Preside Multiservice Data Manager

Device Adapter Installation and Administration

241-6001-121

Preside Multiservice Data Manager

Device Adapter Installation and Administration

Publication: 241-6001-121
Document status: Standard
Document version: 15.1RSUP
Document date: August 2004

Printed in Canada

Publication history

August 2004

15.1RSUP Standard

Commercial availability, except for MPE support, which will be available in a later release.

Contents

About this document

This document contains instructions to plan, install, and administer the Preside Multiservice Data Manager (MDM) Device Adapter software. The Device Adapter 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” (page 11)
- “What you need to know” (page 11)
- “How this document is organized” (page 12)
- “What’s new in this document” (page 12)
- “Text conventions” (page 12)
- “Related documents” (page 13)

Who should read this document and why

This document is intended for experienced network operators who require fault information for Preside Multiservice Data Manager Applications Platforms. Personnel responsible for installing and maintaining 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 Preside Multiservice Data Manager

How this document is organized

This document contains the following sections:

- “Device Adapter” (page 15)
- “Engineering” (page 29)
- “Planning domains and subdomains with redundancy” (page 33)
- “Preparing Preside Multiservice Data Manager” (page 43)
- “Installing Device Adapter software” (page 47)
- “Starting Device Adapter applications” (page 63)
- “Administering Device Adapters” (page 73)

What’s new in this document

This document has been changed to reflect

- updated procedures for configuring the CORBA gateway and MDM hosts as trusted workstations; see “Configuring trusted workstations” (page 49)
- a change to the section “Loading Device Adapter software from CD-ROM” (page 56)
- support for SNMP devices
- DPN and Passport-specific information removal

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

  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 Installation*

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

Chapter 1
Device Adapter

This section contains information about the following topics:

Understanding the 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 MDM software. You can use the Device Adapter software to obtain fault information from the following devices:

- Optical Packet Edge cards
- Ethernet Services Unit 1200/1400/1450
- Ethernet Services Unit 1800
- Ethernet Services Switch 8600/8650
- Business Policy Switch
- Baystack 420

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 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 Device Adapter software. Nortel Networks provides MDM software on a CD-ROM.

The installed and configured 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 Device Adapter” (page 19) shows MDM components associated with 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. Preside Multiservice Data Manager (MDM) software uses SNMP Management Data Router (SMDR) and a SNMP data collection daemon (DCD).

The SNMP Management Data Router (SMDR) merges SNMP surveillance data obtained from DCDs and makes it available to the General Management Data Router (GMDR). The SMDR performs the following functions:

- collects surveillance data from generic and device-specific DCDs
- supports REGISTER, GET, CREATE, and ACTION API requests from GMDR
- forwards alarms to GMDR
- issues proxy alarms for the DCD and the device; these alarms are issued when a polling state conflicts with the component active alarm list, or when a device becomes unreachable or reachable again

The DCD performs the following functions:

- polls the devices using the SNMP protocol to
  - verify subcomponent states
  - verify device reachability
- notifies the SNMP Management Data Router (SMDR) when there is a new component, when a component is deleted, and when there is a change in state of a component
- converts traps received from the trap server (TSVR) to alarms and forwards the alarms to SMDR
- maintains a device seed file containing a list of devices, with their IP addresses and community strings, that is used to rediscover these devices upon restart

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

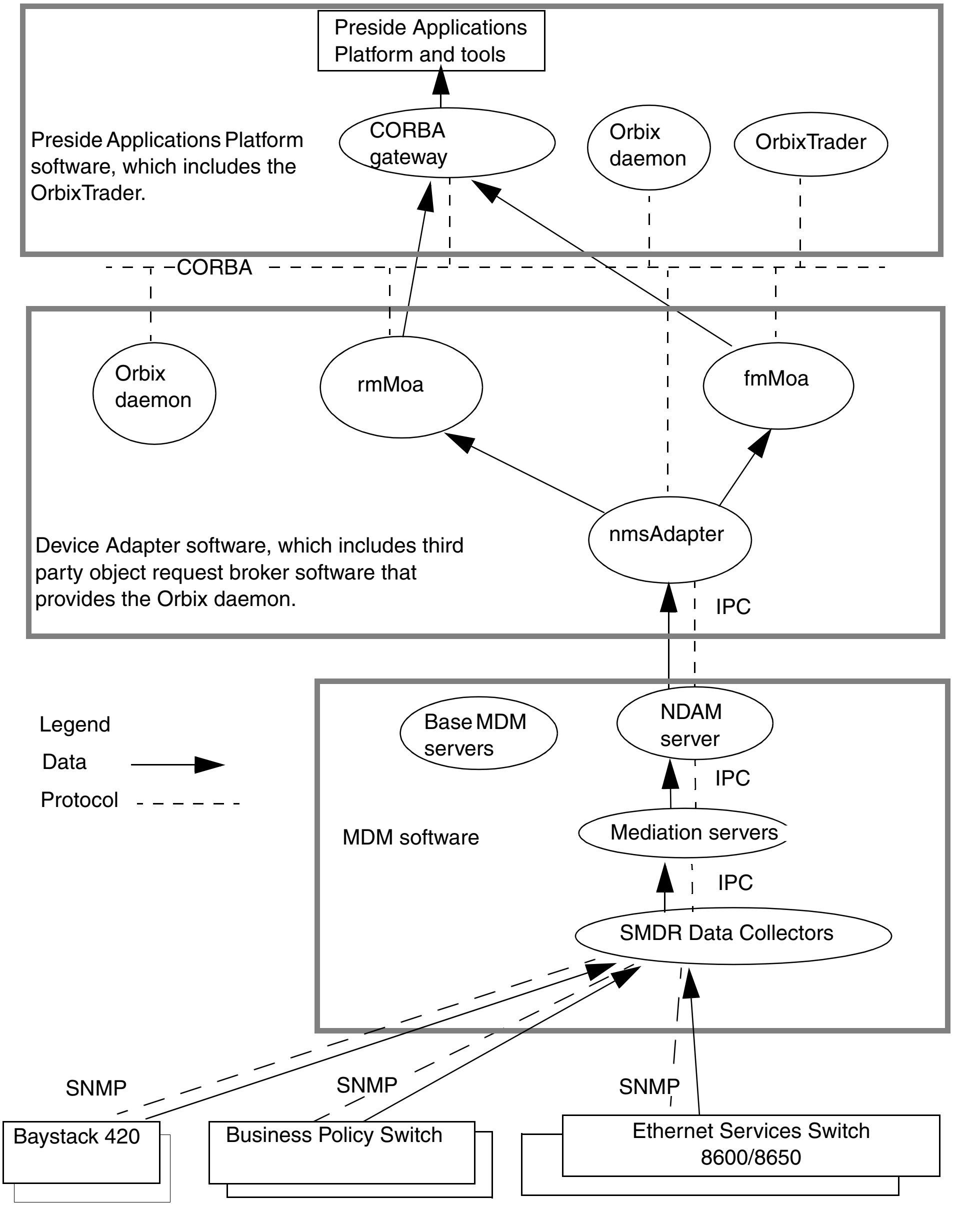
- general management data router (GMDR)
- network model data coordinator (DNMNMC)
- surveillance network model updater (SURNUP)
- network model server (NMSERVER)

Base MDM servers

The base Preside Multiservice Data Manager (MDM) servers start automatically when a user starts a 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 Device Adapter


Preside Applications Platform and tools
CORBA gateway
Orbix daemon
OrbixTrader
Preside Applications Platform software, which includes the OrbixTrader.
CORBA
Orbix daemon
rmMoa
fmMoa
nmsAdapter
Device Adapter software, which includes third party object request broker software that provides the Orbix daemon.
IPC
Legend
Data
Protocol
Base MDM servers
NDAM server
IPC
Mediation servers
MDM software
IPC
SMDR Data Collectors
SNMP
SNMP
SNMP
Baystack 420
Business Policy Switch
Ethernet Services Switch 8600/8650

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.

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 Device Adapter software is to convert fault information delivered in IPC format into CORBA format for the MDM software.

The CORBA applications that make up the Device Adapter are

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

“Items associated with the Device Adapter” (page 19) shows the applications that make up the 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 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 Preside Multiservice Data Manager (MDM). nmsAdapter communicates with the other 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 Device Adapter software.

Device Adapter Network configurations

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

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

In medium and large networks, the Device Adapter software and 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 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 Device Adapter software. You only need to install the MDM software; you do not need to start and configure any of the 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 Server Adapter software

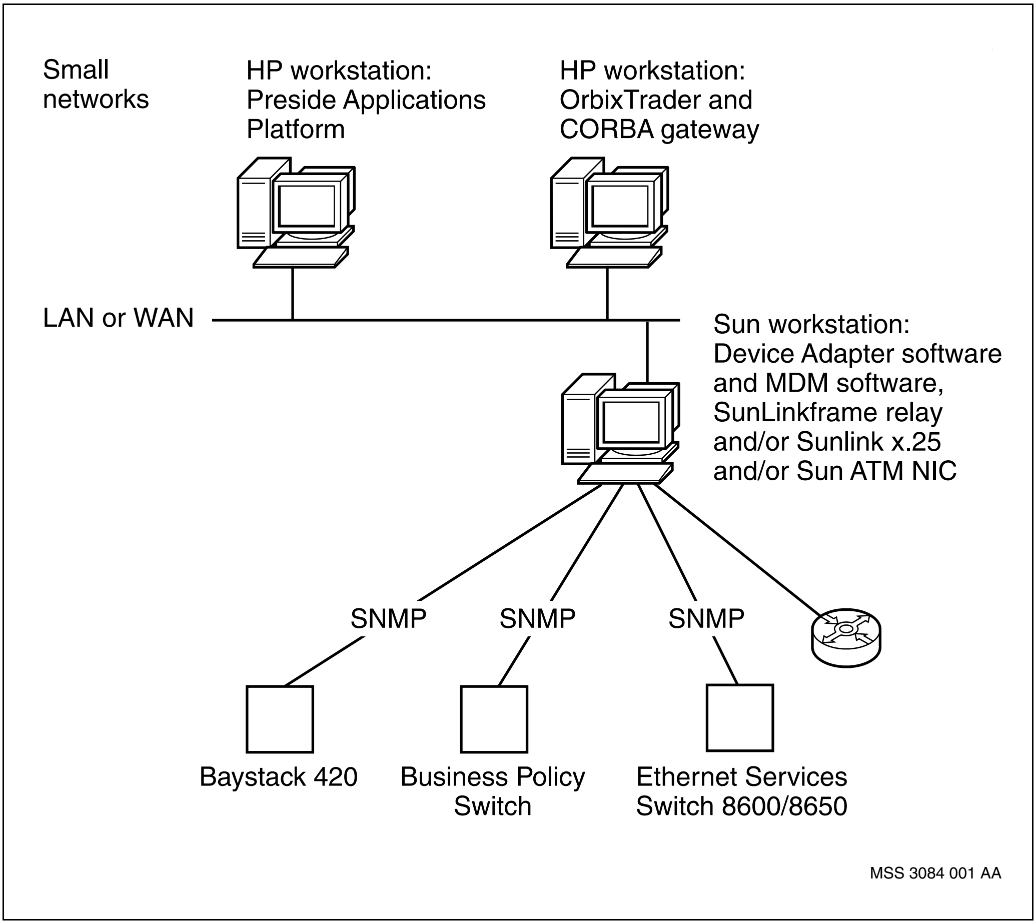
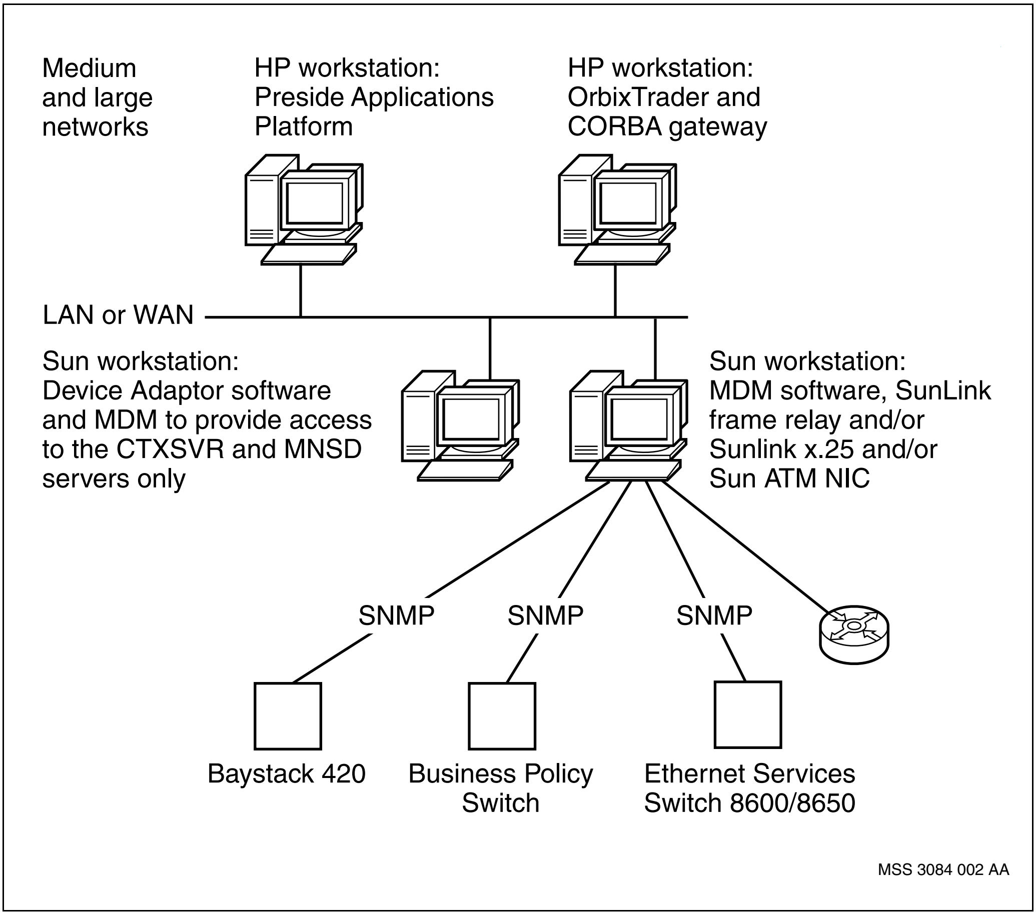

Small networks
HP workstation: Preside Applications Platform
HP workstation: OrbixTrader and CORBA gateway
LAN or WAN
Sun workstation: Device Adapter software and MDM software, SunLinkframe relay and/or Sunlink x.25 and/or Sun ATM NIC
SNMP
SNMP
SNMP
Baystack 420
Business Policy Switch
Ethernet Services Switch 8600/8650
MSS 3084 001 AA

Figure 3
Medium network configuration for running Server Adapter software


Medium and large networks
HP workstation: Preside Applications Platform
HP workstation: OrbixTrader and CORBA gateway
LAN or WAN
Sun workstation: Device Adaptor software and MDM to provide access to the CTXSVR and MNSD servers only
Sun workstation: MDM software, SunLink frame relay and/or Sunlink x.25 and/or Sun ATM NIC
SNMP
SNMP
SNMP
Baystack 420
Business Policy Switch
Ethernet Services Switch 8600/8650
MSS 3084 002 AA

The workstation that runs MDM communicates through SNMP to Ethernet Services Switch 8600/8650, Business Policy Switch and Baystack 420.

Installation overview and workflow

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 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 Device Adapter workstation's nodename to its IP address and identifies two administration userIDs
- the /etc/hosts file on the Device Adaptor workstation contains information that maps the OrbixTrader workstation's nodename to its IP address and identifies two administration user IDs
- SNMP network elements such as Ethernet Services Switch 8600 / 8650, Business Policy Switch and Baystack 420
- the MDM software is installed and configured to monitor all types of devices.
- the MDM servers listed in "Servers that start automatically when a user logs in" (page 26) and "Servers that you must start to manage different devices" (page 27) 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 "Servers that start automatically when a user logs in" (page 26) and "Servers that you must start to manage different devices" (page 27), other servers may be running on a fully configured workstation, but they are not essential for 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.

Servers that start automatically when a user logs in

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

Servers that you must start to manage different devices

Required for	Abbreviation	Full name
SNMP NEs, such as, Ethernet Services Switch 8600 / 8650, Business Policy Switch, Baystack 420	SMDR	SNMP management data router
	GMDR	general management data router
	SURNUP	surveillance network model updater
	NMSERVER	network model server
	NM Coordinator	network model coordinator
	NM EditServer	network model edit server
	NDAM	network data access mediator
	TSVR	trap server
	SNMP IP Discovery Server	SNMP IP discovery server

Installation tasks

Perform the following tasks to install and configure Device Adapter software:

1. Ensure that the workstation meets engineering requirements, see “Engineering” (page 29).
2. Plan domains and subdomains to support redundancy, see “Planning domains and subdomains with redundancy” (page 33).
3. Ensure that Preside Multiservice Data Manager (MDM) is set up to provide fault information to the Device Adapter applications, see “Preparing Preside Multiservice Data Manager” (page 43).
4. Configure MDM as a trusted workstations, see “Configuring trusted workstations” (page 49).

5 Create the necessary UNIX group and user IDs on the MDM workstation, see “Creating an AP group and user IDs on the host” (page 54).

6 Load the Device Adapter software from the Preside Multiservice Data Manager CD-ROM and configure the object request broker (ORB), see “Installing Device Adapter software” (page 47).

7 Set up the ndam.hosts configuration file, then start the network management system Adapter (nmsAdapter), the fmMoa, and the rmMoa, see “Starting Device Adapter applications” (page 63).

Documentation roadmap

For instructions to install and configure Preside Multiservice Data Manager (MDM) software to provide fault information from network elements, see

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

For instructions to install and configure the CORBA gateway, see

- Optical Applications Platform Installation and Administration Guide, 450-3101-201

Chapter 2 Engineering

This section contains information about the following topics:

- "How the software is supplied" (page 29)
- "Licensing" (page 30)
- "Software compatibility" (page 30)
- "Minimum hardware requirements" (page 31)
- "Connectivity requirements" (page 31)

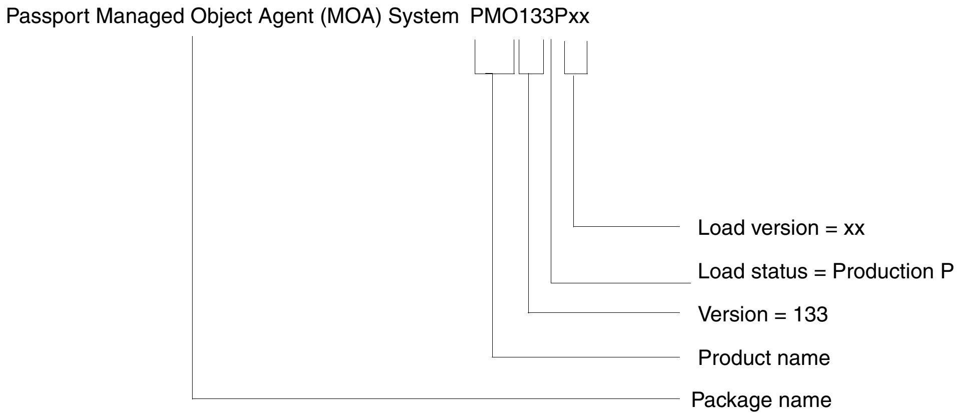
How the software is supplied

Device Adapter software is supplied on the Preside Multiservice Data Manager 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 - PMO151Pxx

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

Figure 4
Example of package naming


Passport Managed Object Agent (MOA) System PMO133Pxx
Load version = xx
Load status = Production P
Version = 133
Product name
Package name

Licensing

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

Device Adapter release 13.3 software

- runs on the Solaris 8 (and up) operating system
- is compatible with Preside Multiservice Data Manager software release 15.1 and above
- is compatible with Optical Applications Platform software release 9.1 and above
- requires access to an OrbixTrader, version 2000 1.2.1

Minimum hardware requirements

For information on the minimum requirements to run Device Adapter software on a workstation refer to the Preside MDM for Optical Ethernet Engineering and Planning Guide (450-3101-671).

Connectivity requirements

For information on the requirements for Internet Protocol connectivity through a local area network (LAN) or a wide area network (WAN), refer to the Preside MDM for Optical Ethernet Engineering and Planning Guide (450-3101-671).

In small networks, the MDM software runs on the same workstation as the Device Adapter software. In medium and large networks the MDM software and the Device Adapter software must run on separate workstations. When the MDM and 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 40).

Domains and subdomains

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

Domain

For the Device Adapter, a domain is a set of SNMP devices 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 35). Guidelines for setting up domains are as follows:

- A domain must contain one instance of each of the following 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 34).

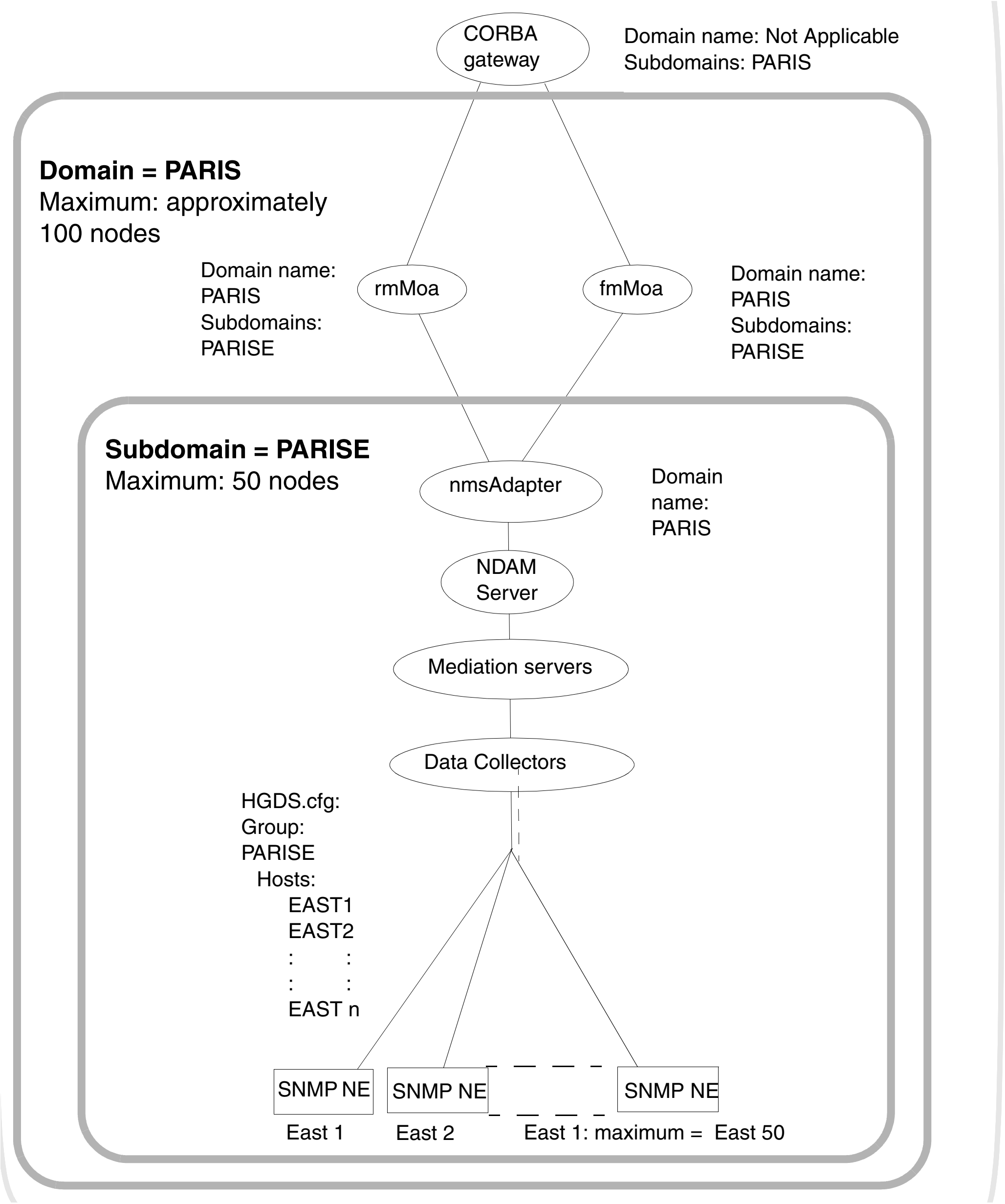
Subdomain

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

- 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 35).

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 Device Adapter, the recommended way is to create redundant instances of

- 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 Preside Multiservice Data Manager software)

Redundancy and the nmsAdapter, the fmMoa, and the rmMoa

Redundant 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 software) that provides the nmsAdapter with node 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 Device Adapter applications and NDAM servers to ensure redundancy, we recommend that you:

- create redundant instances of each Device Adapter application on separate workstations in your network
- configure the Preside Multiservice Data Manager 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 39).

How redundancy operates with the recommended scheme

There are several types of failure to consider:

- failure of a single 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 a Device Adapter application
- failure of an NDAM server, or the connection between an nmsAdapter and the NDAM server

Failure of an Device Adapter application

“Example of a redundant configuration using two workstations” (page 39) 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.

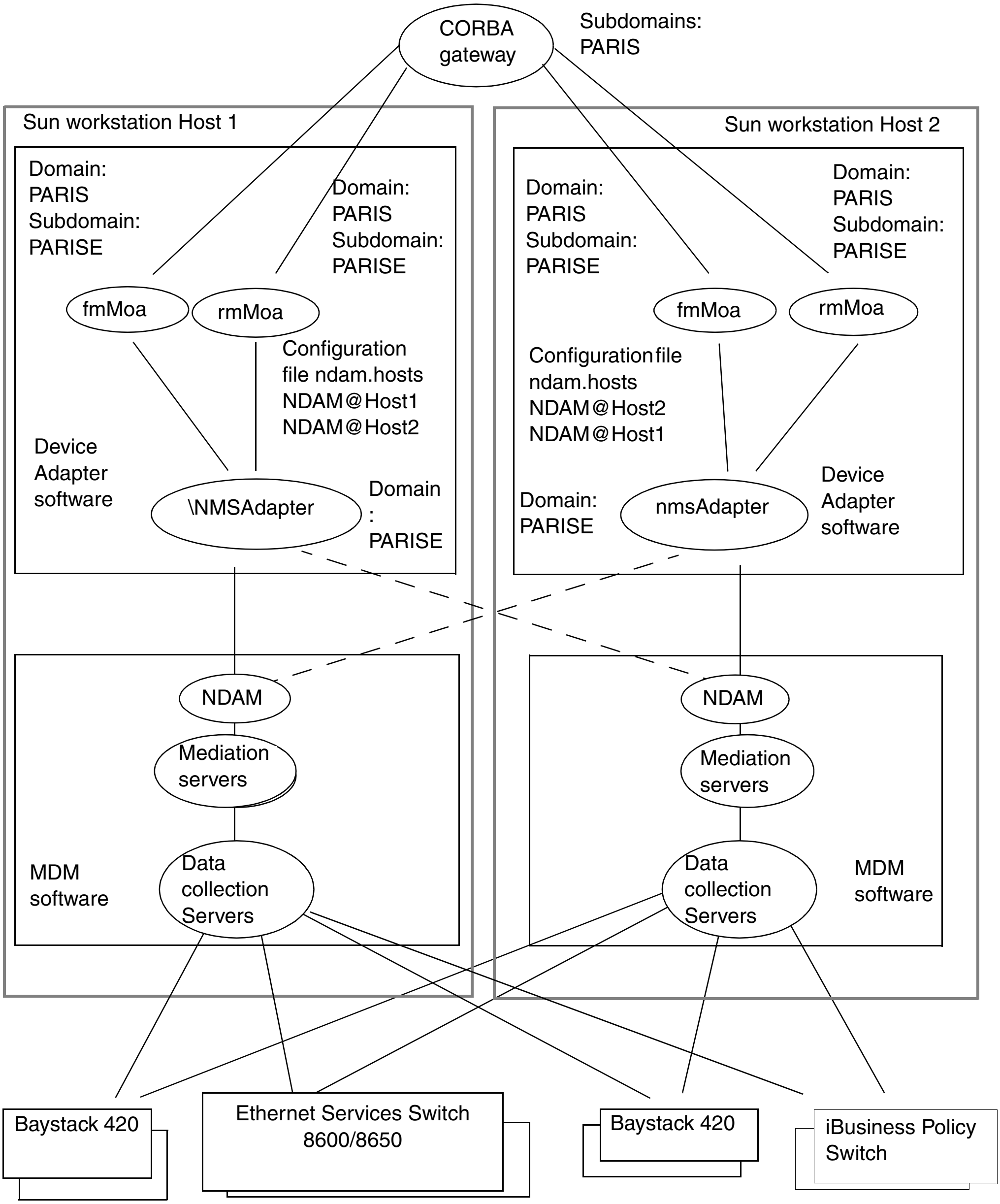
Failure of a workstation that runs Device Adapter applications

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 41). You need this information to start the 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 Device Adapter, see:

- "Domains and subdomains" (page 33)
- "Resiliency and redundancy" (page 36)

1 Write the host name and IP address of the workstation on which you are going to install the Device Adapter software on the planning worksheet "Planning worksheet" (page 41).

2 Determine if you wish to manage your SNMP devices 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 41).

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 Preside Multiservice Data Manager (MDM) software and the 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 Device Adapter applications. See “Preparing Preside Multiservice Data Manager” (page 43).

Planning worksheet

Item	**Information**
Workstation running 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 Device Adapter applications	
	Host name:
	IP Address:

Chapter 4
Preparing Preside Multiservice Data Manager

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

- “Prerequisites” (page 43)
- “Procedures for preparing MDM” (page 43)

Prerequisites

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.

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 software is configured to provide fault information to the Device Adapter applications using the procedures in this section.

- “Checking the software licenses” (page 44)
- “Verifying fault collection from SNMP devices” (page 45)
- “Starting the NDAM server” (page 46)

Checking the 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.

Procedure steps

1 Log in as the root user on the MDM workstation.

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 more information, refer to 241-6001-102 *Preside MDM Planning Guide*.

If MDM Fault Servers and Tools and SNMP Surveillance Adapter do not appear in this list, you need a new license. Contact your Nortel Networks Corporation representative.

3 Perform the following procedure for the devices that you have in your network:

- "Verifying fault collection from SNMP devices" (page 45)

Verifying fault collection from SNMP devices

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

Procedure steps

1 Use the MDM Server Administration tool to verify that the following servers are running and configured to start automatically following a reboot. For more information about the MDM Server Administration tool, see 241-6001-303 *Preside MDM Administrator Guide*.

Server name	**Default directory**
NM Coordinator	/opt/MagellanNMS/bin/dnmnmc
SurNUp	/opt/MagellanNMS/bin/surnup -D all
NMServer	/opt/MagellanNMS/bin/nmserver
NM EditServer	/opt/MagellanNMS/bin/edserver
GMDR	/opt/MagellanNMS/bin/gmdr
NDAM	/opt/MagellanNMS/bin/ndam
TSVR	/opt/MagellanNMS/bin/tsvr
SMDR	/opt/MagellanNMS/bin/smdr
SNMP IP Discovery Server	/opt/MagellanNMS/bin/ipdsvr

2 Using the Server Administration tool, ensure that the GMDR server is set up to obtain serveillance information from a SMDR server for each group of SNMP devices you want to manage. .

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

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.

Procedure steps

1 Use the Server Administration tool to configure a new NDAM server to restart automatically when the Preside Multiservice Data Manager (MDM) workstation reboots, and to start the NDAM server. For instructions to use the 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 MDM software from the CD-ROM. See “Installing Device Adapter software” (page 47).

Chapter 5
Installing Device Adapter software

Use the following procedures to install and configure software associated with the Device Adapter:

- "Installing and configuring the Preside Applications Platform software" (page 48)
- "Configuring trusted workstations" (page 49)
- "Configuring the CORBA gateway host as a trusted workstation" (page 49)

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

- "Creating an AP group and user IDs on the host" (page 54)
- "Loading Device Adapter software from CD-ROM" (page 56)

Installing and configuring the Preside Applications Platform software

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

Procedures steps

1 Use the procedures in Preside Applications Platform, 9.1 Installation and Administration Guide, 450-3101-201 to install and configure the software. Ensure that you select items 2, 7, and 8 from 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 49).

Configuring trusted workstations

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

- “Configuring the CORBA gateway host as a trusted workstation” (page 49)
- “Configuring the MDM host as a trusted workstation” (page 51)

> ***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 user ID 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.

Configuring the CORBA gateway host as a trusted workstation

This 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.

> ***Note:*** This mapping is also required for autologin.

Procedures steps

1 Login to the Preside Multiservice Data Manager (MDM) workstation as the root user.

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 host name.

```
<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 entry to identify the hostname of the CORBA gateway workstation and the associated GNB user IDs.

```
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

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.

This 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.

> ***Note:*** This mapping is also required for autologin.

Procedure steps

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 Preside Multiservice Data Manager (MDM) server to its host name.

```
<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 user IDs.

```
<MDM_server_hostname> admin
<MDM_server_hostname> netmgr
```

7 Save the file /etc/hosts.equiv and exit from it.

8 Perform “Enabling remote launch capabilities” (page 52).

Enabling remote launch capabilities

Use this procedure to allow network management platform users to launch the Data Applications menu from the Graphical Network Browser. For users to log in to the network elements from a remote workstation, and for network element controllers to work, you must:

- establish host equivalency between the network management platform workstations and the Multiservice Data Manager (MDM) Device Adapter
- define user IDs on the Multiservice Data Manager and MDM Device Adapter workstation. When defining user IDs, you must state the user ID and the group to which the user ID belongs.

  The table that follows shows the default network management platform user IDs that are created on the network management platform workstation.

  To maintain consistency, create the same user IDs on the MDM workstation.
-

Group	UserId
nocadm	netmgr operator master admin
noclyout	layout
nocprov	prov
noc	stats netsurv

Prerequisites

- Turn off the automount feature on /home to permit Solaris to create home directories under /home.

Procedure steps

1 Log in to the MDM workstation using the root user ID and password.

2 Create the a group:

```
groupadd <group>
```

where:

`group` is one of the following: nocadm, noclyout, nocprov, or noc.

3 Add user IDs for the group

```
useradd -m -g <group> <userid>
```

where:

`group` is one of the following: nocadm, noclyout, nocprov, or noc.

`userid` is a valid userid for the group.

4 Open the /etc/auto_master file.

5 Edit the /home line by placing a # at the beginning of the line.

6 Apply the changes made to the `/etc/auto_master` file:

```
/usr/sbin/automount
```

Creating an AP group and user IDs on the 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 user IDs to access the GNB host.

- "Creating the GNB group" (page 54)
- "Creating the GNB users" (page 55)

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

> ***Note:*** The passwords used for the new user IDs on the Preside Multiservice Data Manager (MDM) host workstation must be the same passwords used by these user IDs on the GNB host.

Creating the GNB group

Use this procedure to first create the GNB group.

Procedure steps

1 On the MDM host workstation, as user ID 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 edited 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

Use this procedure to populate the GNB group after it has been created. For more information, see "Creating the GNB group" (page 54)

Procedure steps

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 user ID admin

9 Click the Apply button.

The Admintool: Add User window entries are erased.

10 Return to step 3 and create another user ID 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 Device Adapter software from CD-ROM

Use this procedure to load the Device Adapter from the Preside Multiservice Data Manager (MDM) CD-ROM.

Prerequisites

- 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 CD-ROMs are available.

Procedure steps

1 Login 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 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 Device Adapter- <load name> appears in the list of installed packages.

20 From the File menu, choose Exit

The Admintool: Software window closes.

Configuring the object request broker software

Use this procedure to configure the object request broker (ORB) software that is included with the 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.

Procedure steps

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 Device Adapter workstation, 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
00000000010000000000000008a0001010000000009776b706b683
0336400003a99000000303a3e0233311b776b706b683033640054
726164696e6753657276696365504f41000e54726164696e67536
57276696365000000030000000000000008000000000049545f4100
00000100000018000000000001000100000001050100010001010
900000000000000060000000600000000020";
};
```

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
Starting 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” (page 63)
- “Starting the nmsAdapter” (page 66)
- “Starting the fmMoa” (page 68)
- “Starting the rmMoa” (page 70)

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 Preside Multiservice Data Manager (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

Procedure steps

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 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 66).

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.

Procedure steps

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 63).

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>
   ```

   Note: Enabling the propagateMsgAlarms option causes message alarms to appear in the clients as SET alarms. No corresponding CLEAR alarms are generated, so these alarms will accumulate.

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 33).

Example:

```
addToInittab 10 /opt/MagellanMOA/bin/nmsAdapter
nmsAdapter_host1_PARISE -d PARISE
```

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 68).

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.

Procedures steps

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 33

-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 63).

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 70).

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.

Procedures steps

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.

where

<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 33

-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 63).

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”
```

Chapter 7 Administering Device Adapters

This section contains procedures to perform after you install and configure the Device Adapter software. Select one of the following tasks:

- "Stopping a Device Adapter application" (page 73)
- "Removing the Device Adapter software" (page 75)

Stopping a 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)

Procedure steps

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 Device Adapter software

Use this procedure to remove the Device Adapter software from the workstation.

Procedure steps

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.

Index

Preside Multiservice Data Manager

Device Adapter Installation and Administration

R15.1

Publication: 241-6001-121
Document status: Standard
Document version: 15.1RSUP
Document date: August 2004
Printed in Canada

NORTEL NETWORKS