" (page 80)

Understanding filtering

In large networks, the Network Data Access Mediator (NDAM) server provides the network management system Adapter (nmsAdapter) with large amounts of information. You can limit the amount of information using combinations of the following types of configuration files:

- typeset and deviceset configuration files used by the NDAM server on MDM
- the deviceTypeSetFilters configuration file used by the nmsAdapter

Purposes of typeset, deviceset, and deviceTypeSetFilters files

A typeset file specifies the types of nodes and subcomponents for which the Network Data Access Mediator (NDAM) server provides fault information to the network management system Adapter (nmsAdapter).

A deviceset file specifies the names of devices for which the NDAM server provides fault information.

A deviceTypeSetFilters file specifies one or more typeset files and deviceset files that the NDAM server is to use for filtering fault information that it provides to an nmsAdapter. It can also contain optional statements that further exclude fault information that the NDAM server provides.

How the nmsAdapter and NDAM server use typeset, deviceset, and deviceTypeSetFilters files

When you start the network management system Adapter (nmsAdapter), the nmsAdapter reads the contents of the deviceTypeSetFilters file and creates a registration request that it sends to the NDAM server that is specified in the ndam.hosts configuration file. This registration request includes the identities of the typeset and deviceset files that the NDAM server is to use for filtering, along with any optional exclusion statements that you specify in the deviceTypeSetFilters file. When it receives the request, the NDAM server:

1 scans all typeset files for the criteria needed to filter the fault information according to the component type

2 scans all deviceset files to determine criteria to filter the fault information according to the device name

3 scans the additional exclusion statements provided in the request

4 begins forwarding the filtered fault information to the nmsAdapter

Statements in typeset, devicesets, and deviceTypeSetFilters files

See the following sections for the structure of statements in the three types of files:

- "Typeset files" (page 71)
- "Deviceset files" (page 72)
- "DeviceTypeSetFilters file" (page 73)

Typeset files

Typeset files can contain statements that include nodes and their subcomponents, or exclude them.

Samples of include statements are as follows:

```
EM          # includes information from all Passport
            # 6420, 6440, 6480,7480, 8780, 15000.
MPA         # includes information from all Passport
            # 4400 nodes, but not their subcomponents
PM          # includes information from all DPN-100
            # and Passport 4120 nodes, but not their
            # subcomponents
EM-*        # includes information from all Passport
            # 6420, 6440, 6480, 7480, 8780, and 15000,
            # subcomponents
EM-DS1      # includes information about DS1s on
            # all Passport 6420,6440, 6480, 7480,
            # 8780, 15000
PM-*        # includes information about all DPN-100
            # and Passport 4120 subcomponents
```

```
PTK:            # includes information about all
                # priority trunk (PTK) links
*:              # includes information about all links
include         # includes information about the types
NDAM_MPA.typ    # of nodes and subcomponents defined in
                # the NDAM_MPA.typ file
```

Samples of exclude statements are as follows:

```
!EM             # excludes information from all Passport
                # 6420, 6440, 6480,7480, 8780, and 15000.
!EM-*           # excludes information from all Passport
                # 6420, 6440, 6480,7480, 8780, and 15000 subcompo-
                nents
!EM-DS1         # excludes information about DS1s on
                # all Passport 6420,6440, 6480, 7480,
                # 8780, 15000
!PTK:           # excludes information about all
                # priority trunk (PTK) links
```

Note: When adding statements to a typeset file, insert statements without wild cards (the most specific entries) ahead of those with wild card characters (the least specific).

Deviceset files

deviceset files can contain statements that include devices or exclude them.

Samples of include statements are as follows:

```
EM *            # includes information from all Passport
                # 6420, 6440, 6480,7480, 8780, and 15000
                # devices.
MPA *           # includes information from all Passport
                # 4400s regardless of their names
PM *            # includes information from all DPN-100
                # and Passport 4120 regardless of
                # their names
```

```
EM NODER*              # includes information from all
                       # Passports whose names begin with NODER
EM NODER99             # includes information about a Passport
                       # whose name is NODER99
include NDAM_MPA.dev   # includes information about all
                       # devices and components named in the
                       # NDAM_MPA.dev file
```

Samples of exclude statements are as follows:

```
!EM *                  # excludes information from all Passport
                       # 6420, 6440, 6480, 7480, 8780, 15000,
                       # and iBWA 5100 devices, regardless of
                       # their names
!EM NODER*             # excludes information from all Passports
                       # whose names begin with NODER
!EM NODER99            # excludes information from the Passport
                       # whose name is NODER99
```

Note: When adding statements to a typeset file, insert statements without wild cards (the most specific entries) ahead of those with wild cards (the least specific).

DeviceTypeSetFilters file

Sample statements in a deviceTypeSet Filters file are as follows:

```
nmTypeSet: ALL_MPA     # causes the NDAM server to use a
                       # file called NDAM_ALL_MPA.typ
                       # for filtering network model
                       # information
gmdrTypeSet: EXCL_OA   # causes the NDAM server to use a
                       # file called NDAM_EXCL_OA.typ
                       # for filtering GMDR information
nmDeviceSet: ALL_EM    # causes the NDAM server to use a
                       # file called NDAM_ALL_EM.dev
                       # for filtering network model
                       # information
```

```
gmdrDeviceSet: EXCL_CORENCS     # causes the NDAM server to use a
                                # file called
                                # NDAM_EXCL_CORENCS.dev for
                                # filtering GMDR information
nmTypeExcl: !PTK:               # is an optional statement that
                                # excludes network model
                                # information about priority
                                # trunks (PTK)
gmdrTypeExcl: !EM-*             # is an optional statement that
                                # excludes gmdr information about
                                # Passport components
nmDeviceExcl: !OA               # is an optional statement that
                                # excludes network model
                                # information about DPN
                                # Operational Agents and their
                                # components
gmdrDeviceExcl: !PM CORENCS     # is an optional statement that
                                # excludes gmdr information about
                                # all DPN or Passport 4120 devices
                                # called CORENCS
```

Considerations for creating typeset files and deviceset files

Considerations are as follows:

- Create typeset files and deviceset files as needed. Here is how this optionality affects the way the NDAM server filters fault information for the network management system Adapter (nmsAdapter):

If you	Then NDAM
do not create any typeset files or deviceset files	forwards information from the types of nodes and subcomponents defined in the typeset files regardless of their names

If you	Then NDAM
create typeset files but no deviceset files	forwards information from the types of nodes and subcomponents defined in the typeset files regardless of their names
create deviceset files but no typeset file	NDAM forwards information from all devices named in the deviceset files, regardless of their type
create typeset files and deviceset file	NDAM only forwards information from the types of nodes and subcomponents specified in the typeset files that have the device names specified in the deviceset files

- We suggest that you consider filtering information from the network model and from the GMDR server separately. Here is why:

If the	Then
NMSERVER provides node and subcomponent status information from the network model to the nmsAdapter	Initial start-up is much faster if the software has no or few subcomponents to deal with
GMDR server provides alarms from devices and subcomponents to the nmsAdapter.	any alarm that originates on an IP device or component contains the IP address of the device. You need to ensure that the nmsAdapter is notified of the IP address so that the Preside Applications Platform tool can receive and display the new alarm as soon as possible

Note: One way to satisfy these opposing requirements is to create a set of typeset and deviceset filters for information supplied by the GMDR server and a second set for information supplied from the network model.

- Ensure that the combination of type set files and deviceset files produces the filtering required without conflicting statements.
- As soon as you create the first typeset file, the nmsAdapter only receives information from the types defined in that typeset file. The typeset file, must therefore contain definitions that let NDAM provide fault information from all types of devices that you wish to monitor through the nmsAdapter. Alternatively, you must create several typeset files that collectively define all of the types required. The same applies to deviceset files.

- Because the NDAM server reads typeset files first followed by deviceset files, we recommend that you create typeset files first to filter information according to node and subcomponent type, then create the deviceset files to further refine the filtering according to device name. Procedures in this chapter create the files in this order.

Sample set of typeset, deviceset, and deviceTypeSetFIlters files

The following sections contain examples that show how you can use typeset, deviceset, and deviceTypeSetFilters files to filter information that the Network Data Access Mediator (NDAM) server provides to the network management system Adapter (nmsAdapter).

The first four files are for a typical nmsAdapter installation. We did not modify these files because they are already being used to filter information for client applications other than nmsAdapters. Instead, we added entries to the deviceTypeSetFilters file to call up these typeset and deviceset files by, then we added extra entries to the deviceTypeSetFilters file to exclude information that is not intended for the nmsAdapter.

NDAM_ALL_EM.typ

```
#
#   NDAM Passport Device Filterset
#
#   This filterset allows information for Passport nodes
#   but no other type of node.
#
EM *
```

NDAM_ALL_DPN.typ

```
#
#     NDAM DPN Type Filterset
#
#     This filterset allows information for all DPN-100 nodes
#     Passport 4120 nodes, their subcomponents, and links.
#
PM    # includes DPN-100 and Passport 4120 nodes
PM-*  # includes DPN-100 and Passport 4120 subcomponents
OA    # includes all DPN NCS Operations Agents
OA-*  # includes all DPN NCS Operations Agent subcomponents
```

```
NL:   # includes all DPN Network Links and Passport Gateway
      # links
TK:   # includes all DPN trunks and DPN Gateways
DBNL: # includes all DPN Dial Backup Network Links
BWOD: # includes all DPN Bandwidth on Demand Network Links
DNL:  # includes all Dynamic Network Links
MPANL:# includes all Passport 4120 Multi-Protocol Access
      # Network Links
```

NDAM_ALL_MPA.typ

```
#
# NDAM Passport 4400 Type Filterset
# This filterset allows information for all Passport
# 4400 modules, subcomponents, and links
#
MPA       #includes all Passport 4400 and LDM nodes
MPA-*     #includes all Passport 4400 and LDM components
MPANL:    #includes Multprotocol Passport Access Network
          #Links
```

NDAM_ALL_EM.dev

```
#
# NDAM Passport Device Filterset
# This filterset allows information for all Passport modules.
#
EM *
```

deviceTypeSetFilters

```
# NDAM typeset Filters
                        #
nmTypeSet: All_EM       # causes NDAM to use the
                        # NDAM_ALL_EM.typ typeset file
                        # to filter information about
                        # Passport 6420, 6440, 6480,
                        # 7480, 8780, and 15000
                        # from the network model
                        #
nmTypeSet: ALL_DPN      # causes NDAM to use the
                        # NDAM_ALL_DPN.typ typeset file
                        # to filter information about
                        # DPN-100 and Passport 4120
                        # from the network model.
```

```
                        #
nmTypeSet: ALL_MPA      # causes NDAM to use the
                        # NDAM_ALL_MPA.typ typeset file
                        # to filter information
                        # about Passport4400s from
                        # the network model.
                        #
nmTypeExcl: !EM-*       # excludes network model
                        # information about Passport
                        # subcomponents from information
                        # allowed through by the
                        # NDAM_ALL_EM.typ file.
                        #
nmTypeExcl: !PTK        # excludes network model
                        # information about priority
                        # trunks (PTK) from information
                        # allowed through by the
                        # NDAM_ALL_EM.typ file.
                        #
nmTypeExcl: !MPA-*      # excludes network model
                        # information about
                        # Passport 4400 subcomponents from
                        # information allowed through
                        # by the NDAM_ALL_MPA.typ file.
                        #
nmTypeExcl: !MPANL:     # excludes network model
                        # information about Multi-Protocol
                        # Network Access Links (MPANL)
                        # from information allowed through
                        # by the NDAM_ALL_MPA.typ file.
                        #
nmTypeExcl: !PM-*       # excludes network model
                        # information about DPN-100
                        # and Passport 4120 subcomponents
                        # from information allowed through
                        # by the NDAM_ALL_DPN.typ file
                        #
nmTypeExcl: !OA-*       # excludes network model
                        # information about DPN-100
                        # and Passport 4120 Operational
                        # Agent (OA) subcomponents from
                        # information allowed through by the
                        # NDAM_ALL_DPN.typ file
```

```
                        #
nmTypeExcl: !NL:        # excludes network model
                        # information about network
                        # links (NL) from information
                        # allowed through by the
                        # NDAM_ALL_DPN.typ file
                        #
nmTypeExcl: !TK:        # excludes network model
                        # information about trunks
                        # trunks (TK) from information
                        # allowed through by the
                        # NDAM_ALL_DPN.typ file
                        #
nmTypeExcl: !DBNL:      # excludes network model
                        # information about Dial
                        # Backup Network Links (DBNL) from
                        # information allowed through by
                        # the NDAM_ALL_DPN.typ file.
                        #
nmTypeExcl: !BWOD:      # excludes network model
                        # information about Bandwidth
                        # On Demand (BWOD) links from
                        # information allowed through by the
                        # NDAM_ALL_DPN.typ file
                        #
nmTypeExcl: !DNL:       # excludes network model
                        # information about Dynamic
                        # Network Links (DNL) from
                        # information allowed through by
                        # the NDAM_ALL_DPN.typ file.
                        #
nmTypeExcl: !MPANL:     # excludes network model
                        # information about Passport
                        # 4120 Multi-protocol Access Network
                        # links (MPANL) from information
                        # allowed through by the
                        # NDAM_ALL_DPN.typ file
                        #
gmdrTypeExcl: !EM-*     # excludes GMDR information about
                        # Passports from the information
                        # allowed through by the
                        # NDAM_ALL_EM.typ file
```

```
# NDAM deviceset Filters
                        #
nmDeviceSet: ALL_EM     # causes NDAM to use the
                        # NDAM_ALL_EM.dev file to filter
                        # information about
                        # Passport devices
                        # from the network modelnetwork
                        # model


gmdrDeviceSet: ALL_EM

# causes NDAM to uses the
                        # NDAM_ALL_EM.dev file to filter
                        # information about Passport devices
                        # from GMDR
```

Creating configuration files

Use the following procedures to create configuration files.

- “Creating typeset and deviceset files on MDM for NDAM” (page 80)
- “Creating the deviceTypeSetFilters configuration file” (page 82)

Use this optional procedure to create typeset and deviceset configuration files on the Preside Multiservice Data Manager (MDM) Device Adapter workstation that the Network Data Access Mediator (NDAM) server is to use for filtering fault information that the NDAM server supplies to an netowrk management system Adapter (nmsAdapter).

Creating typeset and deviceset files on MDM for NDAM

If you do not understand how typeset files, deviceset files, and the deviceTypeSetFilters file work together to filter fault information, read “Understanding filtering” (page 69).

1. Choose the method you want to use to limit the fault information that NDAM supplies to the nmsAdapter: according to the typeset, according to the device name, or according to both the device namen and the typeset.
2. Log in as the root user at the MDM workstation that is going to run the NDAM server.

3 Access the /opt/MagellanNMS/cfg directory:

```
cd /opt/MagellanNMS/cfg
```

4 Do one of the following:

If you decided to create	Then go to
typeset files	step 5
deviceset files	step 9
deviceset files and typeset files	step 5

5 Use a UNIX editor, such as the text editor provided with the Solaris Common Desktop Environment, to open a new typeset file for editing.

6 Add entries that define the types of devices and components for which NDAM is to provide fault information.

Note: When creating entries, place entries without wild card characters (*) ahead of entries without wild card characters. For more information about entries in a typeset file, see “Typeset files” (page 71). For an example of a typeset file, see “Sample set of typeset, deviceset, and deviceTypeSetFIlters files” (page 76).

7 Save the file with a name that has a prefix of NDAM, an underscore, a file name, and an extension of .typ and exit the file. An example of a file name for a typeset file is NDAM_ALL_EM.typ.

8 Ensure that the file permissions are set correctly:

```
chmod 775 /opt/MagellanNMS/cfg/<typeset file name>
```

9 Use a UNIX editor, such as the text editor provided with the Solaris Common Desktop Environment, to open a new deviceset file for editing.

10 Add entries that define the names of devices for which NDAM is to provide fault information.

Note: When you create entries, place entries without wild card characters (*) ahead of entries with wild card characters. For more information about deviceset files, see “Deviceset files” (page 72). For an example of a deviceset file, see “Sample set of typeset, deviceset, and deviceTypeSetFIlters files” (page 76).

11 Save the file with a name that has a prefix of NDAM, an underscore, a file name, and an extension of .dev and exit the file. An example of a file name for a deviceset file is NDAM_ALL_DPN.dev

12 Ensure that the file permissions are set correctly:

```
chmod 775 /opt/MagellanNMS/cfg/<deviceset file name>
```

13 Display a list of the NDAM servers that are running on the MDM workstation

```
ps -ef | grep NDAM
```

The machine replies with a response similar to the following:

```
root 22780 18884 0 08:19:10 ? 0:00 ndam -g localhost -
m localhost
```

14 Send a signal to the NDAM server to cause it to reload the information from the typeset and deviceset files

```
kill -1 <process id>
```

where

<process id> is the process identifier of the NDAM server. In this example, the process id is 22780.

15 Create a deviceTypeSetFilters file, as described in "Creating the deviceTypeSetFilters configuration file" (page 82).

Creating the deviceTypeSetFilters configuration file

Use this procedure to create an optional deviceTypeSetFilters configuration file to filter information that the Network Data Access Mediator (NDAM) server supplies to the network management system Adapter (nmsAdapter).

1 Ensure that you have created the typeset files and deviceset files that you are going to specify in the deviceTypeSetFilters file, as described in "Creating typeset and deviceset files on MDM for NDAM" (page 80).

2 Log in as root on the workstation that is going to run the nmsAdapter.

3 Using a text editor, such as the text editor supplied with the Solaris operating system, open the /opt/MagellanMOA/cfg/Mdr/deviceTypeSet Filters file for editing.

4 Add entries to the deviceTypeSetFilters configuration file that specify the typeset and deviceset files that NDAM will use for filtering GMDR and network model information that is supplied to the nmsAdapter.

5 Add additional statements that further exclude information from the NDAM server beyond the limitations defined in the typeset and deviceset files you specified in step 4.

For more information about deviceTypeSetFilters files, see "DeviceTypeSetFilters file" (page 73). For an example of a deviceTypeSetFilters file, see "Sample set of typeset, deviceset, and deviceTypeSetFIlters files" (page 76).

6 Save the file and exit from it.

7 Ensure that the file permissions are correct on the newly created file:

```
chmod 775 /opt/MagellanMOA/cfg/Mdr/
deviceTypeSetFilters
```

8 Stop the nmsAdapter. See "Stopping a Preside MDM Device Adapter application" (page 93).

9 Restart the nmsAdapter. See "Starting the nmsAdapter" (page 87).

Chapter 7
Starting MDM Device adapter applications

This section contains procedures for setting up configuration files and for starting the network management system Adapter (nmsAdapter), the fault management managed object agent (fmMoa), and the resource management managed object agent (rmMoa).

This section contains information about the following topics:

Adding the location of the NDAM server to the ndam.hosts configuration file

Use this procedure to specify

- the location of the primary network data access mediator (NDAM) server that provides an nmsAadapter with fault information from MDM
- optionally, the location of a backup NDAM server that can provide the fault information if the primary NDAM server fails, or if the connection to the primary NDAM server fails

1 Log in as the root user on the workstation that is going to run the nmsAdapter.

2 Copy the template ndam.hosts file to the cfg directory:

```
cp /opt/MagellanMOA/cfg/Template/Mdr/ndam.hosts
/opt/MagellanMOA/cfg/Mdr
```

3 Use a text editor, such as the text editor supplied with the Solaris operating system, to open the /opt/MagellanMOA/cfg/Mdr/ndam.hosts file for editing.

4 Use the following syntax to add a line to the file that specifies the location of the primary NDAM server:

```
ndamServer: NDAM[<_service name>]@<host | ip_address>
```

where

[<_service name>] is the service name of the NDAM server on MDM. If there is only one NDAM server running on the workstation that has MDM, just enter NDAM and omit the service name. If however, there are two NDAM servers running on the workstation they must have unique names. The first can be called NDAM but the second must have a name that consists of NDAM, an underscore, and a service name that distinguishes it from all other NDAM servers on the workstation, for example, NDAM_PARIS1

<host | ip address> is the host name or the IP address of the workstation on which the NDAM server is running. To use the host name instead of the IP address, there must be an entry in the /etc/hosts file that maps the workstation's common name to its IP address. If there is no mapping in the /etc/hosts file, you must specify the IP address.

When the primary NDAM server runs on the same workstation as the nmsAdapter and other MDM Device Adapter applications, the first entry in the file is:

ndamServer: NDAM@localhost

5 Add a second entry below the first that specifies the location of an optional backup NDAM server that can provide fault information from MDM if you cannot reach the primary NDAM server.

6 Save the file and close it.

7 Ensure that the file permissions are set to read-write-execute for the user, and read-execute for the group and for others:

```
chmod 775 /opt/MagellanMOA/cfg/Mdr/ndam.hosts
```

8 Start the nmsAdapter(s), see “Starting the nmsAdapter” (page 87).

Starting the nmsAdapter

Use this procedure to start the network management system Adapter (nmsAdapter) from the command line. This procedure adds the startup command for the nmsAdapter to the /etc/inittab file to ensure that the nmsAdapter restarts automatically after a reboot.

1 Ensure that you have configured the ndam.hosts file as described in “Adding the location of the NDAM server to the ndam.hosts configuration file” (page 85).

2 Log in as the root user.

3 Start the C-shell:

```
csh
```

4 Source the environment variables needed to start the application without entering the full path name of the addToInittab command:

```
source /opt/MagellanMOA/bin/moaEnvVars.csh
```

5 Enter the following command to start the nmsAdapter:

```
addToInittab <restart_delay> /opt/MagellanMOA/bin/
nmsAdapter <unique identifier> -d <domain>
-propagateMsgAlarms <0|1> -ipAddressPolling <polling
interval>
```

where

<restart_delay>	is the time in seconds that the software (init process) waits before attempting to restart the nmsAdapter if the nmsAdapter halts. We suggest an initial value of 10 for this parameter
<unique identifier>	is a string that uniquely identifies the nmsAdapter. Although you can specify any unique string, we recommend the scheme nmsAdapter_<hostname>_<domain>.
-d <domain>	is the name of the nmsAdapter's domain, See also "Planning domains and subdomains with redundancy" (page 37).
-propagateMsg Alarms <0|1>	To receive message alarms, set this optional parameter to `1`. The default is `0`; do not receive message alarms.
-ipAddressPolling <polling interval>	is the time interval (in seconds) that the IP address gets polled.

Example:

```
addToInittab 10 /opt/MagellanMOA/bin/nmsAdapter \
nmsAdapter_host1_PARISE -d PARISE \
-propagateMsgAlarms 1 -ipAddressPolling 30
```

6 Display the status of the nmsAdapter you just started:

`ps -ef | grep <unique identifier>`

Example:

`ps -ef | grep nmsAdapter_host1_PARISE`

A response similar to the following appears which indicates that the nmsAdapter is running:

```
root 19332 21481  0 16:11:17 pts/1 /opt/MagellanMOA/
bin/nmsAdapter nmsAdapter_host1_PARISE -d PARISE
```

7 Start the FM MOA from the command line, see "Starting the fmMoa" (page 89).

Starting the fmMoa

Use this procedure to start the fault management managed object agent (fmMoa) from the command line. This procedure adds the startup command for the fmMoa to the /etc/inittab file to ensure that the fmMoa restarts automatically after a reboot.

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

   ```
   csh
   ```

3. Source the environment variables needed to start the application without entering the full path name of the addToInittab command:

   ```
   source /opt/MagellanMOA/bin/moaEnvVars.csh
   ```

4. Enter the following command to start the fmMoa:

   ```
   addToInittab <restart_delay> /opt/MagellanMOA/bin/
   fmMoa <unique identifier> -d <domain>
   -s <“subdomain1 subdomain2 ...”>
   ```

where

<restart_delay>	is the time in seconds that the software (/etc/inittab process) waits before attempting to restart the fmMoa if the fmMoa halts. We recommend an initial value of 10 for this parameter.

where

<unique identifier>	is a unique identifier for the fmMoa. Although you can specify any unique string for this identifier, we recommend the scheme fmMOA_<hostname>_<domain>.
-d <domain>	is the name of the fmMoa's domain. See also "Planning domains and subdomains with redundancy" on page 37
-s <"subdomain1 subdomain2...">	is a list of the subdomains that belong to the fmMoa. The subdomain names must be enclosed in double quotation marks, and each must be a domain name you assigned to an nmsAdapter in "Adding the location of the NDAM server to the ndam.hosts configuration file" (page 85).

Example:

```
addToInitab 10 /opt/MagellanMOA/bin/fmMoa
fmMOA_host1_PARIS -d PARIS -s "PARISE PARISW"
```

5 Display the status of the fmMoa you just started:

`ps -ef | grep <unique identifier>`

Example:

```
ps -ef | grep fmMoa_host1_PARIS
```

A response similar to the following appears which indicates that the fmMoa is running:

```
root 19332 21481  0 16:11:17 pts/1 /opt/MagellanMOA/
bin/
fmMoa fmMoa_host1_PARIS -d PARIS -s "PARISE PARISW"
```

6 Start the rmMoa from the command line, see "Starting the rmMoa" (page 90).

Starting the rmMoa

Use this procedure to start the resource management managed object agent (rmMoa) from the command line. This procedure adds the startup command for the rmMoa to the /etc/inittab file to ensure that the rmMoa restarts automatically after a reboot.

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

   csh

3. Source the environment variables needed to start the application without entering the full path name of the addToInittab command:

   source /opt/MagellanMOA/bin/moaEnvVars.csh

4. Enter the following command to start the rmMoa:

   addToInittab <restart_delay> /opt/MagellanMOA/bin/rmMoa <unique identifier> -d <domain> -s <"subdomain1 subdomain2 ...">

where

<restart_delay>	is the time in seconds that the software (/etc/inittab process) waits before attempting to restart the rmMoa after the rmMoa halts. We recommend an initial value of 10 for this parameter.
<unique identifier>	is a unique identifier for the rmMoa. Although you can specify any unique string for this identifier, we recommend the scheme rmMoa_<hostname>_<domain>.
-d <domain>	is the name of the rmMoa's domain, see also "Planning domains and subdomains with redundancy" on page 37
-s <"subdomain1 subdomain2...">	is a list of the subdomains that belong to the rmMoa. The list of subdomain names must be enclosed in double quotation marks, and each subdomain must match the domain name you assigned to an nmsAdapter in "Adding the location of the NDAM server to the ndam.hosts configuration file" (page 85).

Example:

```
addToInittab 10 /opt/MagellanMOA/bin/rmMoa
rmMoa_host1_PARIS -d PARIS -s “PARISE PARISW”
```

5 Display the status of the rmMoa you just started:

`ps -ef | grep <unique identifier>`

Example:

```
ps -ef | grep rmMoa_host1_PARIS
```

You should get a response similar to the following to indicate that the rmMoa is running:

```
root 19332 21481  0 16:11:17 pts/1 /opt/MagellanMOA/
bin/rmMoa rmMoa_host1_PARIS -d PARIS -s “PARISE
PARISW”
```

6 If you need to set up filtering to limit the amount of fault information that the NDAM server provides to an nmsAdapter, see “Creating typeset and deviceset files on MDM for NDAM” (page 80). Otherwise, you have completed the installation process.

Chapter 8
Administering MDM Device Adapters

This section contains procedures to perform after you install and configure the Preside Multiservice Data Manager (MDM) Device Adapter software. Select one of the following tasks:

Stopping a Preside MDM Device Adapter application

Use this procedure to stop one of the following applications:

- network management system Adapter (nmsAdapter)
- fault management managed object agent (fmMoa)
- resource management managed object agent (rmMoa)

1. Log in as root.
2. Source the environment variables needed stop the application without entering the full path name of the removeFromIInitttab command:

   ```
   source /opt/MagellanMOA/bin/moaEnvVars.csh
   ```

3. Display a list of the applications of the type you want to stop that are running on the workstation.

ps -ef | grep <name>

where:

<name> is the name of the application you want to stop: nmsAdapter, rmMoa, or fmMoa.

A list of all of the running applications with the type of <name> appears on the screen. For example, for two nmsAdapters:

```
root 388 333 0 Aug 08 pts/1 1:12 /opt/MagellanMOA/bin/
nmsAdapter nmsAdapter_host1_PARISE -d PARISE
```

```
root 389 334 0 Aug 08 pts/1 2:20 /opt/MagellanMOA/bin/
nmsAdapter nmsAdapter_host2_PARISW -d PARISW
```

4 Find the unique identifier of the application you want to stop.

5 Remove the startup command from the /etc/inittab file so that the application does not restart automatically when the workstation reboots:

removeFromInittab <unique identifier>

Example:

```
removeFromInittab nmsAdapter_host1_PARISE
```

6 Display the process identifier of the application:

ps -ef | grep <unique identifier>

Example:

```
ps -ef | grep nmsAdapter_host1_PARISE
```

The system produces a response like the following example, in which 2381 is the process_id:

```
root 2381 23809 0 Jan 10 tty1 22:33 /opt/MagellanMOA/
bin/nmsAdapter nmsAdapter_host1_PARISE -d PARISE
```

7 Stop the application process:

kill -9 <process id>

Example:

```
kill -9 2381
```

Removing the Preside MDM Device Adapter software

Use this procedure to remove the Preside Multiservice Data Manager (MDM) Device Adapter software from the workstation.

1. To allow the Preside Applications Platform tools to continue to function, ensure that there are redundant instances of the network management system Adapter (nmsAdapter), fault management managed object agent (fmMoa), and resource management managed object agent (rmMoa) on another workstation.
2. Log in as the root user.
3. Start the C-shell:

   `csh`
4. Start Sun's Admintool as a background process:

   `/usr/bin/admintool &`

   The Admintool window opens.
5. From the Browse menu, select Software.

   The Admintool window lists all software installed on the workstation.
6. Scroll down the list of software and click on the name of the software to select it. For example, click on Passport Managed Object Agent (MOA) System PMO041PabS2600

   Note: From the Edit menu, select Delete.

   A warning dialog opens.
7. Select **Delete**.

   The Admintool: Delete Software dialog opens and contains a message similar to the following example:

   ```
   The following package is currently installed:
   PMO041Pab Passport Managed Object Agent (MOA) System
                        (sparc) Release 020

   Do you want to remove this package?
   ```
8. Type **y**.

   A message like the following example appears:

   ```
   ## Removing installed package instance <PM0041Pab>

   This package contains scripts which will be executed
   with super-user permission during the process of
   removing this package.

   Do you want to continue with the removal of this
   package [y,n,?,q]
   ```

9 Type **y**.

The Admintool begins removing the package. When the removal is complete, a message like the following example appears:

```
15:56:22 NOTE: <postremove> - completed successfully.

## Updating system information.

Removal of <PMO041Pab> was successful.
Press return to continue.
```

10 Press the return key.

The Admintool: Delete Software dialog closes.

Note: In the Admintool: Software window, select Exit from the File menu.

The Admintool: Software window closes.

Removing a Passport 6420, 6480, 7480, 8780, or 15000

Use this procedure to remove a Passport 6420, 6480, 7480, 8780 or 15000 device from the graphical network browser (GNB). To remove the device, perform the following tasks:

- remove information about the Passport from file /opt/MagellanNMS/cfg/HGDS.cfg on the Preside Multiservice Data Manager (MDM) workstation
- restart the FMIP management data router (FMDR) server
- restart the host group directory (HGDS) server
- remove information about the Passport and its subcomponents from the general management data reporter (GMDR) server database
- delete information about the Passport from the network model

For more information about the servers in this procedure, including how to stop and start them, see 241-6001-303 *Preside MDM Administrator Guide*.

1 Log in as the root user.

2 Start the C-shell.

csh

3 Source the MDM environment variables.

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

4 Start MDM.

```
/opt/MagellanNMS/bin/nmstool &
```

A copyright dialog opens.

5 In the copyright dialog, click OK.

The copyright dialog closes, and after a delay, the MDM Toolsets window opens.

6 In the MDM Toolsets window, select System -> Administration -> Server Administration.

The Server Administration window opens.

7 Stop the FMDR server for the Passport group that contains the Passport you are to remove.

8 Stop the HGDS server.

9 Edit the /opt/MagellanNMS/cfg/HGDS.cfg file to delete the entry for the Passport to be removed.

10 Restart the HGDS server.

11 Restart the FMDR server.

12 In the MDM Toolsets window, select System -> Administration -> GMDR Administration.

The main window of the GMDR Administration tool opens.

13 In the main window of the GMDR Administration tool, select Show Components.

The Show Components dialog opens.

14 Find the name of the Passport in the components panel of the Show Components dialog and click on the name of the Passport.

The name of the Passport becomes highlighted to indicate that it is selected.

15 Click the Delete button.

The Passport and its components disappear from the Show Components dialog.

16 In the MDM Toolsets window, select System -> Administration -> Server Administration.

The Server Administration window opens.

17 Use Server Manager Administration to ensure the network model editor server (EDSERVER) is created and running.

If the EDSERVER is not created and running, create it and start it using the following start-up command.

`/opt/MagellanNMS/bin/edserver`

18 In the MDM Toolsets window, select Fault -> Network Viewer.

The Network Viewer window opens.

19 From the Network Model Edit menu, select:

`Enable Network Model Editing`

20 Click on the icon of the node you want to delete.

21 Using the right mouse button select:

`Edit-> Delete`

The Delete Components window opens.

22 Click on the Delete button.

The node icon disappears from the Network Viewer window.

23 From the Network Model Edit menu, select:

`Leave Network Model Editing`

The Leave Editing Network Model window opens.

24 Click the on the Exit and Save button.

25 From the File menu, select:

`Exit`

If you are asked to confirm the exit, click on the Exit and Save button.

26 The Network Viewer window closes. If you have the graphical network browser open, the icon for the node you just have deleted disappears from the browser.

Removing a Passport 4400

Use this procedure to remove a Passport 4400 from the Graphical Network Browser (GNB). To remove the node, perform the following tasks:

- remove information about the Passport 4400 and its subcomponents from the general management data reporter (GMDR) database
- delete information about the Passport 4400 from the network model

For more information about the servers in this procedure, including how to stop and start them, see 241-6001-303 *Preside MDM Administrator Guide*.

1 Log in as the root user.

2 Start the C-shell.

```
csh
```

3 Source the MDM environment variables.

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

4 Start MDM.

```
/opt/MagellanNMS/bin/nmstool &
```

A copyright dialog opens.

5 In the copyright dialog, click on the OK button.

The copyright dialog closes, and after a delay, the MDM Toolsets window opens.

6 In the MDM Toolsets window, select System -> Administration -> GMDR Administration.

The main window of the GMDR Administration tool opens.

7 In the main window of the GMDR Administration tool, select Show Components.

The Show Components dialog opens.

8 Find the Passport 4400 in the components panel of the Show Components dialog and click on the name of the Passport 4400.

The name of the Passport 4400 becomes highlighted to indicate that it is selected.

9 Click Delete.

The Passport 4400 and its components disappear from the Show Components dialog.

10 In the MDM Toolsets window, select System -> Administration -> Server Administration.

The Server Administration window opens.

11 Use Server Manager Administration to ensure that the network model editor server (EDSERVER) is created and running.

If the EDSERVER is not created and running, create it and start it using the following start-up command.

```
/opt/MagellanNMS/bin/edserver &
```

12 In the MDM Toolsets window, select Fault -> Network Viewer.

The Network Viewer window opens.

13 From the Network Model Edit menu, select:

`Enable Network Model Editing`

14 Click on the icon of the Passport 4400 to delete.

15 Using the right mouse button select:

`Edit-> Delete`

The Delete Components window opens.

16 Click on the Delete button.

The Passport 4400 icon disappears from the Network Viewer window.

17 From the Network Model Edit menu, select:

`Leave Network Model Editing`

The Leave Editing Network Model window opens.

18 Click on the Exit and Save button.

19 From the File menu, select:

`Exit`

If you are asked to confirm the exit, click on the Exit and Save button.

The Network Viewer window closes. If you have the graphical network browser open, the icon for the node you just have deleted disappears from the browser.

Removing a DPN-100 or Passport 4120

Use this procedure to remove a DPN-100 switch or a Passport 4120 from the graphical network browser (GNB). To remove the node perform the following tasks:

- remove information about the OA member for the node from file /opt/MagellanNMS/cfg/HGDS.cfg
- restart the DPN Management Data Router (DMDR) server
- restart the Host Group Directory (HGD)S server
- remove information about the node from the GMDR database
- delete information about the node from the network model

For more information about the servers in this procedure, including how to stop and start them, see 241-6001-303 *Preside MDM Administrator Guide*.

1 Log in as the root user.

2 Start the C-shell.

```
csh
```

3 Source the MDM environment variables.

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

4 Start MDM.

```
/opt/MagellanNMS/bin/nmstool &
```

A copyright dialog opens.

5 In the copyright dialog, click on the OK button.

The copyright dialog closes, and after a delay, the MDM Toolsets window opens.

6 In the MDM Toolsets window, select System -> Administration -> Server Administration.

The Server Administration window opens.

7 Stop the DMDR server for the operations agent (OA) group that contains the DPN-100 or Passport 4120 that you are going to remove.

8 Restart the DMDR server.

9 Stop the HGDS server.

10 Using a text editor such as vi, open file /opt/MagellanNMS/cfg/HGDS.cfg.

11 Remove information about the OA member for the DPN-100 or Passport 4120 from file HGDS.cfg.

12 Restart the HGDS server.

13 In the MDM Toolsets window, select System -> Administration -> GMDR Administration.

The main window of the GMDR Administration tool opens.

14 In the main window of the GMDR Administration tool, select the Show Components button.

The Show Components dialog opens.

15 Find the name of the node in the components panel of the Show Components dialog and click on the name of the node.

The name of the node becomes highlighted to indicate that it is selected.

16 Click on the Delete button.

The node and its components disappear from the Show Components dialog.

17 In the MDM Toolsets window, select System -> Administration -> Server Administration.

The Server Administration window opens.

18 Use the server manager administration tool to ensure that the network model editor server (EDSERVER) is created and running.

If the EDSERVER not created and running, create it and start it using the following start-up command.

`/opt/MagellanNMS/bin/edserver &`

19 In the MDM Toolsets window, select Fault -> Network Viewer.

The Network Viewer window opens.

20 From the Network Model Edit menu, select:

`Enable Network Model Editing`

21 Click on the icon of the node you want to delete.

22 Using the right mouse button select:

`Edit-> Delete`

The Delete Components window opens.

23 Click on the Delete button.

The node icon disappears from the Network Viewer window.

24 From the Network Model Edit menu, select:

`Leave Network Model Editing`

The Leave Editing Network Model window opens.

25 Click on the Exit and Save button.

26 From the File menu, select:

`Exit`

If you are asked to confirm the exit, click on the Exit and Save button.

The Network Viewer window closes. If you have the graphical network browser open, the icon for the node you just have deleted disappears from the browser.

Removing iBWA 5100 devices

Use this procedure to remove Radio base station equipment or Radio customer premises equipment from the graphical network browser. To remove the iBWA 5100 device, perform the following tasks:

- delete information about the device from file /opt/MagellanNMS/cfg/gendcd_ibwa5k.sed
- remove information about the node from the general management data reporter (GMDR) database
- delete information about the node from the network model

For more information about the servers in this procedure, including how to stop and start them, see 241-6001-303 *Preside MDM Administrator Guide* and 241-6001-113 *Preside MDM iBWA 5100 Integration Guide*.

1 Log in as the root user.

2 Stop the data collection daemon.

3 Using a text editor, such as vi, open file /opt/MagellanNMS/cfg/gendcd_ibwa5k.sed.

4 Delete the information for the iBWA 5100 devices to remove.

5 Save the file and close it.

6 Use the MDM Administration Tool to restart the data collection daemon.

7 In the MDM Toolsets window, select System -> Administration -> GMDR Administration.

The main window of the GMDR Administration tool opens.

8 In the main window of the GMDR Administration tool, select the Show Components button.

The Components dialog opens.

9 Find the name of the node in the components panel of the Show Components dialog and click on the name of the node to select it.

The name of the node becomes highlighted to indicate that it is selected.

10 Click on the Delete button.

The node and its components disappear from the Show Components dialog.

11 In the MDM Toolsets window, select System -> Administration -> Server Administration.

The Server Administration window opens.

12 Use the server manager administration tool to ensure that the network model editor server (EDSERVER) is created and running.

If the EDSERVER is not created and running, create it and start it using the following start-up command.

```
/opt/MagellanNMS/bin/edserver &
```

13 In the MDM Toolsets window, select Fault -> Network Viewer.

The Network Viewer window opens.

14 From the Network Model Edit menu, select:

`Enable Network Model Editing`

15 Click on the icon of the node you want to remove to select it.

16 Using the right mouse button select:

`Edit-> Delete`

The Delete Components window opens.

17 Click on the Delete button.

The node icon disappears from the Network Viewer window.

18 From the Network Model Edit menu, select:

`Leave Network Model Editing`

The Leave Editing Network Model window opens.

19 Click on the Exit and Save button.

20 From the File menu, select:

`Exit`

If you are asked to confirm the exit, click on the Exit and Save button.

The Network Viewer window closes. If you have the graphical network browser open, the icon for the node you just have deleted disappears from the browser.

Chapter 9
Troubleshooting

This section contains procedures for troubleshooting common problems associated with the Preside Multiservice Data Manager (MDM) Device Adapter software.

Refer to the following symptoms

Messages encountered while loading the Preside MDM Device Adapter software

The Preside Multiservice Data Manager (MDM) Device Adapter software installation scripts perform pre-installation checks, installs the software, and performs a set of post-installation checks. Some messages halt the installation process while others allow the installation process to continue.

```
"Error: You are attempting to perform an upgrade
install of Magellan MOA load PMO030Xxx over previous
load PMO010Yyy. This upgrade is not supported. Please
de-install PMO010Yyy, execute rm -rf /opt/MagellanMOA/
3rdParty and then install PMO030Xxx."
```

This message indicates that you are attempting to install a PMO030 load in place of a PMO010 load. The current installation script does not support this upgrade. Instead

1. use the Sun Admintool to delete the PMO010 load
2. change directories, type

   `cd /opt/MagellanMOA/3rdParty`
3. remove the contents of the directory, type

   `\rm -f *`
4. install the new PMO030 load with the Sun Admintool

Messages from the pre-installation checks that still allow the installation to continue are as follows:

```
"Warning: Previous package (PMO###Xxx) has a different
version of orbix (#.#) than this package (PMO###Xxy,
orbix version #.#). Because the orbix version has
changed, you will have to reconfigure the new orbix
version by editing /opt/MagellanMOA/3rdparty/
Orbix_3.0.1MT/config/trader.cfg. You can see your
previous settings in file /opt/MagellanMOA/loads/
PMO###Xxx/Orbix_#.#/config/trader.cfg."
```

This message indicates that the existing trader.cfg file cannot be reused for the new installation or upgrade.

```
"Warning: The previous release did not appear to have
an orbix version with it. Continuing..."
```

This message indicates that the upgrade install cannot reuse the Orbix configuration from the previous installation because the orbix directory does not exist.

```
"Warning: the previous release did not appear to have
a 3rdparty directory"
```

This message indicates that the upgrade install cannot reuse the Orbix configuration from the previous installation because the 3rdparty directory does not exist.

Messages from the post-installation checks that halt the installation are as follows:

```
"Error: unable to create the directory <dir>."
```

This message indicates that the install cannot create the required directory. Make sure that you are logged in using userID root and that the directory <dir> is owned by root.

```
"Error: unable to change permission for the directory
<dir>."
```

This message indicates that the install cannot set the permissions on a required directory.

Message encountered while removing the Preside MDM Device Adapter software

The removal scripts for the Preside Multiservice Data Manager (MDM) Device Adapter software perform a set of pre-removal checks, remove the software, then perform a set of post-removal checks. Some messages halt the removal of the software while others allow the removal to continue.

Messages associated with the pre-removal checks that halt the removal of the software are as follows:

```
"Error: Package PMO###Xxx does not appear to be
installed."
```

This message indicates that the package was (possibly) removed by deleting directories manually instead of with Sun's Admintool. Use Sun's Admintool to remove the package.

Messages associated with the pre-removal checks that allow the software removal to continue are as follows:

```
"Note: directory <dir> is not empty, not removing."
```

This message occurs when files created by a user or edited by a user exist in the installation directory. To preserve user information when you are performing an upgrade, the product removal does not delete configuration files that a user edits. The removal scripts attempt to remove every directory created by the installation and issue this message for any directory that the scripts cannot remove.

```
Error: no moaLaunch entries matching orbixd found in
/etc/inittab.
```

This message indicates that there was no entry for the Orbix daemon in the /etc/inittab file.

Messages associated with the post-removal checks that allow the software removal to continue are as follows:

```
"Note: directory <dir> is not empty, not removing.
```

This message occurs when files created or edited by a user exist in this installation directory. To preserve user information when you are performing an upgrade, the product removal does not delete configuration files that a user edits. The de-install attempts to remove every directory the script created, and issues this message for any directory that it cannot remove.

Inability to obtain alarms from Passport 6420, 6440, 6480, or 8780

Use the following check list to determine why alarms cannot be obtained from one, or more, Passport 6420, 6440, 6480, or 8780 in the network.

- A common user ID and password with read permission is not set on all Passport switches in the Passport group.
- The IP connection between the workstation that runs the Preside Multiservice Data Manager (MDM) and the Passport switches is down, or is not configured properly.
- The Passport group definitions not entered into file HGDS.cfg.
- The following servers are not configured or not running:
  - context server (CTXSVR)

  - multi-nodal naming server (MNSD)
  - host group directory server (HGDS)
  - FMIP management data router (FDTM)
  - FMDR (one for each Passport group)
  - general management data reporter (GMDR)
  - network model data coordinator (DNMNMC)
  - surveillance network model updater (SURNUP)
  - network model server (NMSERVER)
  - network data access mediator (NDAM)
- The location of the NDAM server is not specified in file ndam.hosts.
- The GMDR server is not configured with the GMDR administration tool to obtain surveillance information from the FMDR server. There is one FMDR server for each Passport group.
- The following applications are not started, or have been started with incorrect domain names or identifiers that are not unique:
  - network management system Adapter (nmsAdapter)
  - fault management managed object agent (fmMoa)
  - resource management managed object agent (rmMoa)

Inability to obtain alarms from DPN-100 or Passport 4120

Use the following checklist to determine why alarms cannot be obtained from one, or more, DPN-100s or Passport 4120s in the network.

- The NCS Capability ID is not set up correctly in the network control system (NCS) for DPN-100 or Passport 4120.
- The X.25 connection to the DPN-100 or the Passport 4120 is down, or is not configured correctly.
- The OA group definitions are not entered into file HGDS.cfg.
- The following servers are not configured or are not running:
  - context server (CTXSVR)

  - multi-nodal naming server
  - network control system manager (NCSMGR)
  - DPN management data router (DMDR) (one for each OA group)
  - host group directory server (HGDS)
  - general management data reporter (GMDR)
  - network model data coordinator (DNMNMC)
  - surveillance network model updater (SURNUP)
  - network model server (NMSERVER)
  - network data access mediator (NDAM)
- The location of NDAM server is not specified in file ndam.hosts.
- The GMDR server has not been configured with the GMDR administration tool to obtain surveillance information from the DMDR server. There is one DMDR server for each OA group.
- The following applications are not started, or are started with incorrect domain names or identifiers that are not unique:
  - network management system Adapter (nmsAdapter)
  - fault management managed object agent (fmMoa)
  - resource management managed object agent (rmMoa)

Inability to obtain alarms from Passport 4400

Use the following checklist to determine why alarms cannot be obtained from one, or more, Passport 4400 in the network.

- The system kernel values for running HP OpenView are not set correctly.
- Internet protocol (IP) connectivity is lost between the Passport 4400 and the workstation that is running HP OpenView.
- IP connectivity is lost between the workstation that is running HP OpenView and the workstation that is running the Preside Multiservice Data Manager (MDM). This only applies when separate workstations are running MDM and HP OpenView.

- The MDM-Passport 4400 application is not fully installed on the workstation running HP OpenView.
- Trap subscription is not set up on the Passport 4400 to provide traps to the workstation running HP OpenView.
- The OpenView management data router (OVMDR) server is not started and running on the workstation running HP OpenView.
- One or more of the following MDM servers has exited or is not configured:
  - general management data reporter (GMDR)
  - network model data coordinator (DMNNMC)
  - surveillance network model updater (SURNUP)
  - network model server (NMSERVER)
  - network data access mediator (NDAM)
- The GMDR server is not set up to obtain surveillance information from the OVMDR server.
- File ndam.hosts does not contain the location of the GMDR server.
- The following applications are not started, or have been started with incorrect domain names or identifiers that are not unique:
  - network management system Adapter (nmsAdapter)
  - fault management managed object agent (fmMoa)
  - resource management managed object agent (rmMoa)
- IP connectivity has been lost between the workstation that runs the MDM Device Adapter and the workstation that runs the integrated network management (INM) applications.

Inability to obtain alarms from iBWA 5100 devices

Use the following checklist to determine why alarms cannot be obtained from iBWA 5100 devices in the network.

- IP connectivity has been lost between the workstation running the DCD and the iBWA 5100 device.

- File /opt/MagellanNMS/cfg/gendcd_ibwa5k.sed has not been configured or does not contain information about the iBWA 5100 device.
- The following servers are not running or are not correctly configured on the Preside Multiservice Data Manager (MDM) workstation:
  - generic data collection daemon (DCD)
  - SNMP management data reporter (SMDR)
  - trap server daemon (TSVR)
  - general management data reporter (GMDR)
  - network model data coordinator DMNNMC
  - surveillance network model updater (SURNUP)
  - network model server (NMSERVER)
  - network data access mediator (NDAM)
- The GMDR server has not been set up to obtain surveillance information from the SMDR server.
- File ndam.hosts does not contain the location of the GMDR server.
- The following applications are not started, or have been started with incorrect domain names or identifiers that are not unique:
  - network management system Adapter (nmsAdapter)
  - fault management managed object agent (fmMoa)
  - resource management managed object agent (rmMoa)

Application stops unexpectedly (core dumps)

If a Preside Multiservice Data Manager (MDM) Device Adapter application stops unexpectedly (performs a core dump), the OrbixTrader software does not remove information about the application's offer to provide service from the OrbixTrader's internal database. To allow other applications to trade for the failed application once it has been restarted, remove the existing offer from the OrbixTrader's database. Use the OrbixTrader documentation to remove the offer.

If you stop the application as described in “Stopping a Preside MDM Device Adapter application” (page 93), the OrbixTrader software removes information about the application and its service name and you do not need to remove the offer of service from the OrbixTrader’s database.

Index

Preside Multiservice Data Manager

Device Adapter Installation and Administration

User Guide

R14.3

Publication: 241-6001-121
Document status: Standard
Document version: 14.3RSUP
Document date: December 2003
Printed in Canada

NORTEL NETWORKS