NORTEL NETWORKS

Preside Multiservice Data Manager

Administration Database

User Guide

241-6001-400

Preside Multiservice Data Manager

Administration Database

User Guide

Publication: 241-6001-400
Document status: Standard
Document version: 14.3RSUP
Document date: December 2003

Printed in Canada

Publication history

December 2003

14.3RSUP Standard
Commercial availability

Contents

Chapter 8
MDM Database Administration tool 127

Appendix A
Reference sheet for a simple Oracle configuration 199

About this document

This document discusses the Preside Multiservice Data Manager (MDM) database capability.

The following topics are discussed in this section:

Who should read this document and why

This document is intended for personnel who manage the service provisioning and circuit management applications.

What you need to know

This document assumes that you have a knowledge of Preside MDM, an understanding of the Passport product, and that you know how to set up and use an Oracle Database Management System.

Information related to Circuit Viewer is contained in 241-6001-011 *Preside MDM Fault Management User Guide*.

The Administration Database schema, and related descriptions are found in 241-6001-405 *Preside MDM Administration Database Schema*.

How this document is organized

This document contains the following sections:

- "Preside MDM database overview" (page 21) provides an overview of the Database and its architecture.
- "Setup and Configuration" (page 35) describes deployment considerations and provides setup procedures.
- "View and journal retrieval and notification" (page 69) describes the processes for retrieving journal and view files by the Backup Server.
- "Database population and synchronization" (page 79) describes how the Database is populated and synchronized with the Passport network.
- "Post-installation procedures" (page 97) describes how to add Passports for synchronizing and loading configuration data through a scheduled cron job.
- "Circuit management" (page 105) provides an overview of the circuit management application for managing virtual circuits.
- "VPN management" (page 117) provides an overview of the role of the MDM Administration Database and of the VPN Discovery process in VPN management.
- "MDM Database Administration tool" (page 127) describes the user interface for the MDM Database Administration tool.
- "Reference sheet for a simple Oracle configuration" (page 199) provides instructions for the end-to-end installation and setup of the Oracle Administration Database for use with Preside MDM 14.3.

What's new in this document

The following feature was added to this document:

- "IP VPN" (page 17)
- "Backup, Restore and Database Synchronization Enhancements" (page 17)

The following information was updated in this document:

- "Oracle configuration" (page 17)

The following chapter was removed from this document:

- Appendix B: InterBase installation and configuration

IP VPN

The following sections were updated or added as part of this feature:

- "Circuit management" (page 105)
- "VPN management" (page 117)
- "MDM Database Administration tool" (page 127)
- "MDM Database Administration procedures" (page 151)

Backup, Restore and Database Synchronization Enhancements

This document has been updated for the following enhancements to the Backup, Restore and Database Synchronization process:

- New Backup and Restore GUI for Passport devices
- Data Synchronization Administration Tool for Passport devices

For additional information, see the following sections:

- "Setup and Configuration" (page 35)
- "Database population and synchronization" (page 79)
- "Post-installation procedures" (page 97)

Oracle configuration

The following chapter was updated to reflect default tablespaces:

- "Reference sheet for a simple Oracle configuration" (page 199)

Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`

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

- **`nonproportional spaced bold type`**

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

- *italics*

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

  Words that appear in italics in text are for naming.

- `[optional_parameter]`

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

- `<general_term>`

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

- UPPERCASE,lowercase

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

- UPPERCASE,lowercase

  Passport commands are not case-sensitive and do not have to match commands and parameters exactly as shown in this document, with the exception of string options values (for example, file and directory names) and string attribute values.

- |

  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

See the following documents for related information:

- NN10600-606 *Passport - MDM Network Security: User Access Configuration*
- 241-6001-011 *Preside MDM Fault Management User Guide*
- 241-6001-405 *Preside MDM Administration Database Schema*
- 241-6001-600 *Preside MDM Service Provisioning for ATM User Guide*
- 241-6001-603 *Preside MDM Service Provisioning for Frame Relay User Guide*
- 241-6001-610 *Preside MDM Nodal Provisioning User Guide*
- 241-6001-611 *Preside MDM Nodal and Service Provisioning Reference Guide*
- 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*

Chapter 1
Preside MDM database overview

This section provides an overview of the Nortel Networks Preside Multiservice Data Manager (MDM) Administration Database. It includes the following topics:

The Nortel Networks Preside Multiservice Data Manager (MDM) Administration Database is used for storing information based on network resources (on-switch mastered data) and off-switch, customer entered data (off switch mastered data). This information is utilized by the MDM applications involved in ATM/FR/FRATM Circuit and IP-VPN (RFC 2764 and RFC2547) management.

The MDM tools assist network operators to provision and manage service-level components within a Passport Multi-Service node network. These include Circuit Viewer, VPN Monitor and Service Provisioning tools for ATM/FR/FRATM and IP VPN.

Circuit management improves the management of virtual circuits, such as ATM and Frame Relay, and increases the visibility of services. You can identify end-to-end circuits and associate circuits with customer information. You can also view diagnostic information for components across a circuit, including state and statistical data.

IP VPN management tools allows the network operator to provision and monitor, and trouble-shoot IP VPNs from end to end in a secure and easy manner. This reduces the service provider's Operational Expenditures and provides opportunities for service differentiation. Correlation of IP VPN services with end customers is provided for RFC2547 and RFC2764 based VPNs.

The following MDM components are associated with these capabilities:

- a relational database, which stores information on aggregated components such as an end-to-end circuit made up of VCC components across multiple devices, and IP VPN components that make up a customer's service in the network. The database also contains off-switch information to help manage the aggregated components, such as customer names and contacts, and circuit identifiers, and customer-VPN associations.
- service provisioning tools which facilitate the provisioning of end-to-end connections. These tools support direct updates of the database information upon on-switch activation, and include automatic association with off-switch data such as an associated customer. You can also retrieve the complete service from the database so that you can make modifications, or delete it from the network.
- Circuit Viewer lets network operators query circuit information from the database and view diagnostic information on ATM/FR/FRATM circuits.
- The VPN Monitor tool provides monitoring of Passport IP Virtual Private Network (VPN) services. As part of the MDM management solution for IP VPNs, it allows VPN providers to easily and efficiently

deploy and manage Passport based IP VPNs for their customers. VPN Monitor supports Passport VPNs based on RFC 2764 and RFC 2547. Direct Virtual Router-Virtual Router based VPNs are also supported. The tool facilitates the deployment of IP VPNs by allowing the provider to monitor the state of the VPNs running over their Passport network and providing notification when issues arise. VPN Monitor displays the state of the underlying components that correspond to the layer 3 service. It also allows the operator to launch other MDM tools to get circuit information such as real time statistics and alarms.

- The MDM Database Administration tool allows the operator to add off-switch data such as customer names, and allows their association to circuits and VPNs. It also allows the operator to discover circuits.
- The database synchronization process populates and updates the Passport network data into the database through the view and journal log files collected from Passport devices by the MDM Backup and Restore capability. The process also allows the automatic discovery of circuits and VPN information. Journaling allows an activation to capture a history of journals for the MDM database synchronization process.
- The Data Synchronization Administration tool supports the administration of the Passport database synchronization process. Users can view synchronization activities and basic status information. This information can be used to determine if the Passport's information is up to date in the database as well as to determine where it is out of synchronization.

  Note: Journaling is supported for PCR Release 5.1 and later only.

See 241-5701-045 *Passport 7400, 15000, 20000 Management System User Interface* for information on Passport journaling.

Preside MDM Administration Database

Preside Multiservice Data Manager (MDM) supports an off-switch, central, relational database management system (RDBMS) to store circuit and IP-VPN management information for an entire Passport network. The database stores information for the Passport 6000, 7000, 15000, and 20000 families.

Note: MDM supports networks with multiple PCR versions. It does not support Enterprise 7.0.x releases for VPN capability. Enterprise 7.0.x releases can be used for Circuit Management (ATM, FR or FRATM) however, some features and functionality such as the use of correlation tag for discovery are not supported.

The Administration Database contains three types of information:

- network resource configuration information, populated from the network
- user-entered administration information (for example, customer)
- discovered information associating network-wide information (for example, circuits)

The MDM Database Administration tool is provided to assist customers in tasks such as entering off-switch mastered data, determining associations between elements such as customers and VPNs and performing basic queries. The management of the database itself, such as performing clean-ups and backups, is done using database tools supplied by the vendor and not through MDM.

For a description of the database schema and the contents of the Administrative Database, see 241-6001-405 *Preside MDM Administration Database Schema*.

The database is supported through a customer supplied Oracle Database (Version 8i or 9i).

The loading of configuration information from the Passport to the database and maintaining the database up-to-date with the Passport network is supported through view and journal log files collected from Passport devices by the Backup and Restore capability. See “View and journal retrieval and notification” (page 69) and “Database population and synchronization” (page 79)

Architecture/System Overview

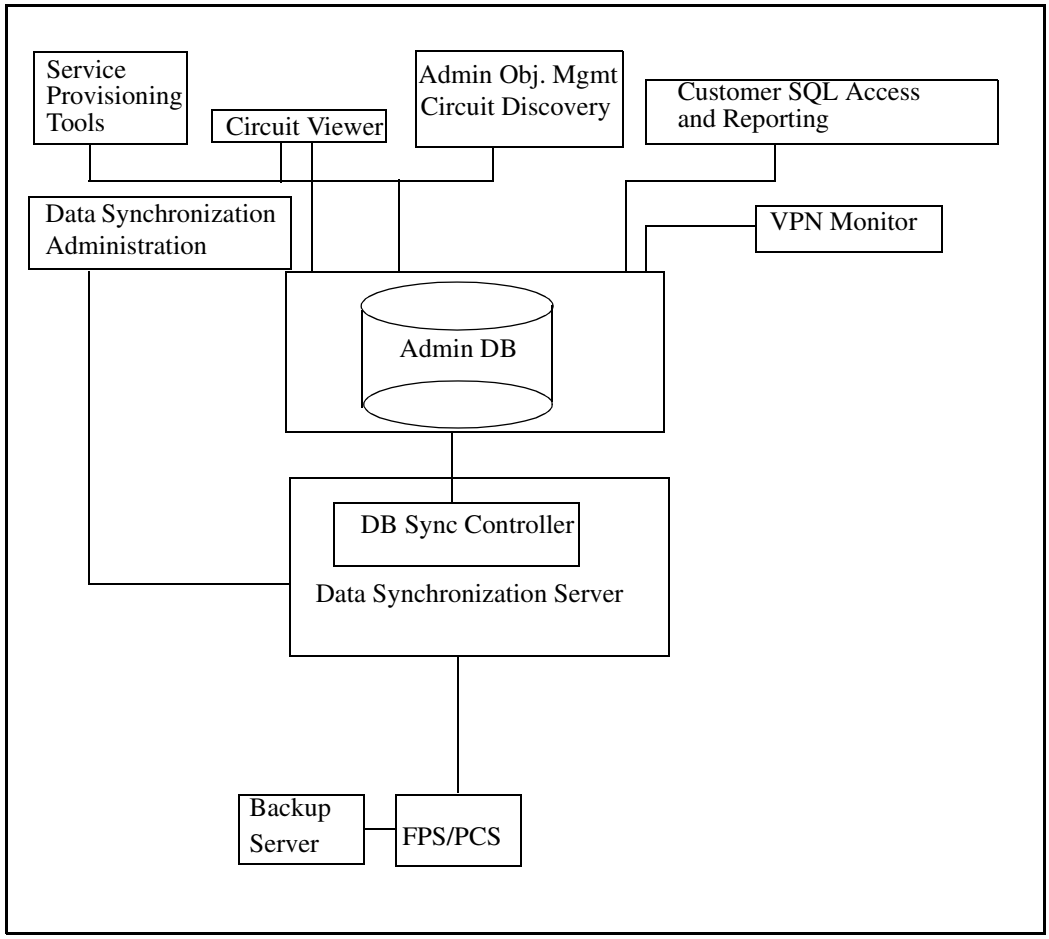
This section provides an overview of the database architecture and the end-to-end processes involved from the point when the Passport notifies the Backup Server of configuration changes, to the point when the database user

accesses the contents of the database. More detailed information about the processes associated with the database components is provided in subsequent sections.

- "Administration Database for Circuit and IP VPN Management" (page 26)
- "Database Synchronization" (page 28)
- "Data Synchronization Server" (page 29)
- "Provisioning stack (PCS/FPS servers)" (page 30)
- "Service provisioning tools" (page 30)
- "Administration object management and discovery" (page 31)

For an illustration of the database architecture, see the figure "Database architecture" (page 26).

Figure 1
Database architecture



Administration Database for Circuit and IP VPN Management

The Administration Database is optimized and structured for use by Preside Multiservice Data Manager (MDM) circuit and VPN management applications, and contains only selected necessary Passport configuration data, as well as data that comes from other sources.

Circuit Viewer

Circuit Viewer provides circuit level diagnostic capability. Circuits are groupings of Passport components into higher level aggregated service components. For example, circuits can be built out of relationships between a number of Passport components. Circuit information is consolidated in the Administration Database to allow for retrieval and circuit-level management by the circuit management applications: Circuit Viewer, Service Provisioning applications and the MDM Database Administration tool. For additional information on the Circuit Viewer, see 241-6001-011 *Preside MDM Fault Management User Guide*.

VPN Monitor

The VPN Monitor tool provides monitoring and trouble-shooting of Passport IP Virtual Private Network (VPN) services. As part of the MDM management solution for IP VPNs, it allows VPN providers to easily and efficiently deploy and manage Passport based IP VPNs for their customers. VPN Monitor supports Passport VPNs based on RFC 2764 and RFC 2547. Direct Virtual Router-Virtual Router based VPNs are also supported.

Service Provisioning

The ATM (including FRATM) and, Frame Relay (including FR IP VPN access), IP VPN service, and IP VPN provider edge provisioning tools are integrated with the Administration Database. This allows for the direct update of Passport configuration data for newly provisioned services into the Administration Database. These tools provide the capability to modify and delete circuits at the service provisioning level. IP VPN service provisioning allows for provisioning of RFC 2547 VPNs as well as RFC 2764 VPNs in autodiscovery mode.

MDM Database Administration

The MDM Database Administration tool is used to facilitate the management of the data stored in the Administration database. For example, the tool allows operators to manage customer contact information, create customer-service associations, and perform network discovery functions.

Customer SQL query for reporting of the Administration Database is also supported.

For a description of the database schema, table structures, and how to use them for reporting, see 241-6001-405 *Preside MDM Administration Database Schema*.

Database Synchronization

The retrieval of configuration information from the Passport for storage in the database, is supported through the view and journal log files collected by the Backup and Restore capability. The Preside Multiservice Data Manager (MDM) Backup Server stores the view and journal files to be available for device "restore" operations, and also for database synchronization.

The Backup application must operate in the Current View backup mode, in order to be used for database synchronization. This ensures that only the actual configuration running in the network is loaded into the database. This Backup function can be triggered in two different ways:

- on alarm by the Passport that a configuration change has been made
- scheduled, initiated through a customer defined cron job or on demand, through the Backup tool GUI.

The operator needs to determine which method of backup is required, and ensure that proper engineering of the management communication system and servers is done to support this. For more information, refer to 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

Note that the Backup tool uses the HGDS groups to define which Passports are to be backed up. You can configure the mode to be used for each group of devices in the network through the backup configuration file. For more information, refer to 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

The Backup Server notifies the Data Synchronization Server each time a backup occurs. The Data Synchronization Server must be registered with the Backup Server in order to receive this notification.

For additional information on the view and journal log file retrieval and notification process, refer to "View and journal retrieval and notification" (page 69).

Data Synchronization Server

The Data Synchronization Server includes the DB SyncController which coordinates the processes involved in keeping the Administration Database up-to-date with the network. Its purpose is to maintain synchronization between the database and the Passport's current view. It controls the database synchronization cycle.

The Data Synchronization Administration tool is used to view synchronization activities and basic status information, based on information provided by the Data Synchronization Server.

The Data Synchronization Server maintains synchronization with the Backup files stored by the Backup Server. Once the Backup Server retrieves the new view and journal log files from the Passports, and completes their storage to a local disk, it notifies the Data Synchronization Server and passes it the view and journal information. These notifications trigger the synchronization process.

The Data Synchronization Server compares the view and journal information that it receives from the Backup Server with the contents of the view and journal information contained in the database to determine if the database is synchronized. If the database is not synchronized with this information, the Data Synchronization Server initiates the translation of the missing views and journals into database compatible format. See "Provisioning stack (PCS/FPS servers)" (page 30).

Once the PCS/FPS process translates the files into a flat file format, the Data Synchronization Server filters the data, aggregates the components, and restructures the data so that it can be loaded into the database. See "Synchronization cycle" (page 81).

For additional information on the database population and synchronization processes, refer to "Database population and synchronization" (page 79).

Database Loaders

The Database Loader performs the following key functions:

- interacts with the Administration Database to identify the current information in the database for a device so the Data Synchronization Server can decide what needs to be loaded, and

- loads administration data

The Database Loader controls the process which loads Passport configuration views and journals (translated by FPS) into the Administration Database. It filters out all data except the data required by the Administration Database, aggregates and converts the data from the CDL format to the database format. It populates and synchronizes the Administration Database with Passport mastered portion of the Administration Database. For more information, refer to "Loading information into the database" (page 82).

Provisioning stack (PCS/FPS servers)

The FPS server of the Nodal Provisioning stack is responsible for view and journal translation. It converts view and journal files into ASCII format that can be loaded into the database.

Once the Data Synchronization Server determines that the database is not synchronized with the network, it requests appropriate view and journals from the Backup Server and requests the PCS to convert the view into a text format. The request from the Data Synchronization Server contains the necessary information for the PCS/FPS server to determine what needs to be converted.

The FPS Server of the Nodal Provisioning stack loads the required current view and/or journals from a mount point of the Backup Server and translates the provisioning data (view files and journal log files) into a set of text-based flat files. The data file location is configured through the Data Synchronization Server configuration file (DataSync.cfg) and is stored in the /opt/MagellanNMS/data/fps directory, and only the file name is returned to the Data Synchronization Server. The Data Synchronization Server deletes the files when the loading is completed.

Service provisioning tools

The following service provisioning tools have been integrated with the Administration Database, allowing for the direct update of newly provisioned data into the Administration Database:

- ATM service provisioning for ATM PVC/P, trunks, and SPVC/Ps
- Frame Relay service provisioning for Frame Relay PVCs
- FRATM service provisioning for FR.8 FrAtm Access SPVC scenarios

- IP VPN service provisioning for RFC2547 and RFC2764 autodiscovery mode-based services
- IP VPN PE provisioning to facilitate BGP configuration for Passport 2547 PE nodes.

In addition, these tools provide the capability to modify and delete services. When you provision a service using these provisioning tools, the tool makes the provisioning changes and automatically stores service information in the Administration Database upon successful activation.

For additional information on the service provisioning tools, refer to the following NTPs:

- 241-6001-600 *Preside MDM Service Provisioning for ATM User Guide*
- 241-6001-603 *Preside MDM Service Provisioning for Frame Relay User Guide*
- 241-6001-611 *Preside MDM Nodal and Service Provisioning Reference Guide*

Administration object management and discovery

The following discovery processes are provided:

- "ATM/FR/FRATM Circuit Discovery" (page 31)
- "IP VPN Service Discovery" (page 32)

ATM/FR/FRATM Circuit Discovery

Circuit discovery is a process that finds selected interface or connection components (synchronized from the network into the Administration Database) that are not part of the existing circuit and then determines the circuit to which they belong. Components which belong to the same circuit are grouped together and treated as a single entity.

You may need to perform circuit discovery in the following circumstances:

- after an initial population, and if auto discovery was not used during synchronization to establish the circuits in the database

- if you provision by methods other than the service provisioning tools. The service provisioning tools build circuits and stores circuit data in the Administration Database, but Nodal Provisioning and direct Passport commands do not.

See “Circuit discovery” (page 109) for more information on the circuit discovery process.

IP VPN Service Discovery

IP VPN Service discovery is a process that finds related Passport components that make up the IP VPN service in the network and correlates them into a VPN. This VPN can be associated with an end customer, allowing for the VPN management tools to provide customer level management of the VPN service.

IP VPN service discovery follows algorithms that are relevant to each VPN type. RFC 2547 VPN uses customer ownership of Route Targets, and RFC2764 / Direct Virtual Router VPNs uses VPN ID. IP VPN discovery is used for initial population of the database from the network, on-going network synchronization, and when the Command Line Interface, or third party provisioning applications are used to provision the network.

ATTENTION	In MDM 14.3, Enterprise P7.0.x virtual routers do not support the VPN ID attribute and consequently are not loaded into the MDM Admin DB. These VRs cannot make use of the VPN management tools in MDM, including IP VPN Service Provisioning and VPN Monitor.

For more information on the IP VPN discovery process, refer to “VPN Discovery” (page 119).

Access to database contents

Information is accessed from the Administration Database through standard SQL access. Query access is provided by the database vendor’s SQL interface. The database is implemented so that you can perform queries using only the SELECT syntax and functions defined by the Entry level of SQL-92 standard.

Customers may use any third party SQL query reporting tools, in order to meet their individual requirements. Note that only a query of the database information is currently supported. All writes to the database must be done through the appropriate MDM tools (through Database Synchronization, Service Provisioning tools and the Database Administration tool)

For a description of the database schema, see 241-6001-405 *Preside MDM Administration Database Schema*.

File and Directory structure

The table "Database file and directory structure" (page 33) summarizes the location of the main database files and directories.

Table 1
Database file and directory structure

Directory/Files	Location
SQL scripts	/opt/MagellanNMS/lib/sql
Configuration parameters for the Administration Database	/opt/MagellanNMS/cfg/cmt/CtDbAdmin.cfg
Devices information file	/opt/MagellanNMS/cfg/devices.cfg
Data synchronization configuration file	/opt/MagellanNMS/cfg/DataSync.cfg
Backup Directory for each Passport device containing the Passport views and journal log files	/opt/MagellanNMS/data/Backup_Data/ PASSPORT<Passport_name>
Journal and associated log files	/opt/MagellanNMS/data/log/<Passport_name>/ <view_timestamp>.<view_name>/ /opt/MagellanNMS/data/Backup_Data/PASSPORT/ <Passport_name>/<view_timestamp>.<view_name>/ <journal_timestamp>.journal/

Logs

The table "Storage location for log files" (page 34) summarizes the location of log files.

Table 2
Storage location for log files

Database component	Location
MDM Database Administration tool and Circuit Viewer	• /opt/MagellanNMS/data/log/ CircuitManagement.log • /log/dataSyncAdmin.log (gui) • /log/dataSyncServer.log (server)
DBSyncController: • Controller • Admin DB Loader	 /opt/MagellanNMS/data/dbsync/error.log /opt/MagellanNMS/data/dbsync/admindb.log
Backup Server	/opt/MagellanNMS/data/log/journalBackup.log

Chapter 2
Setup and Configuration

This section describes deployment considerations for database related applications and setup procedures.

For quick install instructions, for a simple Oracle configuration, see "Reference sheet for a simple Oracle configuration" (page 199).

This section contains the following topics:

- "Configuring the MDM Database Administration tool" (page 56)
- "Starting the Backup Provider" (page 58)
- "Starting the Backup Server (Backup Controller)" (page 59)
- "Starting the Restore Controller" (page 60)
- "Starting the Data Synchronization Server" (page 63)
- "Planning information for setting up and configuring the database" (page 37)
- "Supporting information for configuring the Data Synchronization file" (page 64)

Setup overview

Refer to the DBMS vendor documentation for the following database procedures:

- installing the database
  - For guidance on installing a simple Oracle database, see "Reference sheet for a simple Oracle configuration" (page 199).
- backing up and restoring the database
- implementing recovery strategies
- setting up security and user accounts

Refer to the following sections for information to install and configure the database:

- Determine your deployment option. See "Deployment options" (page 40)
- Review database instance and capacity. See "Database instance requirements" (page 42) and "Database capacity planning" (page 42).
- Create the database instance.For more information, refer to the Oracle documentation.
- Install the schema using "Creating the Administration Database schema for an Oracle RDBMS" (page 43)

- "Specifying the GMDR host" (page 45) for the alarm source if the Backup is triggered on alarm (optional)
- "Configuring backup information for an alarm driven backup" (page 46)
- "Configuring data synchronization information for database use" (page 48)
- "Configuring the secondary Data Synchronization Server for cold standby" (page 49) (optional)
- "Configuring the Passport Configuration Server" (page 50)
- "Setting up the Passport Configuration Server to run from a different workstation" (page 54) (optional)
- "Configuring the Database access file" (page 55) for database client applications
- "Configuring the MDM Database Administration tool" (page 56)
- Start the servers. For more information, refer to "Starting the Backup Server (Backup Controller)" (page 59), "Starting the Restore Controller" (page 60) and "Starting the Data Synchronization Server" (page 63).

Planning information for setting up and configuring the database

This section contains the following topics:

Software requirements

To run the Preside MDM Administration Database related features, the following must be installed and/or setup

- Sun Solaris 2.7 or 2.8 software

- Oracle 8i (8.1.7) or Oracle 9i (9.0.1 and 9.2) client software installed on the machine where DBSyncController, and client application (Service Provisioning, Circuit Viewer, and MDM Database Administration tool are running)
- the Oracle 8i or Oracle 9i Server and Client installed and setup for the Administration Database

Hardware and engineering considerations

To run the Preside MDM Administration Database related features, you must have the following minimum hardware configuration:

Table 3
Hardware and engineering configurations

	Small networks less than 20 devices and 50K endpoints	**Medium networks less than 100 devices and 200K endpoints**
#CPU	2	4
RAM	1.0 GB	2.0 GB
Swap	2.0 GB	3.0 GB
Disk	5.5 GB	8.0 GB
# disks	1 or 2	2 to 4 disks

Note: For large networks, contact Nortel Networks.

Deployment considerations

Before you set up the database and other servers, you need to decide how to deploy the database, based on the following factors:

- size of the network to be managed
- operational organization (centralized or distributed setup)
- reliability and redundancy requirements
- network size

Taking into account these factors, the following provide an example of a small, medium and large network size:

- small networks
  - less than 20 devices
  - less than 50K (@25K circuits) circuit end points in the network
  - 5K to 10K end points on a device
  - less than 5 devices updated every day on average
  - centralized operations
- medium network
  - less than 100 devices
  - less than 200K (100K circuits) endpoints in the network
  - up to 10K circuit end points on a device
  - less than 20 devices updated every day on average
  - centralized and/or regionalized operations
- large network
  - more than 100 (approximately 1000) devices
  - around 1000K circuit end points
  - large device with 50K circuit endpoints
  - less than 100 devices updated every day on average
  - centralized and/or regionalized operations

Centralized vs distributed

The system allows centralized deployment in which all clients and servers are deployed in a centralized workstation. The system also allows servers and clients to be distributed and duplicated on different workstations to increase scalability and availability and/or match customer operational organization.

Data Synchronization Server

Consideration should be given to load balancing for the Data Synchronization Server. The Data Synchronization Server translates, processes, and writes to the database. Due to this workload it may be advisable to distribute the

workload across several machines. To address this issue, multiple Data Synchronization Servers could be deployed. The Backup Server supports broadcasting synchronization requests to multiple Data Synchronization Servers, and the Passports managed by the Data Synchronization Server is controlled through the Backup Server configuration file.

A cold standby configuration of the Data Synchronization Server is supported in this release for reliability. This is achieved by configuring two Data Synchronization Servers with the same name on two different workstations and enabling only one at a time.

Backup Server

You can configure multiple Backup Servers for load balancing as well as redundancy. To ensure Backup server reliability, redundancy can be set up for the Backup Server. This is especially critical for Device recovery. Two or more independent Backup Servers can be running at the same time on different MDM workstations.

Both Backup Servers cover the same Passports and are triggered by the same alarms from GMDR, which are generated by the Passports. A command line option can specify the host to which the GMDR server connects.

The Backup Servers connect to two different GMDR's, one for each Backup Server. In another possible scenario, one common GMDR could be running on a separate workstation. Both Backup Servers would receive alarms from this GMDR and trigger the servers to do backups. Regardless of the setup, two backups are done in parallel and independently. The two Backup Servers do not communicate with each other.

Deployment options

The table "Deployment options" (page 40) provides some deployment options based on the network size, remotability and redundancy/load balancing considerations. Also see 241-6001-807 *Preside MDM Passport/ SNMP Devices Backup and Restore User Guide*.

Table 4
Deployment options

Option	Description
1a (small network)	-centralized; MDM and the database are all on one workstation -MDP is on another workstation -2 to 5 remote clients through an x-term -redundancy through complete duplication, if required
1b (small network)	-centralized; MDM, MDP and the database are on one workstation -2 to 5 remote clients through an x-term -redundancy through complete duplication, if required
2 (small network)	-all servers and the database are on one large workstation -clients are on one or more separate workstations
medium network centralized	-most of the servers and clients are on a central workstation -the Oracle database, and MDP are on separate workstations -multiple remote clients through x-term -redundancy through complete duplication and cross feeding from servers
medium network distributed	-large servers and clients on separate workstations. The size of the workstations is dependent upon the number and size of the servers on a workstation. -Oracle database, and MDP are on separate workstations -multiple remote clients through an x-term -redundancy through redundant servers cross feeding clients -duplicate servers for load balancing

Database instance requirements

For the Oracle database server to provide the best performance, a separate instance of the Oracle Relational Database Management System (RDBMS) is required. If an existing instance supports other databases, you need to create a new database instance for this application only.

Standard Oracle installation procedures may be obtained from the Oracle Administrators Reference for SUN SPARC Solaris, part no A85349-01.

Database capacity planning

You must ensure that you have enough disk space on the Oracle database workstation to store administration data. Database schema require a special table space to contain the Administration Database tables.

Database size estimation

Database tables are populated in varying degrees based on device configurations. The database disk size is derived from the following approximation:

Administration Database	Depends mainly on the number of circuits	5 Kbytes/circuit

This number is approximate, based on average database sizes.

Disk Space Recommendations

This section describes the recommended disk space for the Administration Database. To estimate the disk space required for storing Oracle data contents, use the following formula:

Total = # of thousand circuits x 5M for 1 hop only
= [(# of thousand circuits) x 5M x (1.5/2) x # of hops)], for > 1 hops.

For additional information on disk space requirements, refer to the Oracle documentation.

Creating the Administration Database schema for an Oracle RDBMS

Use this procedure to create to create the Administration Database schema for the Oracle relational database management system. This procedure uses a series of scripts to create the following:

- the Administration Database schema
- the database tables
- user access roles

Prerequisites

The Oracle relational database management system is installed.

Procedure steps

1. Go to the directory that contains the Administration Database schema installation scripts:

   ```
   cd /opt/MagellanNMS/lib/sql/admindb/oracle
   ```

2. Connect to the Oracle database in SQL*Plus, logging in as the owner of the Administration Database schema.

3. At the SQL>prompt, type the following command in one continuous line:

   ```
   @@/opt/MagellanNMS/lib/sql/admindb/oracle/
   admin_ddl.sql
   ```

4. Create access roles for setting various levels of permission for accounts that access the database by entering the following command in one continuous line:

   ```
   @@/opt/MagellanNMS/lib/sql/admindb/oracle/
   admin_roles.sql
   ```

   The following roles are available:

   - ADMIN_REPORTING is the lowest level of permission and has read (SELECT) permission on all Administration Database tables.
   - ADMIN_APPLICATION is an intermediate level of permission and has read (SELECT) permission on all tables and write (INSERT, UPDATE, and DELETE) permission on all tables except the SCHEMA_VERSION table. This role is intended for users of the service provisioning and Circuit Viewer tools.

- ADMIN_ADMIN is the highest level of permission and provides full access to all tables in the Administration Database schema.

5 After creating the roles, you can assign them to Administration Database users.

For example, you can grant ADMIN_APPLICATION to <cv application user>

Warning and error conditions

Errors generated by SQL Plus during this procedure are displayed in standard output. If you want to capture these errors you need to use the SQL Plus spool function.

Configuring MDM for Oracle version compatibility

Oracle 9i is the default selection when Preside Multiservice Data Manager (MDM) is installed. Use this procedure under the following circumstances:

- you are installing a new version of Preside Multiservice Data Manager (MDM) and wish to continue using Oracle 8i
- if you wish to use Oracle 9i after your previous Preside MDM installation was configured to use Oracle 8i

Any subsequent installations of MDM automatically retain the Oracle version that you select.

Prerequisites

You must have root user privileges.

Procedure steps

1 Log in as root on the MDM machine.

To configure MDM for Oracle 8i, go to step 2.

To configure MDM for Oracle 9i, go to step 3.

2 Configure MDM for Oracle 8i:

```
/opt/MagellanNMS/system/config/setoracle 8i
```

3 Configure MDM for Oracle 9i:

```
/opt/MagellanNMS/system/config/setoracle 9i
```

Specifying the GMDR host

This procedure is required if a Passport is backed up on alarm. Use this procedure to specify the GMDR host if the GMDR runs on a different host than the Backup Server. You use the -gmdrhost option.

Procedure steps

1 Enter the following as a continuous command:

```
/opt/MagellanNMS/bin/nsctlbck
-notification
-gmdrhost <hostname>
```

Variable definitions

Variable	Definition
-notification	is requested to synchronize the database.
-gmdrhost <hostname>	specifies the gmdr host.

Migration notes

Version 13.4 and earlier

Note the following information when migrating software from version 13.4 and earlier to version 14.3:

- Migration is automatic.
- The DataSync server is added to the SVM list of servers.

Version 14.1

Note the following information when migrating software from version 14.1 to version 14.3:

- The DBSync.cfg file is replaced by the DataSync.cfg file which may only be edited using the Configuration Editor.
- The DBSynchController.cfg file has been merged into the DataSync.cfg file. This file is automatically migrated at installation.

Version 14.2

Note the following information when migrating software from version 14.2 to version 14.3:

- The DBSync.cfg file is replaced by the DataSync.cfg file which may only be edited using the Configuration Editor.
- The DBSynchController.cfg file has been merged into the DataSync.cfg file. This file is automatically migrated at installation.

Configuring backup information for an alarm driven backup

Use the following procedure to specify the devices you wish to backup and to configure basic backup information in the DataSync.cfg file.

Prerequisites

Verify that all the devices you want to backup and restore have been defined on the Host Group Directory Server (HGDS). For more information, refer to 241-6001-303 *Preside MDM Administrator Guide*.

Procedure steps

1. Start the Server Administration application and complete the required authorization.

   For more information, refer to 241-6001-303 *Preside MDM Administrator Guide*.

2. In the list of servers, select **Backup Controller**.
3. Right click to select **Edit Configuration**->**Backup Server**.

   The **Configuration Editor** opens.

4. Select **Backup Server** element.
5. Right click and select **Add Element**.

   The **Add Element** dialog displays.

6. Verify that **Group** is selected and click **OK**.
7. Select the **New Group** element.
8. Enter the Group name.
9. Verify that the **enabled** field is set to **True**.

   If you do not wish to use the values that have been specified for the default group, perform step 10 through step 18.

10 Select your new group from the element tree.

11 Right click to select **Add Element**.

12 In the **Add Element** dialog, select **Authentication** and click **OK**.

13 Repeat step 11 and step 12, selecting **BackupOptions** and **DBSynchOptions**.

At this point, your new group has three subelements (Authentication, BackupOptions and DBSynchOptions).

14 Click on the group element to expand it.

15 Select **Authentication** and

a. enter the appropriate username

b. either enter the password

OR

c. set the usePassword File to **True** and enter the location of the password file in the passwordFileName field.

16 Select the **BackupOptions** element and verify that onAlarm is set to **True** if you wish backups to be performed on alarm.

Note that you do not have to select this option at this time. You can set this option later using the Backup and Restore tool. For more information, refer 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

17 Select **DBSyncOptions** and:

a. Verify that enabled is set to **True** if you wish to send a notification to the Data Sync server whenever a backup is performed.

b. Enter the name of the DBSyncController in the **server** field. Note that if you leave the server field blank, the system defaults to localhost.

18 Select **Save** from the **File** menu.

For more information on editing the other Backup Server parameters, refer to “Supporting information for configuring the Data Synchronization file” (page 64) or to the more detailed configuration information in 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

Configuring data synchronization information for database use

Use the following procedure to configure data synchronization information for Passport devices in the DataSync.cfg file.

Procedure steps

1. Start the Server Administration application and complete the required authorization.

   For more information, refer to 241-6001-303 *Preside MDM Administrator Guide*.

2. In the list of servers, select **Data Sync Server**.

3. Right click to select **Edit Configuration** -> **Server Configuration**.

   The **Configuration Editor** displays.

4. Expand the **Embedded Servers** selection.

5. Select **DBSynchController**.

6. Set the **enabled** field to **true**.

7. Select **Save** from the **File** menu.

   This ensures that when there is a change to the server information, the Data Sync server will trigger a backup.

8. In the list of servers, select **Data Sync Server**.

9. Right click to select **Edit Configuration** -> **DBSync Controller**.

10. Verify that the information in each field is correct for your system. For more information, refer to “Supporting information for configuring the Data Synchronization file” (page 64).

    Note: In most cases, the information is correct for your system. The only field that requires updating is the authentication.

Configuring the secondary Data Synchronization Server for cold standby

Use this procedure to configure the secondary Data Synchronization Server for cold standby. A cold standby configuration is achieved by configuring two Data Synchronization Server with the same name and identical DataSync.cfg configuration files (specified by the DBSyncName in the devices information file and the Data Synchronization configuration file) on two different hosts and enabling only one at a time.

Procedure steps

1. Copy the data synchronization configuration file /opt/MagellanNMS/cfg/DataSync.cfg from the workstation where the primary Data Synchronization server is running. The primary and secondary Data Synchronization servers should keep the same set of configuration files.
2. If the primary Data Synchronization server was terminated, reset all database LOADING view status to FAILED.
3. Use the following SQL statements for updating AdminDB load status:

   Note: This step should be performed by the Data Base Administrator with an Oracle background.

   update ADMIN_NODE_HISTORY set load_status='FAILED'
   where LOAD_STATUS='LOADING' and DBSYNC_ID='hostname:port';
4. Start the secondary Data Synchronization Server. See “Starting the Data Synchronization Server” (page 63).

Configuring the Passport Configuration Server

The Passport Configuration Server (PCS) is used for both Nodal Provisioning and database synchronization. If PCS is shared by the Data Synchronization Server and Nodal Provisioning, this procedure is not required. You use this procedure to configure the Passport Configuration Server to serve only the Synchronization Server. You can achieve this by running the Passport Configuration Server on a different port than that used by Nodal Provisioning.

Procedure steps

1. In the Preside MDM window, select **System** -> **Administration** -> **Server Administration** to open the **Server Administration** tool.
2. From the Security menu, select the **Authorize** command.
3. In the **SVM Enter Authorization Password** dialog box, type a valid password and click **OK**.
4. From the **Edit** menu, select **Edit** -> **New**.

   The **Server Administration** dialog to edit servers opens.
5. In the **Descriptive name** field, type a new entry by specifying the name of the server that you are adding, for example:

   ```
   pcserver
   ```
6. In the **Startup command** field, type the following command:

   ```
   /opt/MagellanNMS/bin/pcserver
   -p <portNumber>
   ```

   Note: If PCS is configured for only the Data Synchronization server, you need to use a different port number than that used for Nodal Provisioning.
7. Enable the **Automatic startup at reboot time** option.
8. Click **Save and Start**.

   The data that you entered is stored and the server is started.
9. From the **File** menu, select **Refresh Server list**.
10. Modify the PPConfigServer parameter in the /opt/MagellanNMS/cfg/DataSync.cfg file to use the port number specified in step 7.

    <PPConfigServer host="localhost" port="xxxx" dataDir="/opt/MagellanNMS/data/fps" />

11 Restart the Data Synchronization Server.

Variable definitions

Variable	Definition
`-p portNumber`	is the port number. Use a different number than that used by Nodal Provisioning.
`xxxx`	is the port number already specified.

Configuring the Passport Configuration Model Server

The Passport Configuration Model Server (PCMS) is used for both Nodal Provisioning and database synchronization. If PCMS is shared by the Data Synchronization server and Nodal Provisioning, this procedure is not required. You use this procedure to configure PCMS to serve only the Data Synchronization server. You can achieve this by running the PCMS on a different port than used by Nodal Provisioning.

Procedure steps

1. In the Preside MDM window, select **System** -> **Administration** -> **Server Administration** to open the **Server Administration** tool.
2. From the Security menu, select the **Authorize** command.
3. In the **SVM Enter Authorization Password** dialog box, type a valid password and click **OK**.
4. From the **Edit** menu, select **Edit** -> **New**.

   The **Server Administration** dialog to edit servers opens.
5. In the **Descriptive name** field, type a new entry by specifying the name of the server that you are adding, for example:

   ```
   PP Config Server
   ```
6. In the **Startup command** field, type the following command:

   ```
   /opt/MagellanNMS/bin/pcms [-numOfModels <n>] [-
   modelSize <s>] [-preloadModels <v1> <v2>...]
   ```

   where
   n - number of models to be loaded. Default is 2
   s - model size of model in Mb. Default is 20Mb
   v1, v2 - Passport model version number
7. Enable the **Automatic startup at reboot time** option.
8. Click **Save and Start**.

   The data that you entered is stored and the server is started.
9. From the **File** menu, select **Refresh Server list**.

For more information, refer to 241-6001-310 *Preside MDM Server Reference Guide*.

Variable definitions

Variable	Definition
`-p portNumber`	is the port number. Use a different number than that used by Nodal Provisioning.
`xxxx`	is the port number already specified.

Setting up the Passport Configuration Server to run from a different workstation

Use this procedure to set up the Passport Configuration Server to run from a different workstation than the Data Synchronization server workstation.

Note: The primary and secondary Backup Server data directory should be accessed by the Backup Server, Data Synchronization Server, and the Passport Configuration Server.

Procedure steps

1. Mount the PPConfigServer data directory to the local machine.
2. Update the data directory <directory>, <host> and <port> of the PPConfigServer parameter in the data synchronization configuration file.
3. Start the Passport Configuration Server.
4. Restart the Data Synchronization Server.

Configuring the Database access file

Use this procedure to configure the /opt/MagellanNMS/cfg/dba/dbaccess.cfg. This file is required for database client applications (Service Provisioning, Circuit Viewer, MDM Database Administration and Data Synchronization Administration) to access the database. One copy of the file is required on a workstation, and all client applications that workstation shares.

Procedure steps

1. From the **Options** menu of MDM Database Administration, select **Configuration**.

   The **Configuration Options** dialog opens.

2. For the **Database** tab, complete the following parameters for database connectivity:

   - For **Database Vendor:** parameter, specify that Oracle is to be used to support circuit management.
   - For the **Database Host** parameter, specify the IP address of the workstation where the database is installed.
   - For the **Database Name** parameter, specify the database name recognized by the server. For Oracle, the database name is a registered name (called a SID or database ID).
   - For **Database Port** parameter, specify the TCP port on which the database server listens for connections.

3. Save the configuration changes by clicking **OK**.

Configuring the MDM Database Administration tool

Use this procedure to configure the /opt/MagellanNMS/cfg/cmt/CtDbAdmin.cfg. This file lets you specify the configuration of the MDM Database Administration tool.

Procedure steps

1. From the **Options** menu of MDM Database Administration, select **Configuration**.

   The **Configuration Options** dialog opens.

2. With the **Database** tab selected, complete the following parameters:

   - **Database Vendor**: the name of the Database vendor
   - **Database Host**: the IP address of the Database server
   - **Database Name**: the name of the Database
   - **Connection Port**: the Port number
   - **Database disabled**: Set this to false.

3. With the **Other** tab selected, complete the following parameter:

   - **Max. Rows to display**: the maximum number of rows that the MDM Database Administration tool receives from a query. This parameter can help reduce memory consumption or the amount of data to display in the tool window. Any query which would return more objects than this limit is truncated. A zero value indicates no limit. Zero is the default.

4. Save the configuration changes by clicking **OK**.

5. From the **Options** menu, select **Logging**.

   The **Logging Options** dialog opens.

6. Determine the information to be logged. The severity threshold for controlling log message output consists of the following options:

   - **Errors** denotes a severe, unexpected application error.
   - **Errors, Warnings** denotes a warning condition, often expected. This is the default.
   - **Errors, Warnings, Information** identifies a trace message used for problem diagnosis.

- **Errors, Warnings, Information, Debug info** denotes a trace message used for problem diagnosis. Messages with a severity lower than specified will not be written.

7 Select the information to be logged by clicking the appropriate threshold. Then click **OK**.

Starting the Backup Provider

Use this procedure to start the Backup Provider and add it to the server list in the Server Administration tool.

CAUTION

Starting the Backup Controller

The Backup Provider must be started before the Backup Backup Controller (Backup Server) when using the -notification option. The Backup Controller is known as the Backup Server when the -notification option is specified. See 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

Procedure steps

1. In the Preside MDM window, select **System** -> **Administration** -> **Server Administration** to open the **Server Administration** tool.
2. From the Security menu, select the **Authorize** command.
3. In the **SVM Enter Authorization Password** dialog box, type a valid password and click **OK**.
4. From the **Edit** menu, select **Edit** -> **New server**.

   The **SVM New Server Selection** displays.
5. Find the **Backup Provider** in the list by expanding the server categories.
6. Select the Backup Provider and click **Select Server**.

   The **SVM Edit Server** displays.
7. Enable the **Automatic startup at reboot time** option.
8. Click **OK**.

   A confirmation dialog displays.
9. Click **Yes** to confirm.
10. Click **Cancel** to close the **SVM Edit Server** window.
11. Right-click on the Backup Provider entry in the server list.
12. From the pop-up menu, select **Start**.

    The Backup Server starts.

Variable definitions

Variable	Definition
`-port <portno>`	is the port number the Restore Provider uses. The default is 5020.

Starting the Backup Server (Backup Controller)

Use this procedure to start the Backup Server (Backup Controller) and add it to the server list in the Server Administration tool.

Note: The Backup Controller is known as the Backup Server when the -notification option is specified. For more information, refer to 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

Procedure steps

1. In the Preside MDM window, select **System** -> **Administration** -> **Server Administration** to open the **Server Administration** tool.
2. From the Security menu, select the **Authorize** command.
3. In the **SVM Enter Authorization Password** dialog box, type a valid password and click **OK**.
4. From the **Edit** menu, select **Edit** -> **New server**.

   The **SVM New Server Selection** displays.
5. Find the **Backup Server** in the list by expanding the server categories.
6. Select the Backup Server and click **Select Server**.

   The **SVM Edit Server** displays.
7. In the **Startup command** field, type the following command and the appropriate variables:

   `/opt/MagellanNMS/bin/nsctlbck`

   For more information on starting this server, refer to “Turning on the backup function and specifying the number of parallel backups” (page 74).

   For more information on the command variables, refer to “Variable definitions” (page 60).

8 Enable the **Automatic startup at reboot time** option.

9 Click **OK**.

A confirmation dialog displays.

10 Click **Yes** to confirm.

11 Click **Cancel** to close the **SVM Edit Server** window

12 Right-click on the Backup Server entry in the server list.

13 From the pop-up menu, select **Start**.

The Backup Server starts.

Variable definitions

Variable	Definition
`-port <portno>`	is the option to specify the port to use. The default is 5000.
`-c <fn>`	use Controller config file <fn> -full name
`-notification`	starts the Backup Controller as the Backup Server.
`-nbofbck <#>`	is the option to specify the maximum number of parallel backups.
`-DB_Synch_port <port>`	is the option to use that port for communication with the DB_Synch. The default is 5050.
`-h`	is the option to display command line usage.
`-d`	is the option to set debugging on. The default is off.

Starting the Restore Controller

Use this procedure to start the Restore Provider and add it to the server list in the Server Administration tool.

Procedure steps

1. In the Preside MDM window, select **System** -> **Administration** -> **Server Administration** to open the **Server Administration** tool.
2. From the Security menu, select the **Authorize** command.
3. In the **SVM Enter Authorization Password** dialog box, type a valid password and click **OK**.
4. From the **Edit** menu, select **Edit** -> **New server**.

   The **SVM New Server Selection** displays.
5. Find the **Restore Controller** in the list by expanding the server categories.
6. Select the Restore Controller and click **Select Server**.

   The **SVM Edit Server** displays.
7. In the **Startup command** field, type the following command:

   `/opt/MagellanNMS/bin/nsctlrst`

   For more information on these variables, refer to “Variable definitions” (page 61).
8. Enable the **Automatic startup at reboot time** option.
9. Click **OK**.

   A confirmation dialog displays.
10. Click **Yes** to confirm.
11. Click **Cancel** to close the **SVM Edit Server** window
12. Right-click on the Restore Controller entry in the server list.
13. From the pop-up menu, select **Start**.

    The Restore Controller starts.

Variable definitions

Variable	Definition
`-p <portno>`	is the option to specify the port to use. The default is 5001.
`-c <fn>`	is the option to specify the Controller configuration file (<fn> = full name)

Variable	Definition
-d	is the option to set debugging on. The default is off.
`-h`	is the option to display command line usage.

Starting the Data Synchronization Server

Use this procedure to start the Data Synchronization Server, and to add it to the server list in the Server Administration tool.

Procedure steps

1. In the Preside MDM window, select **System** -> **Administration** -> **Server Administration** to open the **Server Administration** tool.
2. From the Security menu, select the **Authorize** command.
3. In the **SVM Enter Authorization Password** dialog box, type a valid password and click **OK**.
4. From the **Edit** menu, select **Edit** -> **New server**.

   The **SVM New Server Selection** displays.
5. Find the **DataSync Server** in the list by expanding the server categories.
6. Select the Data Sync Server and click **Select Server**.

   The **SVM Edit Server** displays.
7. Click **OK**.

   A confirmation dialog displays.
8. Click **Yes** to confirm.
9. Click **Cancel** to close the **SVM Edit Server** window
10. Right-click on the Data Sync entry in the server list.
11. From the pop-up menu, select **Start**.

    The Data Synchronization Server starts.

Variable definitions

Variable	Definition
`-help`	is the option to display command usage information.
`-cfg <configFile>`	is the option to specify the configuration file to be used. If no parameters are specified, defaults are retrieved from the configuration file DataSync.cfg in the /opt/MagellanNMS/cfg directory.
`-log <logFile>`	is the option to have logging enabled and a log of the processing steps written to the specified log file

Supporting information for configuring the Data Synchronization file

The Configuration Editor allows you to edit the DataSync.cfg file. You can launch the Configuration Editor from the Server Administration Tool.

The editor has two panes. The left pane displays the symbol for the DBSynchController which can be expanded to display a tree hierarchy in which you select a parameter category to edit. The right pane displays the parameters contained in the selected category. For more information on configuring the Data Synchronization file, see “Data Synchronization Configuration file parameters” (page 65).

> ***Note:*** The parameters you specify for data synchronization depend on what you have specified to be backed up. For more information on configuring the DataSync.cfg file for backup and restore, refer to 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

Table 5
Data Synchronization Configuration file parameters

Category	Field	Description	Default
DBSyncController Main selection	name	Option to specify the name of the DBSync Controller.	
	maxParallelUpdates	Option to limit the number of simultaneous updates by the DBSyncController that can occur	5
	mode	Option to specify the database that the information is loaded into. This value is always admin.	admin
	connection-Timeout	Option to specify the time-out value which server attempts to connect to the Backup Server	45
	dataDir	Option to specify the directory where the DBSyncController data are stored	
	nRetries	Option to specify the number of retries performed on a node. When synchronization is attempted and failed, the DBSyncController retries the load nRetries times.	3
Authentication	username	Username to access device	
	password	Password to access device	
	usePasswordFile	Determines if a password file is used for access to the account	false
	passwordFile	Path to the file that contains an encrypted password	
AutoDiscovery	type	Type of service autodiscovery is enable for (ATM, FR, IP VPN)	
	autoDiscovery	Option to specify whether or not automatic discovery is enabled.	false

(Sheet 1 of 3)

Table 5
Data Synchronization Configuration file parameters (continued)

Category	Field	Description	Default
	filterOnCorrelationTag	Option to specify whether a provisioned correlation tag can be used as a starting point for discovery	
	atmPVCMethod	Option to specify the discovery or validation method to be used for the ATM PVC circuits	
Logging	logErrorToFile	Option to specify logging DBSyncController errors to file	true
	logFileName	Name of the log file	/opt/ MagellanNMS/ data/dbsync/ dbsync.log
	logError	Option to specify logging	true
PPConfigServer	host	Option to specify the host name or ip of the Passport Configuration server to communicate with.	localhost
	dataDir	Option to specify where the PPConfigServer data are stored.	/opt/ MagellanNMS/ data/fps
	port	Option to specify the Passport Configuration (PCS) server port, to communicate with.	6760
BackupServer	host	Option to specify the Backup server host name or IP address, to communicate with	localhost
	port	Option to specify the Backup server port, to communicate with.	5050
	dataDir	Option to specify the backup data directory where the views and/or journals are stored.	/opt/ MagellanNMS/ data/ Backup_Data

(Sheet 2 of 3)

Table 5
Data Synchronization Configuration file parameters (continued)

Category	Field	Description	Default
	deviceConfigFile	Option to specify the device configuration file directory.	/opt/ MagellanNMS/ cfg/dataSync.cfg
	server	Name of the dbSynchController to notify when a device is backed up	
Note 1: If there is more than one Backup server, you need to specify the above Backup server parameters for each of them.			
Note 2: The following fields are related to the backup and restore functionality.			
BackupServer	port	Option to specify the Backup server port, to communicate with.	5050
	dataDir	Option to specify the backup data directory where the views and/or journals are stored.	/opt/Magellan/ NMS/data/ Backup_Data
Authentication	username	Username to access device	
	password	Password to access device	
	usePasswordFile	Determines if a password file is used for access to the account	false
	passwordFile	Path to the file that contains an encrypted password	
BackupOptions	onAlarm	Determines if the devices in the group are backed up when the sever receives a configuration event from a device	true
DBSync Options	enabled	Determines if a dbsynchcontroller is notified when the device is backed up true	true
	server	Name of the server to notify when a device is backed up	

(Sheet 3 of 3)

Chapter 3
View and journal retrieval and notification

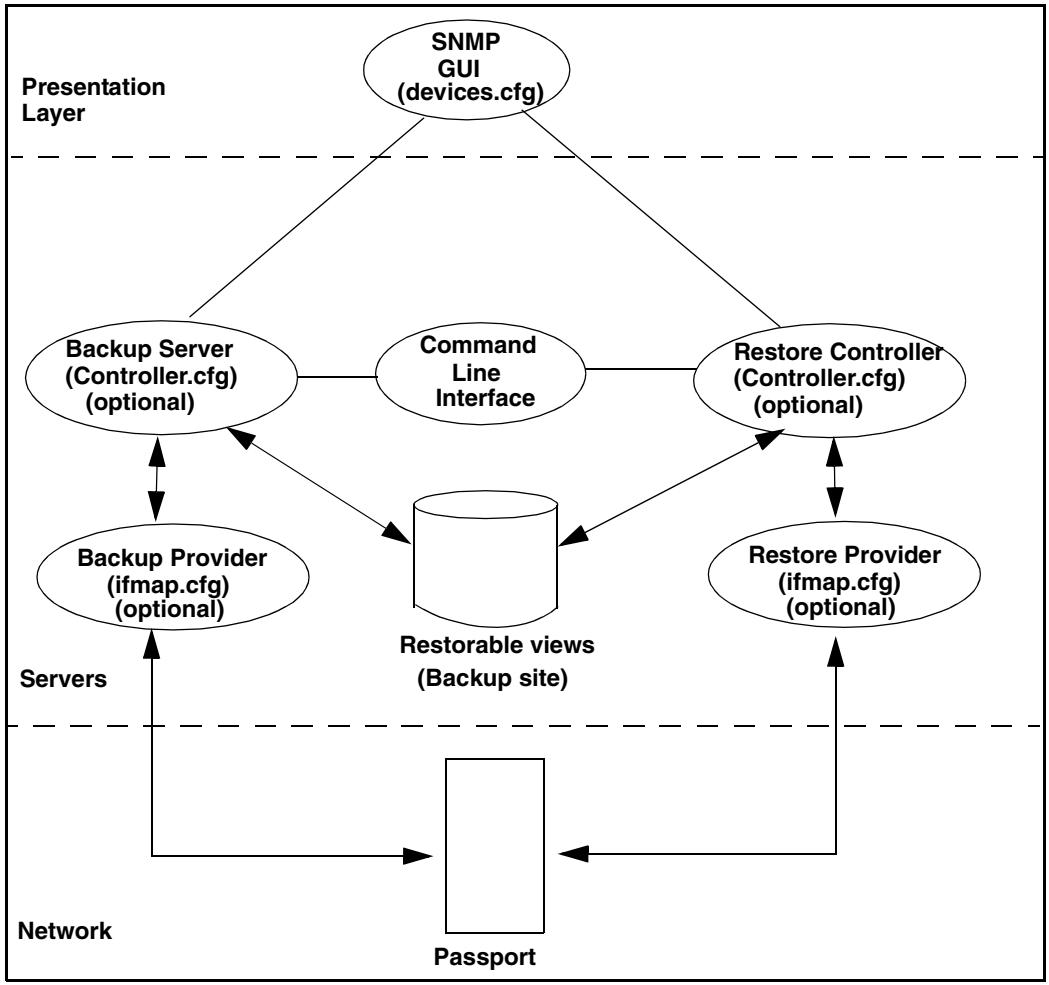
This section describes the view and journal retrieval and notification processes. This section contains the following topics:

Backup Server

The retrieval of view and journal log files from the Passport network is performed by the Backup Server. The synchronization of information from the Passport to the Administration Database is supported through the view and journal files collected by the Backup and Restore capability. The journaling capability on Passport allows for the efficient support of near-real time synchronization of the database with network changes.

The figure "Backup server architecture" (page 70) illustrates the backup server architecture.

Figure 2
Backup server architecture



The Backup Server manages the view and journal log file backup task, monitors the backup and is the source of the files which are loaded into the database. It provides the following specific roles in relation to the database:

- manages the retrieval and storage of the views and journal files for database synchronizing. The Backup Server receives Passport alarms from GMDR, queues them, and monitors the backup.

- notifies the Data Synchronization Server each time a backup triggers the updates to the database. The notifications contain the details of the device's current view, journals, timestamps and state. This information is stored to disk so that the Data Synchronization Server can determine the current state of each device upon start-up.

Triggering backups

Backups can occur on a scheduled basis, they can be initiated by notification of on-switch provisioning changes through the Backup Server or they can be initiated through the Backup and Restore tools. The Backup Server can be triggered to perform a backup in the following ways:

- "On alarm, with journaling supported" (page 71)
- "On alarm with journaling not supported" (page 72). This mode is only recommended for small networks.
- "On demand" (page 72)

On alarm, with journaling supported

You specify the Passport devices that you want to back up using the Data Synchronization configuration file, DataSync.cfg, found in /opt/MagellanNMS/cfg, on the Backup Server workstation. For details on the procedure to add a Passport device for backup, see 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

The following are activities that trigger the Backup server to check if a backup is required:

- confirm prov after an activation (7000 0007 clear)
- commit prov (7000 0039)
- reset of the Passport switch (7000 0038 set)
- MDM reconnect to the Passport switch (09990001 clear). This is a proxy alarm that is generated by MDM, not the Passport.

When the Backup Server receives any of these alarms, it obtains the current view and journals, for restore purposes, from the Passport and stores them in the recovery.INFO file.

If an activate is followed by a commit, all outstanding journals are compressed, loaded, and then the activation tags are checked to verify if the loading of the committed view is required. The activation tag allows the Data Synchronization Server to determine if the committed view is the same as the previous committed view, plus all the journals, since the last commit

On alarm with journaling not supported

This mode is only recommended for a small network. “On alarm, with journaling supported” (page 71) is recommended for larger networks because journaling allows MDM to take advantage of journal “delta” files which allow for the more efficient transfer of changes. In a large network, there is likely to be large numbers of view files. Also, more than one devices will likely be updated several times and concurrently. Where journaling is not used, the entire view file is transferred for each activation. This adds a large amount of data traffic between the Backup Server and the network, requires large disk space to store all views, and puts heavy demand on MDM processing and memory for database synchronization.

Passports that support journaling, but do not use it, only send out Confirm and Node Reconnect alarms generated by the Preside Multiservice Data Manager (MDM). In this situation, the Backup Server is only triggered by the confirm alarms. It obtains only the Committed view from the Passport and stores this information in the recovery.INFO file.

As is the case with journaling supported Passports, the Backup Server checks if the current view has a backup file. If not, it FTPs the file to the backup site.

On demand

Backups can be triggered in three ways; using the Backup and Restore tools, through a cron job or using an operator initiated command.

To use the Backup and Restore tools or cron job, refer to 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

For the command line option, you enter the following command:

```
/opt/MagellanNMS/bin/nsbck -demand <group>
```

When a backup on demand option is selected, a message is sent to the Backup Server to perform a backup on demand for this group. It then puts the devices in this group in the queue to be backed up. From this point, the backup is done in the same way as those that are triggered by alarms.

When you specify the backup on demand command with the <group> option, the backup is executed on all the Passport devices in the specified group. The value <group> is an optional value that triggers a backup on demand of the Passport devices that are defined in the HGDS.

To trigger a backup of all the Passports simultaneously, you configure the DataSync.cfg file to give all the Passport nodes the same group label, and execute the command, /opt/MagellanNMS/bin/nsbck -demand, without specifying a group.

Backup Server processing of alarms

The processing of alarms by the Backup Server is the same for Passport devices which are journal-enabled and those without journaling.

The following sequence of events is followed by the Backup Server when it receives an alarm:

1 Verifies if the committed view is backed up. If not, it does so.

2 If the current view has a name and is not backed up, backs it up.

3 Compares timestamps of journal directory on-switch and on the backup site. If different, a new journal directory is created.

4 Verifies that all journals are backed up. If not, it backs up the missing files.

5 Updates the recovery.INFO file.

6 Gets the running AV list and updates the avl.INFO file.

7 Updates the view.INFO file

8 Notifies the Data Synchronization Server.

Turning on the backup function and specifying the number of parallel backups

Alarm-triggered backups are optional and can be used with both journal and non-journal devices. However, there may be operational considerations if journaling is not supported.

The Backup Server command line can be configured to initiate alarm-triggered backups and to specify the maximum number of parallel backups. The -nbofbck <#> manages the number of parallel backups:

```
/opt/MagellanNMS/bin/nsctlbck -notification -nbofbck
<#>
```

This command is edited using the Server Administration tool. For more information on editing this command and starting the Backup Server, refer to "Starting the Backup Server (Backup Controller)" (page 59).

When the -notification option is added to the /opt/MagellanNMS/bin/nsctlbck command it turns on the alarm-triggered and on demand backup functions. The -notification option is required by the Backup Server to notify the Data Synchronization server, so if the backup function is not turned on, automatic synchronization cannot occur.

If GMDR is on a different workstation than the Backup Server, you need to specify the -gmdrhost option in the command line for the Backup Server for alarm driven backup to work.

The -notification option indicates that the Backup Server is backing up journal log and/or view files automatically as the changes happen on the Passport device. By default, if no option is specified in the Backup Server, it will start in regular backup mode and no database synchronization will occur. You use the Server Administration tool to set the options for the server.

The -nbofbck <#>, where # is the maximum number of backups, limits the number of backups that can be performed in parallel. The default is 20. Backup requests coming after the maximum number are queued in a waiting queue and are transferred to the executing queue if the executing queue is not full. That is, it has less than the maximum number of parallel backups, as

specified in the nbofbck <#> option of the Backup Server command line. By limiting the number of simultaneous backups, you reduce congestion problems that may occur with a large number of simultaneous backups.

To avoid performing multiple backups in parallel on the same Device, two queues are used: an executing queue and a waiting queue. When the Backup Server receives a backup request, and the request is not yet in any queue, it is put at the end of the waiting queue. If it is already in the queue, it is ignored.

If already in the executing queue, or the executing queue is full, that is, it has reached the specified number of parallel backups as defined in the Backup Server command line, the request remains in the waiting queue.

If the executing queue is not full, the request is transferred from the waiting queue to the executing queue and a backup is initiated for each request that is transferred. When the backup finishes, the request is deleted from the executing queue, and the next waiting request is transferred to the executing queue and its backup started.

Specifying the Passport devices to back up

You need to specify the Passport devices to be backed up and synchronized with the database. You specify the Passports whose journal and/or view files you wish to backup in the DataSync.cfg configuration file on the Backup Server workstation. This configuration file is stored in /opt/MagellanNMS/cfg/.

This configuration file is shared with the Data Synchronization Server. The Backup Server interface with the Data Synchronization Server is achieved through the Data Synchronization Configuration file. The Data Synchronization Server initiates connection with the Backup Server using a host and port specified in the Data Synchronization configuration file /opt/MagellanNMS/cfg/DataSync.cfg. See “Configuring backup information for an alarm driven backup” (page 46).

Journal handling

The journal log files are stored in the subdirectory of the view they are associated with, that is, the committed view on the Passport device. If a new set of journal log files is created for the same view, another journal directory is created. The naming convention for the journal directories is

<timestamp>journal. The timestamp comes from the Passport file system and represents the creation date of the file:
/provisioning/journal/current/journalView

This file is created with the first journal log file.

A typical backup site has the following structure:
/opt/MagellanNMS/data/Backup_Data/PASSPORT/NODE_10

The journal and log file under this directory would appear as follows:

...NODE_10.20020214115144.view1.full.001/view

.../NODE_10/20020214115144.view1.full.001/ascii
.../NODE_10/20020214115144.view1.full.001/view1.full.001.INFO
.../NODE_10/20020214115144.view1.full.001/20020214153132journal/journalView
.../NODE_10/20020214115144.view1.full.001/20020214153132journal/scsInfo.1
.../NODE_10/20020214115144.view1.full.001/20020214153132journal/log.1
.../NODE_10/20020214115144.view1.full.001/20020214153132journal/log.2
.../NODE_10/20020214115144.view1.full.001/20020214153132journal/log.3
.../NODE_10/avl.INFO
.../NODE_10/recovery.INFO

One of the files created by the Backup Server is the view.INFO file.

view.INFO file

Whenever a delta view is backed up or restored, the associated base view is also backed up and restored. The base view is a portable, or complete, view. To associate the proper base view to a delta view, the view.INFO file is created on the Backup site for each view. The format of the view.INFO file is as follows:

BASE_NAME <timestamp>.<viewname>

Example:
BASE_NAME 20030126181228.view1.full.001

The view.INFO file is located on the backup site with the view. For example, for a view named view1.full.001 on a Passport NODE1:

/opt/MagellanNMS/data/Backup_Data/PASSPORT/NODE1/
20030126181228.view1.full.001/view.INFO

For each backup and restore, the tool checks if the base view is on the Backup site. If not, it will back up or restore it.

Chapter 4
Database population and synchronization

This section describes how to use the Data Synchronization Administration tool for Passport devices and provides an overview of how the database is synchronized with the Passport network and how data is loaded into the database.

The Data Synchronization Administration tool is used to administer data synchronization for Passport devices. It allows you to view the contents of the administration database, the backup repository and the device.

This section contains the following:

Overview of the synchronization process

This section contains the following information:

Synchronizing the database with the current view on the Passports

Keeping the database up-to-date (synchronized) with the current view on the Passports in the network is the role of the Data Synchronization Server. It controls the synchronization cycle by providing the logic and control to determine the sequence and direction of the synchronization process.

You can deploy multiple Data Synchronization Servers on different workstations for load balancing. Load Balancing of devices is controlled through the Data Synchronization configuration file, /opt/MagellanNMS/cfg/DataSync.cfg, which is shared by the Backup Server and the Data Synchronization Server.

You can also configure identical Data Synchronization Servers on another workstation to act as a "cold stand-by". You can then turn the stand-by on if the main Data Synchronization Server fails to come back up after a failure.

Synchronization cycle

The following sequence of events ensures that the database is up-to-date with the current view of the Passports. This sequence of events applies to both On Demand (scheduled) and On Alarm (near-real-time synchronization), since the Data Synchronization Server does not distinguish between them.

- The Backup Server sends a notification request for a Passport view or journal to all the Data Synchronization Servers that are running. The Backup Server has already stored the view and journal log files in the view storage. Only those Data Synchronization Servers, specified in the device information file, will pick up the request for synchronization.
- The Data Synchronization Server is notified either by the initial synchronization, in the initial synchronization process, or by the Backup Server. In either case, the Data Synchronization Server is notified of view changes and is provided with the following information which is stored in the recovery.INFO file by the Backup Server
  - committedFileName:<timestamp>.<viewname>
  - currentViewFileName: None | <viewName>
  - journalDirectory: <timestamp>.journal
  - journalNumber: <number>
  - journalStatus: Enabled
  - restorePossible: True | False
  - activationTime: <timeStamp>

  The activation time in the case of journals is the confirm time of the last journal. For non-journaling, it is the time when the Backup Server backs up the Passport device.

The Data Synchronization Server compares this information with the contents of the database to determine if there is a need for the views and/or journals to be updated, in other words, determines if there is a need for synchronization. If synchronization is required, it initiates the reformatting, filtering and aggregation of the data.

Initial synchronization

If the Backup Server is running when you start the Data Synchronization Server, initial synchronization for configuration data involves the following events:

- walks of all the devices in the Backup Server's view storage location
- generation of synchronization requests for the devices identified to be synchronized in the Backup Server configuration file
- putting the synchronization requests on the Data Synchronization Server's main queue.

The standard sequence of events continues from this point.

Managing simultaneous synchronizations of different Passports

The Data Synchronization Server supports parallel loading of different Passports. To support simultaneous synchronizations of different Passports, the Data Synchronization Server manages synchronization through the First In First Out (FIFO) principle. To prevent conflicts between synchronizations, only one sync session is allowed to perform synchronization on a device, and a sync session can only process one synchronization at a time.

The Sync Session uses the following strategies:

- It checks the database to see if it has the current view and journals before proceeding with synchronization.
- If multiple activates (journals) are waiting, they are compressed into a single sync session.
- If an activate (journal) is followed by a commit, it compresses all outstanding journals, loads them, and then checks activation tags to verify the loading if the committed view is required. The activate tag allows the DBSyncController to determine if the committed view is the same as the previous committed view plus all the journals since the last commit. the activate is out of date and is not updated.
- If there are multiple views waiting to be loaded, it loads only the latest (current) view.

Loading information into the database

The DBLoader loads Administration data into the database.

The Administration Database contains a single view of the most current state of selected network components. In addition, a history of journal data is maintained in the database and is mapped to backup data in the MDM backup repository.

Loading administration data into the Administration Database

The Administration Database maintains a current view of the network. The following sections describe the various scenarios for loading view data into the Administration Database.

- "Loading a view file" (page 83)
- "Loading a journal file" (page 84)

For details on the Administration data that is collected and loaded into the Administration Database, refer to 241-6001-405 *Preside MDM Administration Database Schema*.

Loading a view file

After the DBSyncController provides the Database Loader (DBLoader) with the device name, view name, and the time when the view was activated, the Administration Database Loader (AdminDBLoader) performs the following sequence of events:

- adds a record for this device to the DEVICE table, if one does not already exist
- merges the records for the subcomponent types into the Administration Database tables. For more information on Database schema, refer to 241-6001-405 *Preside MDM Administration Database Schema.*

The merging of these records is accomplished as follows:

- For every component in the view, if a record does not already exist for the component on this device, then it is added. The synchronization-timestamp is the approximate activation time of the view. The synchronization -status is "added" and is identified by an "A" in the database.
- For every component in the view, if a record already exists for the component on this device **and** its synchronization-timestamp is **not greater** than the activation time of the view, then it is replaced. The synchronization-timestamp is the activation time of the view. In this case,

however, the synchronization-status attribute is “updated” and is identified by a “U” in the database, only if the attributes of the subcomponent have actually changed. If the only change is to update the synchronization-timestamp, the record is not marked “updated”.

- After the view file has been processed completely, every component of the device in the database which was not found in the loaded view is deleted from the database. These records are identified by the device name and a synchronization-timestamp which is strictly less than the activation time of the view. This criterion excludes records with **greater** timestamps from being deleted.

  Note: The convention of not updating or deleting records which already have a timestamp greater than the activation time of the view is an important means of preventing the loading of an older view than what is current. Such a situation could occur in networks which do not use journaling. The service provisioning tools may update the database with newer information than is available to the loader at the time that it loads a view, especially when these service provisioning tools do not save the current view.

Loading a journal file

Journals are a more efficient way to load the Database changes because only the changes are loaded.

As with view files, the AdminDBLoader processes journal files one record at a time to merge the journal records into the same tables. The merging is accomplished as follows:

- For every record representing the addition of a new component a search is made to determine if the record already exists in the database. If it does not exist, or if it has a timestamp older than the activation time of the journal, then it is replaced (or added) as necessary with the status of “added”.
- For every record representing the update of a component a search is made to determine if the record already exists in the database. If it does not, then the loader assumes that it has already been deleted by a service provisioning tool and skips it. This is because the DBSyncController ensures that the views and journals augmenting them are loaded in sequence and completely. Therefore, the only reason that a record cannot

already exist in the database is because it has been deleted by a service provisioning tool. Otherwise, the database record is updated as in the case of view loading (if the timestamp is not already greater).

- For every journal record representing the deletion of a component, the corresponding database record is deleted from the database if it exists.

Administration data synchronization for discovery

Discovery is a process that searches for components in the Administration Database that are not part of a circuit. It determines which circuit the component belongs to. This process is automatic unless it has been disabled.

The following process describes the synchronization function which follows the loading of the Administration Database. This process is intended to assist the discovery process, described in "Circuit discovery" (page 109) and "VPN Discovery" (page 119):

- Any record inserted into the Administration Database by the AdminDBLoader has a synchronization-status of "added", which can direct a later Circuit Discovery or VPN Discovery invocation to potential sites for discovery of new circuits or VPNs
- Whenever Circuit Discovery or VPN Discovery is performed, either requested by the user or automatically, all components of any discovered circuits or VPNs will have their synchronization-status attributes set to "normal" (a discovery-status of "N"), indicating that the component agrees with it associated circuit or VPN. If subsequent loading from the network should change these components again, then the "updated" status values are indications of a possible need for re-discovery.

Specifying the location of the Data Synchronization Server

It is necessary to specify the location of the Data Synchronization Server for the Data Synchronization Administration tool.

Procedure steps

1. Open the file /opt/MagellanNMS/cfg/dataSyncAdmin.cfg.
2. Locate the command line that contains

   `jmx.server.host: localhost`

   Note: The default value for this attribute is localhost.

3 Change the value of localhost to the location of the Data Synchronization Server. For example

```
jmx.server.host: wcars123
```

4 Save then close the file.

Launching the Data Synchronization Administration tool

The Data Synchronization Administration tool is used to administer data synchronization for Passport devices. It can be launched from the unix command line or from the MDM window. Use the following procedure to launch the tool:

Procedure steps

1 From the unix command line, type the following:

```
/opt/MagellanNMS/bin/dataSyncAdmin &
```

OR

in the MDM window, select System->Administration->Data Synchronization Administration.

Searching for devices

Use the following procedure to search for devices to determine their synchronization status. The devices that are found are listed in the Database Results section of the Data Synchronization Administration tool.

Procedure steps

1 Open the Data Synchronization Administration tool. For more information, refer to “Launching the Data Synchronization Administration tool” (page 86).

2 In the **Device(s) Search Criteria** section, enter a specific device name or a wild card string in the **Device** field.

If you leave this field blank, it is equivalent to a * wildcard value.

3 Enter a specific view name or wild card string into the **View** field.

If you leave this field blank, it is equivalent to a * wildcard value.

4 In the **From** and **To** fields, enter start and end dates for this search

To find all the devices that have not been synchronized since a specific date, enter a date in the **To** field only.

5 If you wish to search only for devices within the responsibility of a specific Database Synchronization Controller, check the **DB Sync** checkbox and select a Data Sync Server from the drop-down list.

OR

If you wish to search the entire database, clear the **DB Sync** checkbox.

6 Click **Search**.

7 In the **Database Results** section, click the **Database** tab to display a list of devices that match the criteria you entered

The information displayed in this section can be used to determine if a device is synchronized with the network. For information on automating this process, refer to “Performing a synchronization scan” (page 87).

Performing a synchronization scan

Use this procedure to automate the search for devices which are out of synchronization with the network.

Procedure steps

1 Open the Data Synchronization Administration tool. For more information, refer to “Launching the Data Synchronization Administration tool” (page 86).

2 Perform a search for devices. For more information, refer to “Searching for devices” (page 86).

3 In the **Database Results** section, select the **Diagnostics** tab.

4 Click **Refresh All** to refresh all the devices

OR

Select one device and click **Refresh** to refresh a single device.

The progress of this scan displays. The dialog closes automatically when the scan is complete. If you wish to cancel the scan, press **Cancel**.

Devices that are in synchronization, with the database, display with a blue check. Unsynchronized devices display with a red X. If the synchronization status of a device is unknown a dash (-) is displayed next to the device. For a description of the displayed information, refer to “Database Results” (page 92).

Viewing the synchronization status of a device

Use the following procedure to view the synchronization status of a specific device.

Procedure steps

1. Open the Data Synchronization Administration tool. For more information, refer to "Launching the Data Synchronization Administration tool" (page 86).
2. Perform a search for devices. For more information, refer to "Searching for devices" (page 86).
3. In the **Database Results** section, select the **Diagnostics** tab.
4. Select a single device from the devices list.

   If no devices are listed, perform a search using the procedure "Searching for devices" (page 86).
5. Click **Refresh All** to refresh all the devices

   OR

   Select one device and click **Refresh** to refresh a single device.

   A summary displays the views and journals on this device, the backup repository and the database. For a description of the displayed information, refer to "Synchronization Details" (page 94).

Viewing the synchronization history of a device

Use the following procedure to view the synchronization history of a device.

1. Open the Data Synchronization Administration tool. For more information, refer to "Launching the Data Synchronization Administration tool" (page 86).
2. Perform a search for devices. For more information, refer to "Searching for devices" (page 86).
3. In the **Database Results** section, select the **Database** tab.
4. Select a single device from the devices list.

   The load failure or success reason is displayed at the bottom of the screen.
5. In the **Synchronization Details** section, select the **History** tab.

The synchronization history of this device is displayed. For a description of the displayed information, refer to “Synchronization Details” (page 94).

Forcing a data synchronization for a device

Use the following procedure to force a full synchronization for a specific device.

1. Open the Data Synchronization Administration tool. For more information, refer to “Launching the Data Synchronization Administration tool” (page 86).
2. Perform a search for devices. For more information, refer to “Searching for devices” (page 86).
3. In the **Database Results** section, select the **Database** tab.
4. Select a single device from the devices list.
5. Verify that the **Summary** tab is selected.

   The Summary tab displays all the device information and allows you to see which part of the data synchronization path is out of synchronization with the database.
6. Click **Synchronize**.

   A confirmation dialog indicates that this will backup all the devices in this device’s group. Note that the Synchronize button is only enabled for devices that can be synchronized by the Data Sync Controller and Backup server local to the Data Sync Server. If the device cannot be synchronized by the Data Sync Controller connected, the user must reconnect the Data Synchronization Administration tool to the appropriate server.
7. Click **OK** to continue or **Cancel** to cancel the synchronization.

   Note: During the synchronization, no information is displayed to indicate that synchronization is occurring. You must click **Refresh** to update the screen with the ongoing changes. In addition, in order to determine what files are being updated, you must access the journalbackup.log file.

Supporting information about using the Data Synchronization Administration tool

The Data Synchronization Administration tool allows you to view the contents of the administration database, the backup repository and the device. Based on this information, you can:

- determine if the information for a device is up to date in the database
- determine if the database is out of synchronization with the backup system or the device

Data Synchronization Administration window

The Data Synchronization Administration window consists of the following components”

- “Menu bar” (page 90)
- “Main window” (page 91)

Menu bar

The menu bar is located at the top of the main window. See the following sections for information on the menu bar entries:

- “File menu” (page 90)
- “Tools menu” (page 90)
- “Help menu” (page 91)

File menu

The File menu contains the following item:

- *Reconnect* allows you to reconnect with the database
- *Exit* exits the Data Synchronization Administration tool.

Tools menu

The File menu contains the following item:

- *MDM Data Administration* launches the MDM Database Administration tool.

Help menu

The Help menu contains the following commands:

- *Help On Context* displays online information about objects in the window.
- *Help On Window* accesses the online help information for the Data Synchronization window.

Main window

Three sections display the following information:

- "Device(s) Search Criteria" (page 91)
- "Database Results" (page 92)
- "Synchronization Details" (page 94)

The main window contains the following command buttons:

- *Search* performs a search of the database using the specified criteria
- *Reset* removes the search criteria from the Device(s) Search criteria section
- *Refresh* displays new information for the selected device
- *Refresh All* displays a new set of devices that match the updated retrieval criteria
- *Synchronize* initiates a backup/restore or recover on all the devices in the list

Device(s) Search Criteria

The Device(s) Search Criteria in the main window allows you to specify search criteria for devices by entering values in the following fields:

- *Device:* specific device name or wildcard
- *DB Sync*: checkbox allows you to search for specific devices. If the checkbox is checked, you can specify a device within the responsibility of a specific Data Synchronization Controller using the drop-down list. If the checkbox is clear, the search is performed for all devices in the network.
- *View*: specific view name or wildcard

- *From* and *To* specify the start and end dates for this search.
- *Device selection drop-down list* lists the devices connected to the database

Database Results

The Database Results section uses two tabs in the main window to display the list of devices found using the specified search criteria.

The following information is displayed for each device in the **Database** tab:

- *Device:* the name of the device
- *View*: the name of the last loaded view for the device
- *Journal*: the last loaded journal number. If this is empty the last load was for the displayed view.
- *Time:* used for the view file when no journal number is indicated or used for the journal number. The timestamp indicates when the view or journal was first activated on the device. Note that, in the case of configuration rollbacks or disaster recover, these timestamps may not indicate when the view or journal was last activated.
- *Act Time* (Activation time): used for the view file when no journal number is indicated or used for the journal number. The timestamp indicates when the view or journal was backed up from the device (when the view or journal was seen as active on the device).

The following information is displayed for each device in the **Diagnostics** tab:

- *Device:* the name of the device
- *State*: is an indicator of the synchronization state of the device. The field displays an icon of a checkmark, ‘x’, ‘-’, ‘?’ or ‘.’. A checkmark indicates that the Database is in synchronization with the device and no load or discovery failures have occurred. An ‘x’ indicates that an error has occurred while processing the view or journal in either the loading or discovery steps. You should view the other status columns for details. A ‘-’ indicates that the Database is out of synchronization with the device. You should view the description in the summary table. A ‘?’ indicates that not enough information is available to determine the synchronization status. This may mean that the workstation on which the

Data Synchronization Server is running is unable to access the device. A '.' means that the information needed to determine the synchronization status of the device has not been retrieved and a detailed status determination has not been computed. You can retrieve all the necessary information for a device by selecting the device in the table or pressing the **Refresh All** button. Note that **Refresh All** performs a sequential retrieval for all devices in the table and can take several seconds per device.

- *Synch Status*: indicates if the devices and database are synchronized with the same view and journal files. The field displays values of 'synchronized', 'out of sync' or 'not available'. 'Synchronized' indicates that the Database is in synchronization with the device. 'Out of sync' indicates that the Database is out of synchronization with the device and that you should view the description in the summary table. 'not available' indicates that not enough information is available to determine the synchronization state. This may mean that the workstation on which the Data Synchronization Server is running is unable to access the device.
- *Load Status*: the status of the database synchronization process for the device.This process loads the view and journal information into the database. The field displays values of 'loaded', 'loading' or 'failed'. 'Loaded indicates that the view or journal shown in the database table has loaded successfully. 'Loading' indicates that a new view is being loaded into the database. 'Failed' indicates that the last view or journal, that attempted to be loaded, encountered problems. The view or journal that is being loaded or that has failed is displayed in the last entry of the history table.
- *Discovery Status*: the status of the automatic discovery process for the last loaded view or journal. Possible values for this field are 'success', failed' or 'not_discovered'. If 'failed' is displayed, the reason is listed in the /opt/MagellandNMS/data/dbsync/admindb.log file. A value of 'not_discovered' indicates that automatic discovery has not been enabled for this device.

  Note: The discovery status indicates the status of the discovery process that was last completed for the device. Therefore, the status may be momentarily out of sync for a view that has just completed loading but for which the discovery process hasn't completed.

The reason the device and database are not synchronized is displayed at the bottom of the pane. The reason describes the synchronization state.

Synchronization Details

The Synchronization Details section uses two tabs in the main window to display the list of devices found using the specified search criteria.

The following information is displayed in the **Summary** tab and allows the user to see which part of the data synchronization path is out of synchronization:

- *Database:* the contents of the Administration Database
- *Backup Site:* the last view or journal backed up at the backup site. This is also recorded in the backup site directory in the recover.INFO file for the device at /opt/MagellanNMS/data/Backup_Data/PASSPORT/<device_name>.
- *Device:* the current view and journals that are active on the device. This information is retrieved from the device when you:
  - — initially select it in the database or diagnostic tables
  - — press the **Refresh All** button
  - — press the **Refresh** button for this device

  Note that the retrieval of information may take a few seconds.
- *Source:* the source of information
- *View*: the name of the last loaded view for the device
- *Journal*: the last loaded journal number. If this is empty the last load was for the displayed view.
- *Time:* used for the view file when no journal number is indicated or used for the journal number. The timestamp indicates when the view or journal was first activated on the device. Note that, in the case of configuration rollbacks or disaster recover, these timestamps may not indicate when the view or journal was last activated.

The following information is displayed for each device in the **History** tab:

- *View*: the name of the committed view for the journal. If no journal is provided, this is when the committed view was loaded.
- *Journal*: the name of the journal loaded into the database
- *Time*: the time when the view or journal was loaded into the database
- *Tag*: the activation tag associated with the journal
- *Act Time* (Activation time): used for the view file when no journal number is indicated or used for the journal number. The timestamp indicates when the view or journal was backed up from the device (when the view or journal was seen as active on the device).
- *DB Sync*: the Database Synchronization server that moved the load into the database

The reason for synchronization failure is displayed below this pane.

Chapter 5
Post-installation procedures

This section describes post-installation procedures. This section contains the following topics.

Note: In addition to these procedures, you must add the new Passports to be backed up as well as add any new backup groups. For more information, refer to 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

Synchronization through a scheduled cron job

Use this procedure to set up a scheduled Current Configuration backup.

Prerequisites

You have configured a cron job using the Backup tool executable /opt/MagellanNMS/bin/nsbck with the -demand option. See 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

You must be logged in as root to perform this procedure.

Procedure steps

1. Start the Passport Server Administration application.

   For more information, refer to 241-6001-303 *Preside MDM Administrator Guide*.

2. In the Server list, select **Backup Controller**.

3. Right click to select **Edit Configuration** -> **Backup Server**.

   The **Configuration Editor** displays.

4. Expand the Passport device for which you wish to schedule cron job.

5. Select DBSynchOptions and set the value of the **enabled** field to **True**.

6. In the DBSynchOptions element, verify that the value in the **server** field matches the name field specified in the /opt/MagellanNMS/cfg/DataSync.cfg of the responsible DBSync. This field is used to partition multiple Data Sync servers. If the names do not match, the Data Sync servers will not synchronize that device.

7. The /opt/MagellanNMS/bin/nsbck -demand <group> command option triggers an on-demand backup of all the devices specified in the DataSync.cfg file with the same group label. To execute a backup of all the Passports in the DataSync cfg file at the same, execute the following command (without the group option):

   `/opt/MagellanNMS/bin/nsbck -demand`

8. The cron job can be set up using the UNIX cron utility. The cron utility is a process that schedules and performs tasks at a set time and day. It uses a crontab file to determine the time interval and the commands to execute.

   From the xterm window, type the following command:

   `crontab -e`

An empty vi file is displayed on the screen.

9 Specify the day and time, and the command to be executed.

The following example shows a crontab file that performs backup on all devices from Monday to Friday at midnight:

```
0 0 * * 1-5 /opt/MagellanNMS/bin/nsbck -demand
```

The following example shows a crontab file that performs backup on three different groups on Monday, Tuesday and Wednesday at midnight:

```
0 0 * * 1 /opt/MagellanNMS/bin/nsbck -demand group1
0 0 * * 2 /opt/MagellanNMS/bin/nsbck - demand group2
0 0 * * 3 /opt/MagellanNMS/bin/nsbck - demand group3
```

Database management reports

Database management reports consists of a selection of SQL reports that assist the database administrator in tracking the activity and growth of the Administration Database. These reports are implemented as Oracle SQL *Plus scripts in the /opt/MagellanNMS/lib/sql/reports directory.

Running view/journal loads

The view/journal loads performed or started by the Data Synchronization Server on a specific day are listed in the dbsync_activity.sql report.

The report consists of three sections which list view names and journal numbers loaded, grouped by device name, and consisting of the activation timestamp and load timestamp of the load activity. The first section lists any failed loads, and includes the error messages outlining the reason for the failure. The second section lists the loads that were successfully completed. The third section lists the view/journal information for devices, which is currently being loaded by the Data Synchronization Server.

Run the report nightly as a cron job, with the results delivered by email. A sample crontab entry (as a single command line) is as follows:

```
/oracle/product/8.1.7/bin/sqlplus -S\
  scott/tiger@mdm @/opt/MagellanNMS/lib/sql/reports/
dbsync_activity.sql\ 25-Oct-2002
```

See the procedure, “Reporting on view/journal loads” (page 103).

Verifying view/journal loads

The node_status.sql report lists the most recent view/journal successfully loaded for each Passport device. Devices with later load failures are listed separately to indicate that these devices may be partially updated and different from the last loaded view/journal.

The report is separated into two sections which list view names and journal numbers loaded, consisting of the activation timestamp and load timestamp of the load activity. The first section of the report lists any failed loads following the last successful load for each device, and includes the error messages indicating the reason for the failure. The second section lists the most recent successful load for every device.

Run the report nightly as a cron job, with the results delivered by email. A sample crontab entry (as a single command line) might be as follows:

```
/oracle/product/8.1.7/bin/sqlplus -S
  scott/tiger@mdm @/opt/MagellanNMS/lib/sql/reports/
node_status.sql
```

See the procedure, “Reporting on the current view/journal loaded for all devices” (page 104).

Stopping access to the database

Use this procedure to stop access to the database for maintenance.

Procedure steps

1. From the **Options** menu of MDM Database Administration, select **Configuration**.

   The **Configuration Options** dialog opens.

2. Disable access to the database by clicking **False**, and then click **OK**.

Reporting on view/journal loads

The view/journal loads performed or started by the Data Synchronization Server on a specific day are listed in the dbsync_activity.sql report. Run the report nightly as a cron job. This report consists of three sections that assist you in tracking the activity and growth of the Administration Database. The three sections list:

- load failures, if any, and includes the error message describing the problem
- loads that were successfully completed
- loads which were started on the specified day and are still in progress at the time the report was executed.

Procedure steps

1 Run the dbsync_activity.sql report using the variable values listed below.

```
sqlplus -S <username>/<password>@<database>
@/opt/MagellanNMS/lib/sql/reports/dbsync_activity.sql
<date>
```

2 Verify the creation of the report.

Variable definitions

Variable	Definition
<username>	is the name of the Oracle account which owns the Administration Database
<password>	is the password corresponding to the <username> account
<database>	is the Oracle SID (database name) of the Administration Database instance
<date>	The sql date is in the format DD-MMM-YYY. For example, 25-Oct-2002.

Reporting on the current view/journal loaded for all devices

The node status report displays the current status of all Passport nodes in the MDM Administration database. This report consists of two sections that list:

- all of the load failures, if any, following the most recent successful load for each node. Included on each line of the report is the node name and journal number, along with the error message.
- the most recent successful load for every device.

Use this procedure to display the current view or journal that is loaded for each device.

1 Run the node_status.sql report using the variable values listed below.

```
sqlplus -S <username>/<password>@<database>
@/opt/MagellanNMS/lib/sql/reports/node_status.sql
```

2 Verify the creation of the report.

Variable definitions

Variable	Definition
<username>	is the name of the Oracle account which owns the Administration Database
<password>	is the password corresponding to the <username> account
<database>	is the Oracle SID (database name) of the Administration Database instance

Chapter 6
Circuit management

This section provides an overview of the Nortel Networks Preside Multiservice Data Manager (MDM) circuit management application for managing virtual circuits. This section includes the following topics:

Circuit management

The Preside Multiservice Data Manager (MDM) circuit management application is a set of software tools that let you provision and manage service-level components within a Passport network. Circuit management links network components that make up a circuit treating the circuit as a unified network management object rather than a collection of unrelated components.

Circuit management provides improved management functions for virtual circuits and better visibility of services. You can identify end-to-end circuits and associate circuits with customer information. You can also view diagnostic information for the components across a circuit, including state and statistical data. In addition, it provides validation of circuits for all

changed components. This validation is performed independent of the autoDiscovery on/off settings and validates circuits for all changed components, regardless of how the circuit was created.

Circuit management capabilities

Circuit management supports the following functions:

- provisioning of ATM, Frame Relay and IP VPN Access circuits in the network and storage, in the Administration Database, of provisioned circuit data and off-switch data (for example, customer associations)
- automatic discovery and storage, in the Administration Database, of ATM, Frame Relay and IP VPN Access circuits.
- retrieval and display of circuit data from the Administration Database. In addition, it supports the display of real-time circuit component information retrieved from the network (in particular, component state and statistics).

Supported Passport services

Circuit Management provides facilities to:

- create ATM, FRATM and Frame Relay circuits in the network and stores the circuit information in the Administration Database using the service provisioning tools
- retrieve ATM/FRATM/FR circuit discovery processes and stores the circuit information in the Administration Database

ATM PVC, PVP, SPVC, SPVP, FRATM FRF 8 Access, Frame Relay and IP VPN services are supported by the MDM service provisioning tools.

Circuit management supports the following services:

- ATM
  - PVC and PVP, excluding virtual path terminators and point-to-multipoint
  - SPVP and SPVC, including storage in the database of adminContol, aisGeneration, and MDTL attributes
  - trunk over ATM PVC

- Frame Relay PVC
- Frame Relay IP VPN Access
  - Backhaul Access (2764)
  - Direct Access (2764)
  - IP Optimized Direct (2764)
  - IP Optimized Direct (2547)
  - IP Optimized Backhaul (2764 and 2547)
- FRATM FRF.8 Access, for both SPVC and NPVC

Circuit management components

The circuit management application consists of a collection of software tools that work in conjunction to provide circuit management functionality. This software includes the following items:

- "Administration Database" (page 107)
- "MDM Database Administration tool" (page 108)
- "Circuit Viewer tool" (page 108)
- "ATM service provisioning tool" (page 108)
- "Frame Relay service provisioning tool" (page 108)

Administration Database

The Administration Database stores both off-switch and on-switch data. Off-switch data includes circuit definitions, customers, and traffic management profile names. The off-switch data is managed by the MDM Database Administration tool.

On-switch (switch-mastered) data includes circuit components such as devices, interfaces, facilities (ports), and connection components as well as any attributes that are relevant to circuit management. On-switch data is stored in the database by a service provisioning tool when you define a circuit, or by the Data Synchronization Server when you activate a new view on the switch.

MDM Database Administration tool

The MDM Database Administration tool is the primary tool for ensuring that on-switch data is synchronized with network data and for managing off-switch data. You can view the status of circuits. You can also discover circuits that have been provisioned by tools other than service provisioning, provided there is sufficient information for discovery.

For more information about the MDM Database Administration tool, see "MDM Database Administration tool" (page 127) and "MDM Database Administration procedures" (page 151).

Circuit Viewer tool

The Circuit Viewer tool lets you retrieve a circuit from the Administration Database and view all related information for that circuit. Using this tool, you can retrieve and view information about a selected circuit. You can view details about a specific circuit including related customer and circuit component information. The Circuit Viewer tool also supports ATM, Frame Relay and IP VPN Access service diagnostic capabilities. For more information about the Circuit Viewer tool, see the Circuit Viewer section in 241-6001-011 *Preside MDM Fault Management User Guide*.

ATM service provisioning tool

The ATM service provisioning tool provides a graphical user interface for provisioning tasks. When you activate the provisioned information, the tool automatically updates the Administration Database. For more information about ATM service provisioning, see 241-6001-600 *Preside MDM Service Provisioning for ATM User Guide*

Frame Relay service provisioning tool

The Frame Relay service provisioning tool provides a graphical user interface for provisioning tasks. When you activate the provisioned information, the tool automatically updates the Administration Database. For more information about Frame Relay service provisioning, see 241-6001-603 *Preside MDM Service Provisioning for Frame Relay User Guide*

Circuit discovery

When you provision a circuit using the MDM service provisioning tools, these tools automatically build circuits and store that information in the Administration Database. However, if you provision circuits by tools other than service provisioning, these other tools do not automatically build circuits in the Administration Database. In these cases, circuits are built by the circuit discovery process after the database has been updated with new Passport configuration data (via the Database synchronization process). Circuit discovery is a process that searches for components in the Administration Database that are not part of any circuit and determines the circuit to which they belong. Circuit discovery can make this determination provided sufficient information was initially provisioned for the circuit components. The circuit discovery process is automatic unless it is has been disabled.

For more details about circuit discovery, see the following topics:

- "Manual and automatic discovery" (page 109)
- "Prerequisites for initial circuit discovery" (page 112)
- "Changing the autodiscovery parameters for circuits" (page 112)
- "Validation" (page 113)

Manual and automatic discovery

The following methods of circuit discovery are supported:

- "Automatic discovery" (page 109)
- "Manual discovery" (page 111)

For more information on default discovery settings, refer to "Default circuit discovery settings in DataSync.cfg file" (page 111).

Automatic discovery

Automatic discovery automates the discovery of new circuits for newly added components or modified components in the MDM Administration Database. It also automates the discovery of deleted circuits that are no longer present in the network. This process can associate components with an existing circuit or create new circuits.

The successful load of a view or journal file into the Administration Database triggers automatic discovery for new components for which automatic discovery has been enabled.

When the automatic discovery process creates a new circuit, it associates the default customer with the new circuit.

The Data Synchronization configuration file (DataSync.cfg) specifies which type of circuits should be automatically discovered. It contains an entry for each service type (ATM, FR, IP_VPN_ACCESS). The following parameters are set for each entry:

- autoDiscovery: If this is set to "true", auto-discovery is enabled for this service type. If it is set to "false", auto-discovery is not enabled.
- filterOnCorrelationTag: If this is set to "true", only connection components that have a provisioned correlation tag are starting points for discovery. These correlation tags are used as the circuit ID. If this is set to "false", then any connection component can be used as a starting point for discovery. Note that if a starting component has a correlation tag, it is used as the circuit ID for ATM and Frame Relay circuits, otherwise a circuit ID is generated.
- atmPvcMethod: This parameter specifies the discovery or validation method to be used for the ATM PVC circuits. It's value can be
  - remoteInterfaceLabel: The AtmIF relationships, determined from the remoteAtmInterfaceLabel attribute are used to discover and validate ATM PVC circuits. **Note: If you select the removeInterfaceLabel method of discovery, the circuit path will be discovered. As a result, in the Circuit Viewer, the circuit components are listed in the order in which they occur in the circuit path and a graphical view of the circuit path is available. This is an optional attribute that is not checked for correctness. Therefore, when you provision the remoteInterfaceLabel attribute, you must verify that the value refers to the right AtmIf and that it has the correct format (EM/<node name> AtmIf/ <atmif id>).**
  - correlationTag: Provisioned correlation tags are used to discover and validate ATM PVC circuits. **Note: If you select the correlationTag method of discovery, only the components that make up the**

circuit will be discovered; the circuit path is not discovered. As a result, in the Circuit Viewer, the circuit components will be listed in random order and a graphical view of the circuit path is not available.

Note: Choose and maintain one discovery method for ATM PVC circuits. RemoteInterfaceLabel and correlationTag discovery methods are very different. Therefore, you may have unexpected behavior if you switch methods.

To change the autodiscovery parameter values, refer to "Changing the autodiscovery parameters for circuits" (page 112).

Manual discovery

You can use the Circuit Discovery feature of the Database Administration tool to manually discover circuits that were not created using a Service Provisioning tool or not discovered automatically. This tool allows you to select a component as a starting point for the discovery, and specify a Circuit ID and an associated customer for the discovered circuit.

For ATM PVC circuits, two manual discovery methods are supported which correspond to the two methods for automatic discovery:

- correlation tag: uses provisioned correlationTag attributes to determine the components making up a circuit
- path data: uses provisioned AtmIf remoteInterfaceLabel attributes to determine the circuit path. The path data method is not supported for SPVC circuits as address matching is not supported. If this method is chosen for an SPVC Vcc component, a circuit will be created containing only that component.

For the other supported circuit types (Frame Relay and IP VPN Access), only the path data method is supported because, for these circuit types, there is sufficient provisioned information to determine the circuit path.

Default circuit discovery settings in DataSync.cfg file

The following table lists the default settings for each service type.

Service	ATM	FR	IPVPN Access
ServiceDiscovery type	ATM	FR	IP_VPN_Access
autoDiscovery	true	true	true
filterOnCorrelationTag	false	false	false
atmPVCMethod	correlationTag	n/a	n/a

Prerequisites for initial circuit discovery

The following prerequisites must be satisfied in order that circuit discovery occurs:

- Data Sync Server must be configured. For more information, refer to "Configuring the Database Synchronization Controller file" (page 206).
- Backup Server must be running correctly. For more information, refer to "Configuring backup information for an alarm driven backup" (page 46).
- The Data Sync Server must be synchronized correctly.
- The DB Loader must load the data correctly.
- The Discovery Engine needs to trigger circuit discovery according to the autodiscovery flags specified in the DataSync.cfg file.

Changing the autodiscovery parameters for circuits

The ATM, Frame Relay and IP VPN Access circuits are set to be automatically discovered. If you wish to change which circuits are autodiscovered and stored in the database, use the following procedure.

Procedure steps

1. Start the Server Administration application and complete the required authorization.

   For more information, refer to 241-6001-303 *Preside MDM Administrator Guide*.

2. In the list of servers, select **Data Sync Server**.
3. Right click to select **Edit Configuration**->**DBSync Controller**.

   The **Configuration Editor** opens.

4. Expand the **Auto Discovery** selection.
5. Select the service type for which you wish to change the autodiscovery.

6 Set the **Auto Discovery** field to true or false depending on your requirements.

7 Change any other fields if required.

8 Click **Apply**.

9 Select **Save** from the **File** menu.

10 Verify that no loading activity is taking place.

Use the tail -f option in the admindb.log file and the dsync.log file (in /opt/MagellanNMS/data/dbsync)

11 In the list of servers, in the Server Administration tool, select **Data Sync Server**.

12 Right click to select **Stop**.

13 Right click to select **Start**.

Note: Do not stop or start the Data Synchronization server in the middle of the database loading process.

14 Verify that the DBLoader has completed loading the data into the MDM Database using the Data Synchronization Administration tool.

If autodiscovery is on with the defined service, the change is successful.

Validation

When the database loader detects that a component has changed in a way that could affect the validity of the circuit to which it belongs, the circuit is automatically validated. The validation occurs regardless of the automatic discovery configuration settings. The validation will result if one of the following occurs:

- the changed component is removed from the circuit and the circuit is left with its other components: for example, if the changed component is a Frame Relay backup slave that no longer points to the master.
- the changed component is left in the circuit and another component is removed. For example, if the changed component is the master of a Frame Relay circuit that no longer points to the slave, then the slave component is removed. In this case, the circuit status is set to "Incomplete".
- if all components have been deleted or if the circuit is deleted.

When validation results in the changed component being removed from a circuit, an attempt is made to discover the circuit to which the component now belongs.

Facility ID

The Administration Database stores the facilities associated with interface components. These are the logical LP ports or channels linked to interfaces by the interfaceName attribute provisioned on the interface or on a component. The Facility ID is provided by the provisioned commentText attribute on the port or channel. This information is loaded into the database during the synchronization process.

The Circuit Viewer and MDM Database Administration tools display the Facility IDs associated with the endpoints of circuits. You can also use Facility IDs as a search criterion with these tools. The tools will match against the Facility IDs associated with circuit endpoints.

Circuit management log files

The MDM Database Administration tool stores log messages in the /opt/MagellanNMS/data/log/CircuitManagement.log file. These log files have a maximum size of 10 megabytes (MB). When this limit is reached, the content of CircuitManagement.log is moved and stored in CircuitManagement.log.1. New log messages accumulate in CircuitManagement.log once again. When CircuitManagement.log reaches is maximum size again, the following changes occur:

- the content of CircuitManagement.log.1 moves to CircuitManagement.log.2
- the content of Circuit Management.log moves to CircuitManagement.log.1
- new log messages accumulate in CircuitManagement.log

Current log messages are always stored in CircuitManagement.log. When this file reaches its size limit, the content is moved to another file in sequence. This roll-over process continues to create additional log files up to CircuitManagement.log.9. This method allows for a maximum of ten log files—one actively accumulating new log messages and nine others

containing progressively older messages. When the maximum number of log files is reached, the roll-over process continues but the content of the oldest file, CircuitManagement.log.9, is lost.

> ***Note:*** If a log file does not roll over as expected, another application may have a process that has the log file open. A rollover will occur when no process has the log file open and the log file nears its maximum size.

Since each log file can occupy up to 10 MB of disk space, and there are up to 10 log files, storage for log files can reach 100 MB. Therefore, it is recommended that you have a file management strategy that includes archiving and deleting older log files.

The Circuit Viewer tool also writes to the circuit management log file. As well, the ATM service provisioning tool writes to the circuit management log file if the provisioning causes errors in the administration database Therefore, if you want to delete a current log file, first ensure that the log file is not being used by another application.

Chapter 7
VPN management

The MDM Administration Database (MDM Admin DB) facilitates the provisioning and management of RFC 2547 VPNs and RFC 2764 VPNS with autodiscovery enabled.

Through the discovery process, the database creates VPN entities based on switch-mastered objects by following certain VPN discovery algorithms and rules. Off-switch VPN entities are added to the database and associated with the relevant switch-mastered objects through the use of the IP VPN service provisioning and the IP VPN provider edge provisioning tools. For information about these tools, see 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*.

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

The main processes and procedures that enable the MDM Admin DB to support VPN provisioning and management are as follows:

- “Database population” (page 118)
- “VPN Discovery” (page 119)
- “Setting up the MDM Admin DB for VPN provisioning” (page 124)

Database population

Passport components are loaded from the network by the DB synchronization server to the MDM Admin DB as entities.

Other entities are created when the database schema are created.

Passport component entities supporting VPNs

The entities that support the VPN provisioning and management include:

- VRFRAMER-GATEWAY from the *VirtualFramer* subcomponent of the *FRUni, FrNni, FrAtm, and FrDte* interface components
- CORE-ROUTER from the *VirtualRouter* component instances that have the *carrier* mode attribute
- VPN-ROUTING-FUNCTION from the *VirtualRouter* component instances that have the *customer* mode attribute, including various components of the *VirtualRouter Ip* component tree in the RFC 2764 model, and the Router *VirtualRouterForwarder* component and its sub-tree in the RFC 2547 model
- IP-LOGICAL-INTERFACE from the VirtualRouter *ProtocolPort IpPortLogicalInterface* component and the Router *VirtualRouterForwarder* interface component
- PTMP-TUNNEL from the *VirtualRouter Ip Tunnel* component and its sub-components
- IP-MEDIUM from the *FrDte RemoteGroup, IpDlciGroup, AtmMpe, LanApplication, PointToPointProtocol, VirtualMedia Interface, Router VirtualRouterForwarder Loopback Interface, VirtualRouter Ip Tunnel MultipointStaticEndPoint*, and *Router Ethernet* components

Database entities supporting VPNs

Upon creation of the DB schema, the MDM Admin DB is seeded with two special customer objects. One is the Default Customer representing the default owner of discovered entities, including VPNs. The other is the Service Provider object representing the service provider that owns the network being managed by Preside MDM.

The Default Customer entity enables querying the database to find autodiscovered objects which have not yet any specific ownership assigned.

VPN Discovery

When you configure a VPN using the IP VPN service provisioning (IP VPN SP) tool, the tool automatically builds the VPNs and stores that information in the MDM Admin DB. However, if you configure a VPN using tools other than the IP VPN SP tool, these other tools do not automatically build VPNs in the MDM Admin DB. In these cases, the VPNs are built by the VPN discovery process.

The VPN discovery process searches for components in the MDM Admin DB that are not part of any VPN and determines the VPN to which they belong. The VPN discovery can make this determination provided sufficient information was initially configured for the VPN components. The VPN discovery process is automatic unless it is has been disabled.

ATTENTION	Autodiscovered and re-discovered RFC 2764 VPNs assigned to the Default Customer may have to be re-assigned to the appropriate customer. See “Associating a VPN to a customer” (page 187).

ATTENTION	The route targets of autodiscovered and re-discovered RFC 2547 VPNs that have been assigned to the Default Customer may have to be re-assigned to the appropriate customer. See 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*, *2547 VPN Configuration*, Adding Route Targets to the customer VPN.

Automatic discovery of RFC 2764 VPNs

The automatic discovery of a 2764 VPN is driven by the VPN ID provisioned on the customer VR and consists of three stages:

1. Searching for an existing VPN which has a VPN ID matching the VPN ID provisioned on the customer VR. If a match is not found, a new one is created and is assigned to the Default Customer in the database. VPN ID is a mandatory attribute for automatic discovery.
2. Associating the VR with the VPN found at stage 1.
3. Setting the VPN type indicator according to the following criteria:

a. If the VR does not have a PTMP tunnel, the VPN type indicator is set to 2764Direct.

b. If the VR has a PTMP tunnel with the *autoDiscovery* attribute set to *disabled*, the VPN type indicator is set to 2764Static.

c. If the VR has a PTMP tunnel with the autoDiscovery attribute set to enabled, the VPN type indicator is set to 2764.

ATTENTION	If the logical interfaces are mapped one-to-one with the protocol ports, access points are associated with circuits automatically. If there are multiple logical interfaces under a protocol port, in order for discovery to properly associate the discovered access points with discovered circuits, you must provision the following links on the node: • TolpLogicalInterface (under static dlcis) • TolpLogicalInterface (under FrConn)

Re-discovery of 2764 VPNs

The VPN Discovery process maintains consistency between the VPN information in the database and the VPN provisioned in the PE network. If you change the VPN ID, the VPN re-discovery will restructure the 2764 VPNs as follows:

- the VR is removed from the VPN which currently includes it
- the VR is added to the VPN matching the new VPN ID or, if no such VPN is found, a new VPN is created for the VR and assigned to the Default Customer.

Automatic discovery of RFC 2547 VPNs

The automatic discovery of a 2547 VPN is driven by the customer ownership of Route Targets and the VRF implementations of Route Targets. See 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide* for information about 2547 VPNs.

There are two stages in the automatic discovery of a 2547 VPN:

1 Grouping Route Targets according to customer ownership as follows:

a. For a VRF that uses Routes Targets that are owned only by customers (not the Service Provider or Default customers), the Route Targets it uses are grouped according to the customer ownership of those Route Targets.

b. For a VRF that uses Route Targets that are owned by customers (not the Service Provider or Default customers) and Route Targets that are owned by the service provider, the discovery process ignores those owned by the service provider and groups those owned by actual customers.

c. For a VRF that uses Route Targets that are owned only by the service provider, these Route Targets are implemented for management of the network elements and not for customer service. This allows the service providers VRFs to be managed as a VPN without including all of the PE node VRFs in that VPN.

2 Implementing the Route Targets for each customer (not the Service Provider or Default customers) by:

a. searching for an existing VPN that is associated with any of the Route Targets owned by that customer and used by the VRF, or if there is no other VPN owned by that customer, creating a new VPN for the customer.

b. associating the VRF with the customer VPN found/created at stage 2a.

c. associating all of the Route Targets used by the VRF (including those that are owned by other customers) with the VPN found/created at stage 2a.

ATTENTION	For RFC 2547 VPNs, after discovery has discovered all 2547 VPNs based on the route targets, all the discovered VPNs are assigned to the Default Customer. The IP VPN SP tool can then be used to re-assign route targets to the appropriate customer.

Re-discovery of 2547 VPNs

The VPN Discovery process maintains consistency between the VPN information in the database and the VPN provisioned in the PE network. If you change the information about the VRFs or the Route Target implementation, the VPN re-discovery will restructure the existing 2547 VPNs as follows:

- When you add a Route Target to a VRF
  - — if the new Route Target is owned by the service provider, it is ignored
  - — if the new Route Target is not owned by the service provider, it is added to all VPNs which include the VRF, or, if there are no VPNs that include the VRF, a new VPN is created and the VRF is added to it

ATTENTION	If you add a Route Target that is in one VPN, to a VRF that belongs to another VPN, the ownership of the VPNs affects the resulting VPN architecture as follows: • if both VPNs are owned by the same customer, this causes the two VPNs to merge • if the VPNs are not owned by the same customer, the VPNs are not merged but the Route Target is marked as an extranet Route Target.

- When you remove a Route Target from a VRF, the VRF is removed from the VPN only if the VRF no longer uses any Route Target owned by the customer who owns the VPN. If you remove all Route Targets from a VRF, the VRF remains in the MDM Admin DB, but it no longer belongs to any VPN.

ATTENTION	If you remove a Route Target from a VRF, this may cause a VPN to be split. This happens when the removal of a Route Target causes a group of VRFs in the VPN to not have any Route Targets in common with another group of VRFs in the same VPN. Each group of VRFs will then consist of a new VPN.

- When you change the Route Target customer ownership, the VRFs that used this Route Target are removed from the customer's VPN and are added to the new owner's VPN. If the new owner does not have an existing VPN, re-discovery creates a new VPN and the VRFs using the newly-owned Route Target are added to that VPN.

ATTENTION	Changing the Route Target ownership can cause one or more VRFs to implement extranet access.

Setting up the MDM Admin DB for VPN provisioning

Perform the following procedures to set up the MDM Admin DB for VPN provisioning:

1 After the Oracle database has been installed, disable the discovery process and load the existing network configuration into the MDM Admin DB with discovery de-activated. See "Initial database loading" (page 209) and "Disabling discovery" (page 211).

2 Enable discovery and restart Data Sync server. See "Enabling discovery" (page 211). This will assign any existing RFC 2547 VPNs and RFC 2764 VPNs with auto-discovery enabled, to the Default Customer entity in the MDM Admin DB.

3 Create the provider edge (PE) network entity using the DB Admin tool. See "Adding a Provider Edge Network" (page 182).

4 Assign core routers to the PE network entity. See "Adding core routers to a Provider Edge Network" (page 181).

5 Create the Customer entities using the DB Admin tool. See "Adding a new customer" (page 168).

6 Re-assign all VPNs that were assigned to the Default Customer to the appropriate Customer entity.

7 Re-assign all Route Targets that were assigned to the Default Customer to the appropriate Customer entity.

8 Optionally, associate each VPN access node to the appropriate customer entity. See "Associating a customer to a site" (page 178).

9 Launch the IP VPN service provisioning (IP VPN SP) tool and verify that each existing VPN appears under the appropriate customer entity. See 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*.

10 Launch the Frame Relay access provisioning tool and verify that all discovered IP access circuits can be properly retrieved.

11 For the VPN Monitor feature, the NDAM server must be started with the -F option. If there is already an NDAM server running without the -F option, start another NDAM server with the -F option and give it a different name. Start the VPN Monitor server using the command line option:

VPNMonitorServer -ndam <serviceName@host>

Chapter 8
MDM Database Administration tool

This section describes the MDM Database Administration interface and contains the following topics:

For details about MDM database administration procedures, see "MDM Database Administration procedures" (page 151).

MDM Database Administration overview

The MDM Database Administration tool provides capabilities for network operators to manage off-switch information (such as circuits and customers) and perform database maintenance activities.

For more information, refer to "Management of the Administration Database" (page 128).

Management of the Administration Database

The Administration Database contains two types of information:

- On-switch (switch-mastered)
- Off-switch (manually entered)

The on-switch, or switch-mastered data is loaded by the DataSyncController and reflects the on-switch view of the network. Switch-mastered data includes device, service interface, circuit endpoint, address, and facility information.

Off-switch information consists of data that does not correspond to components on the Passport switch. This information consists of circuit and customer data as well as PE Networks and Sites and must be entered into the database manually. In addition, there is off-switch information such as IP Access Points and VPNs that is automatically created by the discovery engine.

You use the MDM Database Administration tool to:

- query and display a subset of switch-mastered data
- query, display, and modify off-switch data

Working in a multi-user environment

Working in a multi-user environment may result in the following:

- differences between the information displayed in the MDM Database Administration tool and the database. See “Discrepancy with information displayed” (page 129).
- the unsuccessful creation of an object because another user has already created it. See “Unsuccessful creation of an object” (page 129).
- the unsuccessful modification of an object because another user may have modified it. See “Unsuccessful modification of an object” (page 129).

Discrepancy with information displayed

Each time a user clicks **Retrieve** in the **Circuit retrieval criteria** panel, a new transaction opens. When the user completes the search, the transaction closes. In a multi-user environment, the information displayed in the tool may become stale and differ from the information in the database. Clicking **Retrieve** refreshes the data.

Unsuccessful creation of an object

When a user clicks **Apply**, a new transaction opens. In a multi-user environment, another user may have already created an object that precludes the successful creation of the object in progress. If this occurs, the MDM Database Administration tool opens a dialog to alert the user. An example of this is the creation of a customer with the same name (not allowed). To ensure that the information is up-to-date, click **Retrieve** in the **Customer retrieval criteria** panel. Then proceed with creating the new object.

Unsuccessful modification of an object

An object may not be successfully modified if another user has made a modification between the time the object was first retrieved from the database, and the time when the current user of the MDM Database Administration tool makes a modification to the object. If a modification has occurred in another instance of the MDM Database Administration tool or a service provisioning tool, then a conflict may occur. If a user attempts to change an object that has already been modified, the tool will fail the change because the user has attempted to modified an object that does not have the

latest change. To correct this, click **Retrieve** in the **Customer retrieval criteria** panel to refresh the data, and then make the modifications. If the object was not modified in the interim, a conflict will not occur.

> ***Note:*** There is only one default customer, which cannot be deleted. This occurs because the because the default customer is a special type of object. There can only be one default customer but the properties of the default customer can be modified. In addition, there is a special customer, the ISP customer. The properties of the ISP customer may be modified but the role of ISP cannot be assigned to another customer

We recommend that administration actions are performed by one user rather than by all operators at a customer installation.

MDM Database Administration window

The MDM Database Administration tool lets you

- display switch-mastered data
- display and modify user-defined customer, circuit and IP VPN information

Modifications that you make via the MDM Database Administration tool are saved in the administration database only. No corresponding provisioning changes are made to the device.

The MDM Database Administration window consists of the following elements:

- "Menu bar" (page 131)
- a selection of tabbed panes
  - — "Circuits form" (page 133)
  - — "Customers form" (page 136)
  - — "Contacts form" (page 139)
  - — "Site form" (page 140)
  - — "PE Network form" (page 142)
  - — "VPN form" (page 143)

Each form has its own retrieval criteria panel where you specify search criteria, a results panel that displays the results of the search, and a details information panel that provides additional information.

Menu bar

The MDM Database Administration menu bar contains the following menus:

File menu

The **File** menu contains the following commands:

- **Login** lets you login to a database other than the default. This command is available only if you cancel the MDM Administration Database authentication dialog to the default database. See the procedures "Starting the MDM Database Administration tool" (page 154) and "Setting configuration options" (page 158).
- **Exit** exits the MDM Database Administration tool.

Edit menu

The **Edit** menu contains the following commands:

- **Copy** copies the selected text to the system clipboard. You can paste this information into another application.

- **Cut** deletes any selected text from the window and saves it to the system clipboard.
- **Paste** copies the current contents of the system clipboard to the current cursor position.
- **Select All** selects all entries in any editable text area.
- **Deselect All** cancels the selection of the Select All command.

Options menu

The **Options** menu contains the following commands:

- **Configuration** opens the Configuration Options dialog where you configure database connectivity and administration scripts.
- **Logging** opens the Logging Options dialog where you can specify the type of information to log. You can log error, warning, information, and debug messages. Log messages are saved in the /opt/MagellanNMS/data/log/CircuitManagement.log file. For details about managing the size of log files, see "Circuit management log files" (page 114).

Tools menu

The **Tools** menu contains the following commands:

- **Circuit Discovery** starts the circuit discovery process. For procedures, see "Discovering circuits" (page 160).
- **ATM Service Provisioning** starts the ATM service provisioning tool. For information about ATM service provisioning, see 241-6001-600 *Preside MDM Service Provisioning for ATM User Guide*.
- **Frame Relay Service Provisioning** starts the Frame Relay service provisioning tool. For information about Frame Relay service provisioning, see 241-6001-603 *Preside MDM Service Provisioning for Frame Relay User Guide*.
- **Circuit Viewer** starts the Circuit Viewer tool. For information about the Circuit Viewer tool, see the section on Circuit Viewer in 241-6001-011 *Preside MDM Fault Management User Guide*.

Help menu

The **Help** menu contains the following commands:

- **Help On Window** accesses the online help information for the MDM Database Administration main window.
- **Help On Context** displays online information about objects in the window.

MDM Database Administration forms

The MDM Database Administration main window provides the following forms to manage the administration database:

- "Circuits form" (page 133)
- "Customers form" (page 136)
- "Contacts form" (page 139)
- "Site form" (page 140)
- "PE Network form" (page 142)
- "VPN form" (page 143)
- "IP Access form" (page 145)
- "Devices form" (page 147)
- "Interfaces form" (page 148)

Circuits form

Use the Circuits form to list available circuits, display circuit details, and manage user-defined circuits in the database.

Circuits are created by the service provisioning tools or by the discovery process. You can use the MDM Database Administration tool to delete circuits. However, you cannot use the tool to add or delete circuit components as these circuit components are switch-mastered.

The Circuit Viewer tool retrieves circuit information from the Administration Database. You can use it to view data that includes circuit information such as the circuit ID and type, customer information, circuit components and

connection states of those components. For details about the Circuit Viewer tool, see the Circuit Viewer section in 241-6001-011 *Preside MDM Fault Management User Guide*.

The Circuits form consists of the following panels:

- "Circuit retrieval criteria" (page 134)
- "Circuit(s) found" (page 134)
- "Circuit details" (page 134)

Circuit retrieval criteria

Use this retrieval panel to specify the criteria for retrieving circuits from the Administration Database. You can filter your retrieval requests by applying search patterns that limit the display of circuits.

In the retrieval criteria panel, the asterisk (*) acts as a wildcard. When a retrieval field contains both an asterisk and underscore (_) character, the database interprets the underscore as a single character wildcard. This interpretation may cause unintended search results. If you omit the asterisk, underscore are interpreted literally.

The following command buttons are available in the retrieval criteria panel:

- **Retrieve** initiates a database retrieval based on the specified retrieval criteria.
- **Reset** resets the values in the retrieval panel back to their default settings.

The results of any circuit retrieval request display in the Circuit(s) found list.

Circuit(s) found

The Circuit(s) found panel lists the composite circuit that the circuit belongs to. Selecting an entry in the Circuit(s) found list populates the Circuit details panel.

Circuit details

The circuit details panel displays the details of the circuit selected in the Circuit(s) found list. The details are presented in the following tabbed panes:

- "General" (page 135)

• “Components” (page 136)

General

The General pane displays general circuit attributes, some of which you can edit. This pane contains the following fields:

- **Circuit name** is the 128-byte circuit identifier that operators use to assign meaningful names to circuits to facilitate searches and end customer associations. Note that this database field can be set to be the same value as the on-switch provisioned correlation tag (through discovery options or use of the Service Provisioning tool). This method is recommended, to ensure automatic co-ordination between on-switch components, database and down-stream processes (through the accounting records). This field can be set independently from the correlation tag. No restriction or uniqueness checking on the device is done. **This name may not contain commas**. For ATM permanent virtual circuits (PVC), the identifier is set to the same value for all components in the end-to-end circuit. For ATM soft permanent virtual circuits (SPVC), it is set at the source device only.

  Note: If accounting collection is enabled at the ATM Interface, then setting the correlationTag attribute automatically turns on accounting for that virtual circuit. If accounting is not desired, then it should be disabled at the ATM Interface or the correlationTag should not be used.

- **Circuit Type** displays the circuit type of the selected circuit.
- **Site Name** displays the name of the site. **This name may not contain commas**.
- **IP Access Point Name** displays the name of the IP Access Point. **This name may not contain commas**.
- **Circuit Status** displays the synchronization status of a circuit after discovery.
- **Last Updated On** displays the time the circuit is created or modified, whether by discovery or by a service provisioning tool.

- **Customer** specifies the customer associated with the circuit. To search the database for a customer, click the browse button [...]. A Search for Customer dialog opens to let you query the customer names in the database. From the results of your query, you can select an entry to populate the Customer field. **This name may not contain commas**.
- **Description** adds descriptive information about the circuit. Such descriptive information might include a contact name and telephone number. This field can contain up to 1000 characters.

Components

The Components pane displays the A and Z endpoints of the circuit, if they exist. Circuit endpoints display as A and Z. It also displays the TM Profile, if appropriate.

Customers form

The Customers form contains information about the subscriber of the circuit. The customer, along with associated information, is defined in the database and can be associated with specific components.

When you install the database, the system automatically creates two customers; the Default customer and the ISP customer. Initially, the Default Customer contains no description or associated contacts. You can modify the contents, but you cannot delete the Default Customer. Some objects in the Administration Database require an association to a customer. If there is no specific customer association, then the Default Customer is used.

The Customers form consists of the following panels:

- “Customer retrieval criteria” (page 136)
- “Customer(s) found” (page 137)
- “Customer details” (page 137)

Customer retrieval criteria

Use this retrieval panel to specify the criteria for retrieving customer names from the Administration Database. You can filter your retrieval requests by applying search patterns that limit the display of customers in the database.

The following command buttons are available in the retrieval criteria panel:

- **Retrieve** initiates a database retrieval based on the specified retrieval criteria.
- **Reset** resets the values in the retrieval panel back to their default settings.

The results of any customer retrieval request display in the Customer(s) found list.

Customer(s) found

The Customer(s) found panel lists those customers that meet the criteria specified in the retrieval criteria panel. Selecting an entry in the Customer(s) found list, populates the Customer details panel.

Customer details

The customer details panel displays the details of the customer selected in the Customer(s) found list.The details are presented in the following tabbed panes:

- "General" (page 137)
- "Address" (page 138)
- "Route Targets" (page 138)

General

The General pane displays general customer attributes that you can edit.

- **is default** specifies this is a default customer.
- **is ISP** specifies this is an ISP customer.
- **Customer Name** displays the customer name displays. To create a new customer, add the new customer name in this field. You can enter up to 50 text characters in this field. **This name may not contain commas**.
- **ASN** displays the Autonomous System Number.
- **Business Category** displays the organization's business type.
- **Description** contains descriptive information about the customer. You can modify any existing descriptive customer information or you can add descriptive information for a new customer. You can enter up to 2000 text characters in this field.

Address

The address pane contains details about the customer address including the following information:

- Street
- City
- State/Province
- Country
- Postal Code
- Phone Number
- Fax Number
- e-mail
- Registered Address

Route Targets

The Route Target pane lists the Rout Targets associated with the Customer.

For RFC 2547 VPNs, the VPN is defined by associating customers to Route Targets using the Customer panel. This, in turn, automatically builds the IP VPN. For more information, refer to "Associating route targets to a customer" (page 170).

For RFC 2764 VPNs, the VPN is defined by the on-switch VPN Id attribute. For more information, refer to "Associating a VPN to a customer" (page 187).

This pane displays a **Change RT Owner** button which launches the **New RT Owner** window. This window is used to associate Route Targets with a Customer.

> ***Note:*** For 2547 VPNs, when you associate a Route Target with a different Customer, the tool automatically performs VPN discovery.

Contacts form

The Contacts form lets you manage Contact data and associate a contact with one or more customers.

The Contacts form consists of the following panels:

- “Contact retrieval criteria” (page 139)
- “Contacts(s) found” (page 139)
- “Contact details” (page 139)

Contact retrieval criteria

Use this retrieval panel to specify the criteria for retrieving contact names from the Administration Database. You can filter your retrieval requests by applying search patterns that limit the display of customers in the database.

The following command buttons are available in the retrieval criteria panel:

- **Retrieve** initiates a database retrieval based on the specified retrieval criteria.
- **Reset** resets the values in the retrieval panel back to their default settings.

The results of any contact retrieval request display in the Contact(s) found list.

Contacts(s) found

The Contacts(s) found panel lists those contacts that meet the criteria specified in the retrieval criteria panel. Selecting an entry in the Contacts(s) found list, populates the Contact details panel.

Contact details

The Contact details panel displays the details of the contact selected in the Contact(s) found list.The details are presented in the following tabbed panes:

- “General” (page 140)
- “Address” (page 138)

General

The General pane displays general contact attributes.

- **Customer Name** displays the customer that the contact represents. **This name may not contain commas**.
- **Last Name** displays the surname of the contact.**This name may not contain commas**.
- **First Name** displays the first name of the contact. **This name may not contain commas**.
- **Title** displays the business title of the contact
- **Description** contains descriptive information about the contact. You can modify any existing descriptive contact information or you can add descriptive information for a new contact. You can enter up to 2000 text characters in this field.

Address

The address pane contains details about the customer address including the following information:

- Street
- City
- State/Province
- Country
- Postal Code
- Phone Number
- Fax Number
- e-mail
- Registered Address

Site form

Use the Site form to create, delete and modify a site and to link a customer to a site.

The Site form consists of the following panels:

- "Site retrieval criteria" (page 141)
- "Site(s) found" (page 141)
- "Site details" (page 141)

Site retrieval criteria

Use this retrieval panel to specify the criteria for retrieving site names from the Administration Database. You can filter your retrieval requests by applying search patterns that limit the display of sites in the database.

The following command buttons are available in the retrieval criteria panel:

- **Retrieve** initiates a database retrieval based on the specified retrieval criteria.
- **Reset** resets the values in the retrieval panel back to their default settings.

The results of any contact retrieval request display in the Site(s) found list.

Site(s) found

The Site(s) found panel lists those sites that meet the criteria specified in the retrieval criteria panel. Selecting an entry in the Site(s) found list, populates the Site details panel.

Site details

The Site details panel displays the following details of the site selected in the Site(s) found list.

- **Site name** displays the name of the site. **This name may not contain commas**.
- **Customer** displays the customer that the site represents. This field must be filled when creating a new site. **This name may not contain commas**.
- **Extranet enabled** is a checkbox which identifies whether the Site is extranet enabled.

- **Description** contains descriptive information about the site. You can modify any existing descriptive site information or you can add descriptive information for a new site. You can enter up to 2000 text characters in this field.

PE Network form

Use the PE form to:

- create, delete and modify a Provider Edge Network
- add and remove Core Routers from a Provider Edge Network

The PE form consists of the following panels:

- "PE Network(s) retrieval criteria" (page 142)
- "PE Network(s) found" (page 142)
- "PE Network details" (page 143)

PE Network(s) retrieval criteria

Use this retrieval panel to specify the criteria for retrieving PE Network names from the Administration Database. You can filter your retrieval requests by applying search patterns that limit the display of PE Networks in the database.

The following command buttons are available in the retrieval criteria panel:

- **Retrieve** initiates a database retrieval based on the specified retrieval criteria
- **Reset** resets the values in the retrieval panel back to their default settings

The results of any PE Network retrieval request display in the PE Network(s) found list.

PE Network(s) found

The PE Networks(s) found panel lists those PE Networks that meet the criteria specified in the retrieval criteria panel. Selecting an entry in the PE Networks(s) found list, populates the PE Networks details panel.

PE Network details

The PE Networks details panel displays the details of the PE Network selected in the PE Networks(s) found list. The details are presented in the following tabbed panes:

- "General" (page 143)
- "Components" (page 143)

General

The General pane displays general PE Network attributes.

- **PE Network Name** displays the name of the Provider Edge network. **This name may not contain commas**.
- **ASN** displays the name of the Autonomous System Number.
- **Network Type** displays a 2547 or 2764 IP VPN.
- **Peering Topology** displays a mesh or route reflector topology
- **Description** contains descriptive information about the PE Network. You can modify any existing descriptive information or you can add descriptive information for a new PE Network. You can enter up to 2000 text characters in this field

Components

The Components pane lists all the Core Network Routers associated with the PE Network.

VPN form

2547 VPN ownership is determined by the Route Target. For more information, refer to "Route Targets" (page 138).

Use the VPN form to:

- manage the Name and Description attributes of the VPN
- change the link to the default customer for the RFC 2764 VPN to another selected customer.
- delete a VPN with a status of OBSOLETE.

Note: Creation and deletion of VPNs is done via automatic discovery of VPNs during the discovery phase or by provisioning through the IP VPN Service Provisioning Tool.

The VPN form consists of the following panels:

- "VPN retrieval" (page 144)
- "VPN(s) found" (page 144)
- "VPN details" (page 144)

VPN retrieval

Use this retrieval panel to specify the criteria for retrieving VPN names from the Administration Database. You can filter your retrieval requests by applying search patterns that limit the display of VPNs in the database.

The following command buttons are available in the retrieval criteria panel:

- **Retrieve** initiates a database retrieval based on the specified retrieval criteria.
- **Reset** resets the values in the retrieval panel back to their default settings.

The results of any contact retrieval request display in the VPN(s) found list.

VPN(s) found

The VPN(s) found panel lists those VPNs that meet the criteria specified in the retrieval criteria panel. Selecting an entry in the VPN(s) found list, populates the VPN details panel.

VPN details

The VPN details panel displays the following details of the VPN selected in the VPN(s) found list.

- **Customer** displays the customer that the VPN represents. **This name may not contain commas**.
- **PE Network Name** displays the name of the Provider Edge network. **This name may not contain commas**.
- **VPN name** displays the name of the VPN. **This name may not contain commas**.

- **VPN Type** displays either 2764 or 2547 IP VPN type.
- **VPN Id** displays the VPN identification number.
- **Description** contains descriptive information about the VPN. You can modify any existing descriptive VPN information or you can add descriptive information for a new VPN. You can enter up to 2000 text characters in this field.

IP Access form

Use the IP Access form to:

- link an IP Access Point to a site
- link Circuits to the IP Access Point if it was not done during the loading and circuit discovery (for RFC 2764 only) or if the circuits were not created using the Service Provisioning tools.

The IP Access form consists of the following panels:

- "IP Access Point retrieval criteria" (page 145)
- "IP Access Point(s) found" (page 146)
- "IP Access Point details" (page 146)

IP Access Point retrieval criteria

Use this retrieval panel to specify the criteria for retrieving IP Access Point names from the Administration Database. You can filter your retrieval requests by applying search patterns that limit the display of IP Access Point in the database.

The following command buttons are available in the retrieval criteria panel:

- **Retrieve** initiates a database retrieval based on the specified retrieval criteria.
- **Reset** resets the values in the retrieval panel back to their default settings.

The results of any contact retrieval request display in the IP Access Point(s) found list.

IP Access Point(s) found

The IP Access Point(s) found panel lists those IP Access Points that meet the criteria specified in the retrieval criteria panel. Selecting an entry in the IP Access Point(s) found list, populates the IP Access Point details panel.

IP Access Point details

The IP Access Point details panel displays the details of the IP Access Point selected in the IP Access Point(s) found list. The details are presented in the following tabbed panes:

- "General" (page 146)
- "Components" (page 146)

General

The General pane displays the following IP Access Point attributes.

- **Site -**the Site associated with the IP Access Point.
- **Customer** - the Customer associated with the IP Access Point. Note that the Customer is derived from the association of an IP Access Point with a Site. It cannot be directly assigned to the IP Access Point but rather is associated with a Site when the IP Access Point is assigned to a Site. **This name may not contain commas**.
- **IP Access Point Name** - the name of the IP Access Point. **This name may not contain commas**.
- **IP Logical Interface** - the IP Logical Interface associated with the IP Access Point
- **VRF Name** - the name of the VRF instance with which the IP Access Point is associated
- **VRF Type** - the type of the VRF (2547 or 2764).
- **Description** - adds descriptive information about the IP Access Point

Components

The Components pane lists all the Circuits associated with the IP Access Point.

Devices form

Use the Devices form to list devices and view device details. The results of any device retrieval request displays in the Devices(s) found list. A device can represent a Passport or any other device type.

The Devices form consists of the following panels:

- "Devices retrieval criteria" (page 147)
- "Device(s) found" (page 147)
- "Device details" (page 147)

Devices retrieval criteria

Use this retrieval panel to specify the criteria for retrieving ATM interfaces from the database. You can retrieve Devices using the following fields:

- **Device Name** specifies a device name or device name search pattern. This field supports context. To use context, right click in the field to open a popup menu. From the popup, select Get Context.
- **Device Type** specifies a device type or device type search pattern.

The following command buttons are available in the retrieval criteria panel:

- **Retrieve** initiates a database retrieval based on the specified retrieval criteria.
- **Reset** resets the values in the retrieval panel back to their default settings.

The results of any device retrieval request display in the Device(s) found list.

Device(s) found

The Device(s) found panel lists those devices that meet the criteria specified in the retrieval criteria panel. Selecting an entry in the Device(s) found list populates the Device details panel.

Device details

- **Device Name** displays the selected device name from the Device(s) found list. Passport device names begin with the prefix EM/.
- **Device Type** specifies the device type of the selected device, either Passport or other.

- **Address Prefix** displays the network address prefix of the selected device.
- **Vendor Name** specifies the vendor of the device, if that information is available.
- **Last time loaded** specifies the modification date and time of the selected device.

Interfaces form

Use the Interfaces form to list interfaces and view interface details. The interface represents an interface of any networking protocol and vendor implementation. interface components.

The Interfaces form consists of the following panels:

- "Interface retrieval criteria" (page 148)
- "Interface(s) found" (page 149)
- "Interface details" (page 149)

Interface retrieval criteria

Use this retrieval panel to specify the criteria for retrieving interfaces from the Administration Database. You can retrieve interfaces using the following fields:

- **Device Name** specifies the device name or device name search pattern for retrieval. **This name may not contain commas**.
- **Interface Name** specifies the interface name or search pattern for retrieval. For logical instances on Passport, this name is the full Passport component name excluding the device, for example AtmIf/1200 or Trk/34.
- **Interface Type** specifies the type of interface. For Passport devices, the values are AtmIf, FrUni, FrNni, FrAtm, and Trk.
- **Customer Name** specifies the name of the customer that owns the interface. Every interface has an owner, including the service provider as owner. **This name may not contain commas**.
- **Facility ID** specifies the facility for billing and other customer relationship management purposes.

The following command buttons are available in the retrieval criteria panel:

- **Retrieve** initiates a database retrieval based on the specified retrieval criteria.
- **Reset** resets the values in the retrieval panel back to their default settings.

The results of any interface retrieval request display in the Interface(s) found list.

Interface(s) found

The Interface(s) found panel lists those interfaces that meet the criteria specified in the retrieval criteria panel. Selecting an entry in the Interface(s) found list populates the Interface details panel.

Interface details

The details panel contains the following fields:

- **Device Name** displays the device name of the selected service interface.
- **Interface Name** displays the interface name of the selected service interface.
- **Interface Type** displays the interface type of the selected service interface.
- **Address** displays the network address of the selected service interface.
- **Remote Interface** displays the interface on the remote end of the link.
- **Facility ID** displays the facility ID associated with the selected service interface.
- **Customer Name** displays the customer associated with the selected service interface. **This name may not contain commas**.
- **Last time loaded** displays the date and time that the selected interface was loaded into the database.

Command buttons

The MDM Database Administration window contains a combination of the following command buttons:

- **New** allows you to create an object in the database.

- **Delete** allows you to delete an object in the database.
- **Apply** saves the changes to the database.
- **Cancel** cancels any changes that you made from the time you last clicked the Apply button.

Status bar

The status bar indicates the status of the MDM Database Administration tool and displays the host name of the workstation to which you are connected.

Online Help

There are various types of online help available in the MDM Management tool. You can access the following help:

- Tool tips are available by placing the mouse pointer over fields in the form. A description of the field displays for a few seconds.
- The **Help** menu provides the following information:
  - **Help On Window** displays general descriptive information about the MDM Database Administration tool.
  - **Help On Context** displays general information about objects in the window.
- The **Help** button in a dialog provide general descriptive information for that dialog.

Chapter 9
MDM Database Administration procedures

This section provides procedures and information for using the Preside Multiservice Data Manager (MDM) Administration Database and contains the following topics:

Getting Started

Managing circuits

Managing customer data

Managing IP Access Point data

Managing device data

Managing ATM interface data

Using component context

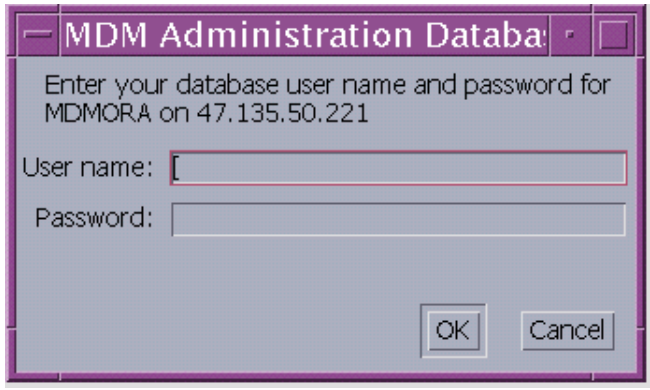
Starting the MDM Database Administration tool

Use this procedure to start the MDM Database Administration tool.

Procedure steps

1 On the Preside MDM window, select **System -> Administration -> MDM Database Administration**.

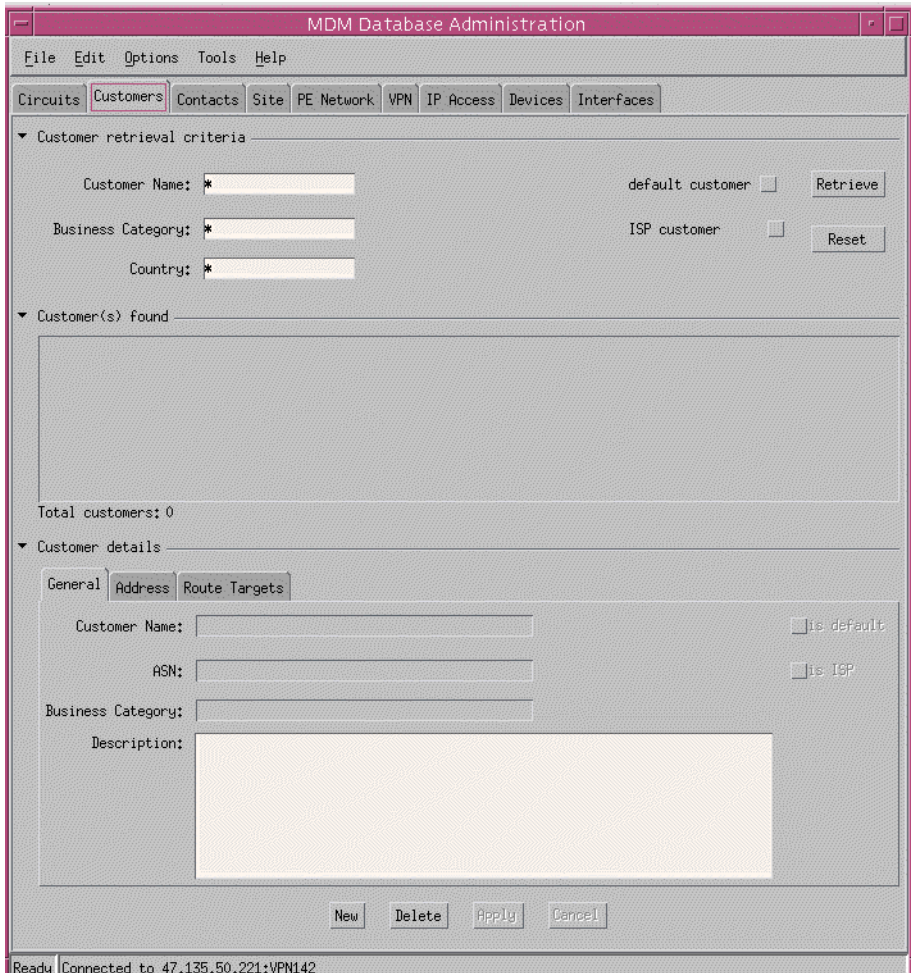
The MDM Database Administration tool opens but is not enabled. The MDM Admin DB authentication dialog opens with the default database selected.



2 In the MDM Admin DB authentication dialog, select one of the following methods:

- To access the default database, type a valid user name and password and click **OK**.
- To change the default database, click **Cancel** and go to the procedure “Setting configuration options” (page 158).

The dialog closes and the MDM Database Administration window is enabled.



When the status bar at the bottom of the window displays “Ready” and “Connected”, you can proceed with other database administration tasks.

Displaying MDM Database Administration online help

Use this procedure to view online help for the MDM Database Administration tool.

The Help menu provides online help information for the MDM Database Administration tool. You can view general descriptive information for the tool or context-specific help information.

Procedure steps

1. For an overview description, from the MDM Database Administration window **Help** menu, select **Help On Window**.

   The online help window opens with a general description of the MDM Database Administration tool.

2. For help on a specific area of the main window, from the **Help** menu, select **Help On Context**.

   The mouse changes to a question mark (?).

   a. Move the mouse onto an area of the Database Administration window for which you want help and then click the mouse.

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

Setting log file information levels

Use the Logging Options dialog to set the appropriate information level to save in the MDM Database Administration log file

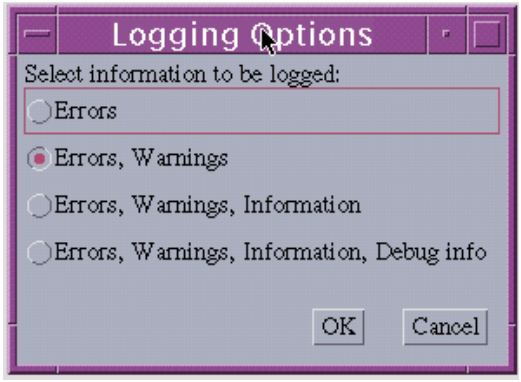
Expected results

The Logging Options dialog sets the level of information to save in the MDM Database Administration log file. The MDM Database Administration tool stores the specified logging options in the /opt/MagellanNMS/data/log/CircuitManagement.log file. For more information about log files and file size restrictions, see “Circuit management log files” (page 114).

Procedure steps

1 From the **Options** menu, select **Logging.**

The Logging Options dialog opens.



2 Click the appropriate information level that you want to log.

3 Click **OK**.

The logging options are set and the dialog closes.

Setting configuration options

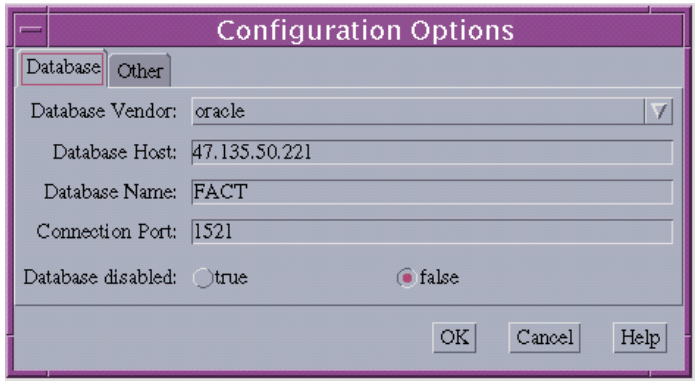
The Configuration Options dialog lets you modify the MDM Database Administration configuration options. Use this procedure to change the default settings for the database vendor, the database name and connection ports.

Procedure steps

1. From the **Options** menu, select **Configuration.**

   The **Configuration Options** dialog opens.

2. To change the options for database connectivity, click the **Database** tab and complete the fields, as required.



3. To change the options for the maximum rows received from a query, select the **Other** tab and enter a new number.
4. To save the changes and close the dialog, click **OK**.
5. If you make any changes in the **Database** tab, the **MDM Administration Database** authentication dialog opens with the new default database selected. Type a valid user name and password and click **OK**.

Managing circuit data

You manage circuit data by using the Circuits form in the MDM Database Administration window. This form lets you modify off-switch information in the Administration Database. Use the following procedures to perform circuit administrative tasks:

- “Discovering circuits” (page 160)
- “Querying circuits” (page 163)
- “Deleting a circuit record” (page 164)
- “Associating information with circuits” (page 165)

Discovering circuits

Use this dialog to manually discover circuits if auto-discovery is not turned on. This procedure:

- identifies components in the database that are not currently part of a circuit and determines the circuit to which they belong
- identifies components that are already part of a circuit and determines if they are valid. If a circuit is no longer valid the component is removed from the circuit and an attempt is made to discover a new circuit for the component.

Prerequisites

When you provision a circuit by methods other than the MDM service provisioning tools, you need to provide sufficient information about the circuit so that circuit discovery can succeed.

Perform circuit discovery after the database has been updated with the latest view and journal files. For more information, see "Database population and synchronization" (page 79).

Expected results

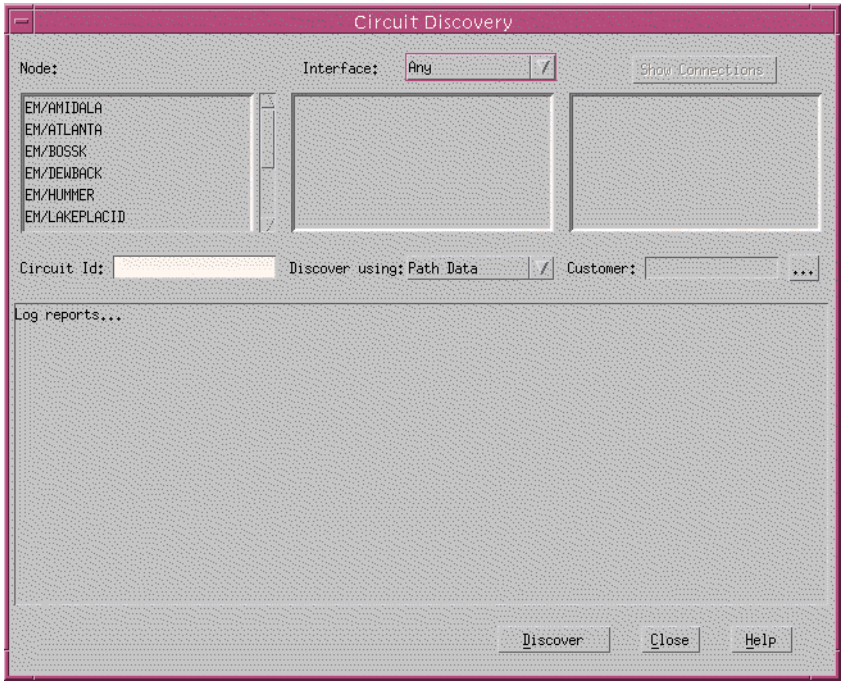
If the circuit discovery process finds more than one circuit, then the discovery process also provides new circuit IDs for each circuit. The naming convention uses the circuit ID specified in the Discover Circuits Dialog as a prefix, followed by a dash, and then an incrementing integer value starting at zero (for example, 383B-0, 383B-1, 383B-2).

Note: If you do not see circuits discovered in Circuit Viewer, view the dependency list to determine possible causes. Turn on the Debug mode in the Data Synchronization server to view the trace information in admindb.log (in /opt/MagellanNMS/data/dbsync).

Procedure steps

1 From the **Tools** menu, select **Circuit Discovery**.

The Discover Circuits Dialog opens with a list of devices from the Administration Database.



2 Select a device by clicking on an entry in the **Node** list.

3 In the **Interface** box, select an interface type from the drop down list.

The **Interface** list displays a list of interfaces.

4 To select an interface, click on an entry in the **Interface** list.

5 If needed, to select a connection component:

- Double-click on an interface to display in the **Show Connections** list all connection components for the interface.
- Select one or more connection components in the **Show Connections** list.

6 In the **Circuit ID** box, type a valid circuit ID for a single component or type a circuit ID prefix for multiple components.

If you try to discover circuits but leave this field blank, a dialog opens and prompts for whether or not a circuit ID is to be generated. If you choose to generate a circuit ID, the correlation tag of the target component is used, if available. Otherwise, a circuit ID will be generated with the following format: new circuit: <unique circuit ID number>. Note that, for IP VPN Access circuits, the Id is ignored as 'IPCoS' is used for the circuit Id. If you choose not to generate a circuit ID, the dialog closes.

7 From the **Discover using** drop-down list, select a method of circuit discovery.

8 To select a Customer:

a. Press the **Browse** button to the right of the **Customer** box.

A dialog is displayed which allows you to search for available customers.

b. Select a customer from the **Customer(s) found** list and click the **OK** button.

9 Click **Discover** or **Validate/Re-Discover**.

The **Discover** button changes to **Validate/Re-Discover** if you select a connection component that is already in a circuit.

Results of this process display in the text box. If the discovery is successful, you can view the circuit. If the discovery fails, the reason for failure displays in the text box. Alternatively, you can check the /opt/MagellanNMS/data/log/CircuitManagement.log file.

10 To close the dialog, click **Close**.

11 To view the newly discovered circuit, in the Circuit retrieval criteria panel of the MDM Database Administration window, type the circuit ID and click **Retrieve**.

Querying circuits

Use this procedure to specify the criteria for retrieving circuit information from the Administration Database.

Note: The Circuit Viewer tool also displays circuit information. For more information about the Circuit Viewer tool, refer to 241-6001-011 *Preside MDM Fault Management User Guide*.

Procedure steps

1. In the MDM Database Administration window, click the **Circuits** tab.
2. In the **Circuit retrieval criteria** panel, specify at least one of the following fields for circuit retrieval:
   - **Circuit ID** - Type a search pattern to display a selection of circuit IDs, or type an asterisk (*) to display all circuit IDs in the Administration Database.
   - **Customer** - Type the customer name, or type an asterisk (*) to display all customers in the Administration Database.
   - **Service Type** - Select an entry (Any, ATM, FR, IP VPN Access) from the drop-down list.
   - **Component** - Type a search pattern to display a selection of components, or type an asterisk (*) to display all components in the Administration Database.
   - **TM Profile**- Select the browse button [...] to display the **Search for TM Profile** window. Type a search pattern in the **Profile Name** field to display a selection of TM Profiles, or type an asterisk (*) to display all TM Profiles in the Administration Database. Select a profile type from the **Profile Type** drop-down list. Click **OK**.
   - **Facility ID** - Type a search pattern to display a selection of facility IDs, or type an asterisk (*) to display all facility IDs in the Administration Database.
   - **Circuit Type** - Select a circuit type from the drop-down list.
   - **Circuit Status** - Select a circuit status from the drop-down list.
3. Click **Retrieve**.

   A list of circuits displays in the **Circuit(s) found** panel.

Deleting a circuit record

Use this procedure to delete a circuit record from the Administration Database.

Expected results

When you delete a record, the MDM Database Administration tool deletes all components related to a circuit.

Procedure steps

1. In the MDM Database Administration window, click the **Circuits** tab.
2. If needed, query the database (see “Querying circuits” (page 163)).

   A list of circuits displays in the **Circuit(s) found** field.
3. From the list, select the circuit to delete.
4. Click **Delete**.

Associating information with circuits

Use this procedure to associate a customer to a circuit.

Procedure steps

1. In the MDM Database Administration window, click the **Circuits** tab.
2. Query the database (see “Querying circuits” (page 163)) to display of list of circuits.

   A list of circuits displays in the **Circuit(s) found** field.
3. In the Circuit(s) found list, select a circuit.
4. To find a customer to associate with a circuit:
   - Click the **General** tab.
   - Click the Customer browse button […] to open the Search for Customer dialog.
   - In the Search for Customer dialog, specify the appropriate retrieval criteria.
   - Click **Retrieve**.
5. Select the customer from the **Customer(s) found** list.
6. Click **OK**.

Managing customer data

You manage off-switch customer data using the Customers form in the MDM Database Administration window. Use the following procedures for administrative tasks on customer data:

Querying customers

Use this procedure to specify the criteria for retrieving customer information from the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **Customers** tab.
2. In the **Customer retrieval criteria** area, specify at least one of the following fields for customer retrieval:
   - **Customer Name**- Type a search pattern to display a selection of customers, or type an asterisk (*) to display all customers in the Administration Database.
   - **Business Category** - Type a search pattern to display a selection of business categories, or type an asterisk (*) to display all business categories in the Administration Database.
   - **Country** - Type a search pattern to display a selection of countries, or type an asterisk (*) to display all countries in the Administration Database.
   - **default customer** - Select this checkbox to retrieve the default customer.
   - **ISP customer** - Select this checkbox to retrieve the ISP customer.

   Note: You cannot query for both the ISP customer and the default customer at the same time. One or the other checkbox must be selected.
3. Click **Retrieve**.

   A list of customers displays in the Customer(s) found panel.
4. From the list, select a customer for which you want to view data.

   The **Customer Details** panel displays the associated customer data.

Adding a new customer

Use this procedure to add a new customer record to the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **Customers** tab.
2. Click **New**.
3. In the **Customer Name** field, type the new customer name.
4. In the **Business Category** field, type the customer's business category.
5. In the **Description** field, type descriptive customer information.
6. To save the changes in the database, click **Apply**.

   The new customer appears in the **Customer(s) found** window.

Modifying customer data

Use this procedure to change the customer information in the Administration Database.

Note: The **is Default** and **is ISP** attributes cannot be changed.

Procedure steps

1. In the MDM Database Administration window, click the **Customers** tab.
2. If needed, query customer information in the database (see “Querying customers” (page 167)).
3. Select a customer from the **Customer(s) found** list.
4. In the General pane, modify the text in the **Description**, **name** and **ASN** fields.
5. In the Address pane, modify the appropriate information if required.
6. To save the changes, click **Apply**.

Deleting a customer

Use this procedure to delete a customer record from the Administration Database. You cannot delete a customer record if it is associated with any circuit.

Note: You cannot delete the **is Default** and **is ISP** customer.

Procedure steps

1. In the MDM Database Administration window, click the **Customers** tab.
2. If needed, query customer information in the database (see "Querying customers" (page 167)).

   A list of customers displays in the Customer(s) found field.
3. From the list, select a customer.
4. To remove the customer, click **Delete**.

   A Confirm Delete dialog opens.
5. In the Confirm Delete dialog, click **Yes**.

Associating route targets to a customer

For 2547 VPNs, use this procedure to assign route targets to a customer.

Procedure steps

1. In the MDM Database Administration window, click the **Customers** tab.
2. In the **Customer details** section, select the **Route Targets** tab.
3. Click **Change RT Owner**.

   The **New RT Owner** window displays the Route Targets associated with the Customer.
4. Select one or more of the Route Targets.
5. Click **OK**.

   A confirmation dialog indicates that by reassigning RT ownership, you will invoke VPN discovery.
6. Click **OK** to confirm.

Managing contact data

Use the Contacts form in the MDM Database Administration to display and modify customer contact data. You can also use this form to associate a contact with one or more customers. Use the following procedures to manage contact data:

Querying contacts

Use this procedure to specify the criteria for retrieving customer contact information from the database.

Procedure steps

1. In the MDM Database Administration window, click the **Contacts** tab.
2. In the **Customer Name** field, type an asterisk (*) to retrieve all contacts, or type a contact name or name pattern.
3. In the **Contact Last Name** field, type an asterisk (*) to retrieve all last names, or type a name or name pattern.
4. Click **Retrieve**.

   A list of contacts displays in the Contact(s) found field.
5. From the list, select a contact for which you want to view data.

   The Details area displays the associated contact data.

Adding a new contact

Use this procedure to add a new customer contact to the database.

Procedure steps

1. In the MDM Database Administration window, click the **Contacts** tab.
2. Find the Customer to which you wish to add the new contact.
   a. Click the **General** tab
   b. Click the browse button to the right of the **Customer Name** field
   c. Select the box opposite either **Default Customer** or **ISP Customer**.

      To deselect either choice, click **Reset**.
   d. Click **Retrieve**.
   e. Select the customer from the **Customer(s) found** section.
   f. Click **OK**.
3. Select the **Address** tab and add address and telephone number details.
4. Click **Apply**.

Modifying contact data

Use this procedure to change the contact information in the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **Contacts** tab.
2. Query the contact information in the database (see “Querying customers” (page 167))
3. A list of contacts displays

   in the Contact(s) found panel.
4. From the **Contact(s) found** list, select a contact.
5. To modify contact names, titles, and descriptive text:
   - Click the **General** tab.
   - Modify the fields, as needed.
6. To modify address and phone numbers:
   - Click the **Address** tab.
   - Modify the fields, as needed.
7. Click **Apply**.

Deleting contact data

Use this procedure to delete contact information from the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **Contacts** tab.
2. Query the contact information in the database (see “Querying customers” (page 167)).
3. A list of contacts displays in the Contact(s) found panel.
4. From the **Contact(s) found** list, select the contact that you want to delete.

   The contact information displays in the **Contact details** panel.
5. Click **Delete**.

   A **Confirm Delete** dialog displays.
6. Click **Yes**.

   The contact is removed from the **Contact(s) found** section.

Managing site data

You manage site data using the Site form in the MDM Database Administration window. Use the following procedures for administrative tasks on sites:

Querying sites

Use this procedure to specify the criteria for retrieving site information from the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **Site** tab.
2. In the **Site retrieval criteria** panel, specify at least one of the following fields for circuit retrieval:
   - **Customer Name** - Enter the customer name or type an asterisk (*) to display all customers in the Administration Database.
   - **Site Name** - Type a search pattern to display a selection of sites, or type an asterisk (*) to display all sites in the Administration Database.
   - **Extranet enabled** - Check the box to indicate if this site is extranet enabled.
3. Click **Retrieve**.

   A list of sites displays in the **Site(s) found** panel.

Adding a site

A site can support either IP VPN as per RFC 2764 or RFC 2547.

Procedure steps

1. In the MDM Database Administration window, click the **Site** tab.

2 Click **New**.

3 In the Site details section, click the Customer browse button beside the Customer field ([...]).

The **Search for Customer** dialog displays.

4 Specify one or more of the following search criteria in the Customer Retrieval criteria section:

- Customer name
- Business Category
- Country
- Default Customer
- ISP Customer

Note: Click **Reset** to clear all entries in the criteria fields.

5 Click **Retrieve**.

6 Select a customer from this list.

7 Click **OK**.

8 Enter the site name.

9 If extranet is allowed, check the **Extranet Allowed** field.

10 You may add a description of the site in the Description field.

11 Click **Apply**.

Modifying a site

Note: If you modify the Customer reference, this data is modified for all circuits associated with this customer at this site.

Procedure steps

1 In the MDM Database Administration window, click the **Site** tab.

2 Query the site information in the database (see “Querying sites” (page 176)).

3 A list of sites displays in the Site(s) found panel

4 From the **Sites(s) found** list, select the site that you want to modify.

The site information displays in the **Site details** panel.

5 Modify the required information.

6 Click **Apply**.

Deleting a site

Prerequisites

An IP Access Point must not reference the site.

Procedure steps

1 In the MDM Database Administration window, click the **Site** tab.

2 Query the contact information in the database (see “Querying sites” (page 176)).

3 A list of sites displays in the Site(s) found panel

4 From the **Site(s) found** list, select the site that you want to delete.

The site information displays in the **Site details** panel.

5 Click **Delete**.

The system asks you if you wish to delete the site.

6 Click **Yes** to continue or **No** to cancel the deletion.

The site is removed from the list of sites. If the site is referenced by an IP Access Point, the deletion will fail.

Associating a customer to a site

Procedure steps

1 In the MDM Database Administration window, click the **Site** tab.

2 Query the site information in the database (see “Querying sites” (page 176)).

3 A list of sites displays in the Site(s) found panel

4 From the **Site(s) found** list, select the site.

The site information displays in the **Site details** panel.

5 Click the Customer browse button beside the Customer field ([...]).

The Search for Customer dialog displays a list of customers.

6 Narrow your search by specifying one or more of the following in the Customer Retrieval criteria section:

- Customer name
- Business Category

- Country
- Default Customer
- ISP Customer

7 Click **Retrieve**.

8 Select a customer to associate with the site.

9 Click **OK**.

10 Click **Apply**.

Modifying a customer site association

1 In the MDM Database Administration window, click the **Site** tab.

2 Query the site information in the database (see “Querying sites” (page 176)).

3 A list of sites displays in the Site(s) found panel

4 From the **Site(s) found** list, select the site.

The site information displays in the **Site details** panel.

5 Click the Customer browse button beside the Customer field ([...]).

The Search for Customer dialog displays a list of customers.

6 Narrow your search by specifying one of the following in the Customer Retrieval criteria section:

- Customer name
- Business Category
- Country
- Default Customer
- ISP Customer

7 Click **Retrieve**.

8 In the Site Details section, click the Customer browse button to display a list of customers.

9 Select a new customer to associate with this site.

10 Click **OK** to close this window.

11 Click **Apply**.

Managing Provider Edge Network data

You manage Provider Edge Network data using the Provider Edge Network form in the MDM Database Administration window. Use the following procedures for administrative tasks on Provider Edge Networks:

Querying Provider Edge Networks

Use this procedure to specify the criteria for retrieving Provider Edge Network information from the Administration Database.

Procedure steps

1 In the MDM Database Administration window, click the **PE Network** tab.

2 In the **PE Network retrieval criteria** panel, specify at least one of the following fields for information retrieval:

- **PE Network Name** - Type a search pattern to display a selection of Provider Edge networks, or type an asterisk (*) to display all Provider Edge networks in the Administration Database.
- **Network Type** - Use the drop-down list to select Any, 2547 or 2764 network types.
- **VPN Name** - Enter the VPN name or type an asterisk (*) to display all VPNs in the Administration Database. The Provider Edge Network that is retrieved are those associated with this VPN.
- **Router Name** - Enter the Router name or type an asterisk (*) to display all Routers in the Administration Database. The Provider Edge Network that is retrieved are those associated with this Router Name.
- **ASN** - Enter the Autonomous System Number or type an asterisk (*) to display all ASNs in the Administration Database. The Provider Edge Network that is retrieved are those associated with this ASN.

- **Peering Topology -** Use the drop-down list to select mesh or route reflector topology**.**

3 Click **Retrieve**.

A list of the networks displays in the **PE Network(s) found** panel.

4 Select one of the networks from the **PE Network(s) found** list.

The details for this network display in the **PE Network details** panel under the **General** tab. The routers in this network display under the **Components** tab.

Adding core routers to a Provider Edge Network

Procedure steps

1 In the MDM Database Administration window, click the **PE Network** tab.

2 Query the network information in the database. For more information, see “Querying Provider Edge Networks” (page 180).

3 Select a PE network from the **PE Network(s) found** panel.

4 Click the Components tab in the Details area of the pane.

5 Click **Add**.

The **Search for PE Routers** browser displays.

6 Enter values in the following search criteria:

- **Device Name** - The Device name field contains EM/*; all Passport devices names begin with this text. Type the Device name, or type an asterisk (*) to display all devices in the Administration Database.
- **Router name** - Type the Router name, or type an asterisk (*) to display all routers in the Administration Database
- **Has Provisioned VRF** - include only routers that have a provisioned VRF

7 Click **Retrieve**.

The **Router(s) found** panel displays the Core Routers.

Note 1: Only the core routers with the same ASN as the Core Network’s ASN are displayed.

Note 2: The core network must be created in order for the VPNs to be properly assigned to the core networks. After a core network is created and the VCGs or Routers are assigned to it, the VPNs are automatically assigned to the correct core network.

8 Select one or more Core Routers from the list (multi-select using the Ctrl key).

9 Click **OK**.

10 Click **Apply**.

The Core Routers are added to the Provider Edge Network and are listed in the Components section.

Removing core routers from a Provider Edge Network

Procedure steps

1 In the MDM Database Administration window, click the **PE Network** tab.

2 Query the PE Network information in the database (see "Querying Provider Edge Networks" (page 180)).

3 A list of networks displays in the **PE Network(s)** found panel.

4 From the **PE Network(s) found** list, select the network that contains the router you wish to delete.

5 Click the **Components** tab in the **PE Network details** panel.

6 Select one or more core router that you wish to delete (multi-select using the Ctrl key).

7 Click **Remove**.

8 Click **Apply**.

The Core Routers are deleted from the Provider Edge Network and are removed from the list in the Components section.

Adding a Provider Edge Network

Use the following procedure to add a Provider Edge Network.

For 2547 VPNs, you can create the PE Network object using the IP VPN Provider Edge Provisioning (PEP) tool. See 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*.

Procedure steps

1 In the MDM Database Administration window, click the **PE Network** tab.

2 In the **PE Network Details** pane, in the **General** pane, click **New**.

3 Enter the name of the Provider Edge Network in the **PE Network Name** field.

4 Enter the ASN.

5 Click on the **Network Type** drop-down list and select either 2754 or 2547 IP VPN.

6 Click on the **Peering Topology** drop-down list and select either mesh or route reflector.

7 Click **Apply**.

The Provider Edge Network is displayed in the **PE Network(s) found** pane.

8 Select the **Components** tab.

9 Click **Add**.

The **Search for PE Router** displays.

10 Enter a search criteria to find the appropriate routers to add to this Provider Edge network and click **Retrieve**.

The routers are displayed in the **Router(s) found** pane.

11 Select the routers you wish to add and click **OK**.

The routers are displayed in the **Components** pane.

12 Click **Apply**.

Modifying a Provider Edge Network

Use the following procedure to modify a Provider Edge Network.

Procedure steps

1 In the MDM Database Administration window, click the **PE Network** tab.

2 Query the PE Network information in the database (see “Querying Provider Edge Networks” (page 180)).

3 A list of networks displays in the **PE Network(s)** found panel.

4 From the **PE Network(s) found** list, select the network that you wish to modify.

5 In the **General** tab, change the appropriate information.

6 If you wish to add routers to this Provider Edge Network:

a. click the **Components** tab.

b. Click **Add**.

c. In the **Search for PE Router** window, click **Retrieve**.

d. From the **Router(s) found** pane, select the router you wish to add.

e. Click **OK**.

7 Click **Apply**.

Deleting a Provider Edge Network

Note: You cannot delete the Provider Edge Network if there are Core Routers associated with it. You must remove the Core Routers first and then delete the Provider Edge Network.

Use the following procedure to delete a Provider Edge Network

Procedure steps

1 In the MDM Database Administration window, click the **PE Network** tab.

2 Query the PE Network information in the database (see "Querying Provider Edge Networks" (page 180)).

3 A list of networks displays in the **PE Network(s)** found panel.

4 From the **PE Network(s) found** list, select the network that you wish to delete.

5 Click **Delete**.

6 Click **Yes** in the confirmation dialog.

The Provider Edge Network name is removed from the **PE Network(s) found** list,.

Managing VPN data

VPNs can created by VPN discovery as well as provisioned through the IP VPN Service Provisioning Tool. It is possible to delete the VPN or modify the name and description of an existing VPN using the following procedures:

Note: It is only possible to delete the VPN if the status of the VPNS is obsolete.

- "Querying VPNs" (page 185)

Querying VPNs

Use this procedure to specify the criteria for retrieving VPN information from the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **VPN** tab.
2. In the **VPN retrieval criteria** panel, specify at least one of the following fields for circuit retrieval:
   - **Customer Name** - Enter the customer name.
   - **VPN Name** - Type a search pattern to display a selection of sites, or type an asterisk (*) to display all VPNs in the Administration Database.
   - **VPN Id** - The id of the VPN.
   - **VPN type**: Select one of the following (Any, 2547, 2764, Direct, 2764 Static)
   - **Route Target name** - The name of the Route Target that is in the 2547 VPN.
   - **PE Network name** - The name of the Provider Edge Network.
3. Click **Retrieve**.

   A list of VPNs displays in the **VPN(s) found** panel.
4. Select a VPN in the **VPN(s) found** panel.

   The details for this VPN display in the **VPN details** panel.

Deleting a VPN

Use the following procedure to delete a VPN only if its status is Obsolete.

Procedure steps

1. In the MDM Database Administration window, click the **VPN** tab.
2. Query the VPN information in the database (see "Querying VPNs" (page 185)).

3. A list of VPNs displays in the VPN(s) found panel
4. From the **VPN(s) found** list, select the Obsolete VPN you wish to delete.

   The VPN information displays in the **VPN details** panel.
5. Click **Delete**.

   A dialog asks you if you are sure you wish to delete this VPN.
6. Click **Yes**.

Modifying VPN data

Use this procedure to change the VPN name, description and customer reference (for 2764 only) in the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **VPN** tab.
2. Query the VPN information in the database (see “Querying VPNs” (page 185)).
3. A list of VPNs displays in the VPN(s) found panel
4. From the **VPN(s) found** list, select the VPN you wish to modify.

   The VPN information displays in the **VPN details** panel.
5. Modify VPN name, Customer reference, and descriptive text in the VPN details section.

   Note: The Customer reference can only be changed for IP VPNs that are RFC 2764 VPNs.
6. Click **Apply**.

Associating a VPN to a customer

This procedure may only be used for RFC 2764 IP VPNs.

Note: For information on associating Route Targets to a Customer, refer to “Managing customer data” (page 166).

Procedure steps

1. In the MDM Database Administration window, click the **VPN** tab.
2. Query the VPN information in the database (see “Querying VPNs” (page 185)).
3. A list of VPNs displays in the VPN(s) found panel
4. From the **VPN(s) found** list, select the VPN you wish to associate to a customer.

   The VPN information displays in the **VPN details** panel.
5. Click the Customer browse button [...]. to open the Search for Customer dialog.
6. In the dialog, specify the retrieval criteria and click **Retrieve**.

7 Select a customer from the Customer(s) found list and click **OK**.

The dialog closes and populates the Customer field.

8 Click **Apply**.

A dialog indicates that if you change ownership then your circuit ownership will also be updated.

9 Click **OK**.

Managing IP Access Point data

You manage IP Access Point data using the IP Access form in the MDM Database Administration window. Use the following procedures for administrative tasks on IP Access Points:

- "Querying IP Access Points" (page 189)
- "Associating a site with IP Access Point" (page 190)
- "Adding circuits to an IP Access Point" (page 191)
- "Removing circuits from an IP Access Point" (page 191)

Querying IP Access Points

Use this procedure to specify the criteria for retrieving IP Access Point information from the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **IP Access** tab.
2. In the **IP Access Point retrieval criteria** panel, specify at least one of the following fields to retrieve IP Access Points that have an association matching the criteria:
   - **Customer Name** - Type the customer name or type an asterisk (*) to display all the customers in the Administration Database.
   - **Site Name** - Type a search pattern to display a selection of IP Access Points, or type an asterisk (*) to display all IP Access Points in the Administration Database.
   - **IP Access Point Name** - Type the IP Access Point name or type an asterisk (*) to display all the access points in the Administration Database.
   - **VRF Name** - Type the VRF name or type an asterisk (*) to display all the VRFs in the Administration Database.
   - **VRF Type** - Select the VRF type (Any, 2547 or 2764).
   - **is default customer**- Select the checkbox to search for default customers.
   - **unassigned to a site** - Select the checkbox to search for IP Access Points not currently assigned to a site.
3. Click **Retrieve**.

A list of IP Access Points displays in the **IP Access Point(s) found** panel.

4 Select an IP Access Point from the **IP Access Point(s) found** panel.

5 Click the **General** tab in the **IP Access Point details** panel to display general information for this access point.

6 Click the **Components** tab to view a list of circuits associated with this access point.

Associating a site with IP Access Point

An IP Access Point is associated with, or belongs to, a Site. For example, A Site contains IP Access Points and these IP Access Points contain Circuits.

Procedure steps

1 In the MDM Database Administration window, click the **IP Access** tab.

2 Query the IP Access Point information in the database (see “Querying IP Access Points” (page 189)).

3 A list of IP Access Points displays in the IP Access Point(s) found panel.

4 From the **IP Access Point(s) found** list, select the IP Access Point you wish to associate with the site.

The site information displays in the **Site details** panel. The site that is displayed is currently associated with the selected IP Access point. If there is no site listed, this IP Access Point does not have a site associated with it.

Note: Once the site is selected, the Customer field displays the customer associated with the site. You may not edit this field.

5 Click on the **Components** tab to view a list of the Circuits associated with this IP Access Point.

6 Click the Site browse button.

The Search for Site dialog and the Search for Customer dialog are displayed.

7 Select a site to associate with the IP Access Point.

8 Click **OK**.

9 Click **Apply**.

Adding circuits to an IP Access Point

You may only add circuits to IP Access Points that are associated with IP VPN as per RFC 2764.

Procedure steps

1. In the MDM Database Administration window, click the **IP Access** tab.
2. Query the IP Access Point information in the database (see “Querying IP Access Points” (page 189)).
3. A list of IP Access Points displays in the IP Access Point(s) found panel.
4. From the **IP Access Point(s) found** list, select the IP Access Point to which you wish to add a circuit.
5. Click the **Components** tab in the Details area of the pane.
6. Click **Add**.
7. Enter values in the following search criteria:
   - **Circuit Name** - Type a search pattern to display a selection of circuit names, or type an asterisk (*) to display all the circuits in the Administration Database.
   - **Circuit has no IP Access Point** - Select this checkbox to search for circuits that have no association with an IP Access Point.
8. Click **Retrieve**.
9. Select one or more circuits from the list (multi-select using the Ctrl key).
10. Click **Add**.
11. Click **Apply**.

    The circuits are added to the IP Access Point and are listed in the Components section.

Removing circuits from an IP Access Point

Procedure steps

1. In the MDM Database Administration window, click the **IP Access** tab.
2. Query the IP Access Point information in the database (see “Querying IP Access Points” (page 189)).
3. A list of IP Access Points displays in the IP Access Point(s) found panel.
4. From the **IP Access Point(s) found** list, select the IP Access Point from which you wish to delete a circuit (multi-select using the Ctrl key).

The site information displays in the **IP Access Point details** panel.

Note: Once the site is selected, the Customer field displays the customer associated with the site. You may not edit this field.

5 Click the **Components** tab in the **IP Access Point details** panel.

6 Click **Remove**.

7 Click **Apply**.

The circuits are deleted from the IP Access Point and are removed from the list in the Components section.

Managing interface data

You manage interface data using the Interface form in the MDM Database Administration window. Use the following procedures for administrative tasks on interfaces:

- "Querying interfaces" (page 194)

Querying interfaces

Use this procedure to specify the criteria for retrieving interface information from the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **Interface** tab.
2. In the **Interface retrieval criteria** panel, specify at least one of the following fields for interface retrieval:
   - **Device Name**- Type an asterisk (*) to display all devices in the Administration Database or type a search pattern to display a selection of devices.
   - **Interface Type** - Select an entry from the drop-down list.
   - **Interface Name** - Type an asterisk (*) to display all interfaces in the Administration Database or type a search pattern to display a selection of interfaces.
   - **Customer Name**- Type an asterisk (*) to display all customers in the Administration Database or type a search pattern to display a selection of customers.
   - **Facility ID** - Type an asterisk (*) to display all facility IDs in the Administration Database or type a search pattern to display a selection of facility IDs.

   Note: If you enter a value in the Facility ID field, this may cause slow search results because of the inter-relationships of database tables.
3. Click **Retrieve**.

   A list of interfaces displays in the **Interface(s) found** field.
4. From the **Interfaces(s) found** list, select an interface for which you want to view data.

   The **Interface details** panel displays the selected interface data.

Managing device data

You manage device data using the Devices form in the MDM Database Administration window. Use the following procedures for administrative tasks on devices:

- “Querying devices” (page 196)

Querying devices

Use this procedure to specify the criteria for retrieving device information from the Administration Database.

Procedure steps

1. In the MDM Database Administration window, click the **Device** tab.
2. Enter values in the following search criteria:
   - **Device Name** - Type an asterisk (*) to retrieve all devices or type a device name pattern.
   - **Device Type** - Type an asterisk (*) to retrieve all device types or type a device name pattern.
3. Click **Retrieve**.

   A list of devices displays in the **Device(s) found** field.
4. From the **Device(s) found** list, select a device for which you want to view data.

   The **Device details** panel displays the selected device data.

Getting information from context

Use this procedure to get component context. Some fields in the Retrieval criteria panel support the use of context which are variables shared among the fault tools using the MDM Context Server.

Procedure steps

1. Position the cursor over any of the fields in the Retrieval criteria panel that support context and right-click.

   A Get Context popup menu opens.

2. From the popup menu, select **Get Context**.

   The MDM Database Administration tool retrieves the value in context and performs a search based on that value.

Appendix A
Reference sheet for a simple Oracle configuration

This section provides instructions for the end-to-end installation and setup of the Oracle Administration Database for use with Preside MDM 14.3.

See the following sections:

MDM database creation and schema setup

This section describes how to set up the Administration Database and schema. This section includes:

Note: You must set up your database using the procedure for the default tablespace.

Prerequisites

Verify that the following prerequisites have been achieved:

- MDM 14.3 software is installed. See 241-6001-100 *Preside MDM Installer Guide*
- Oracle 8i or 9i is installed as per your Oracle Installation guide. Note that it is better to separate your data files from the software file to ensure that when you upgrade your software, the data files remain intact.
- A default database is created

Database setup for default tablespace

Use this procedure to set up small databases. This procedure is not recommended for medium or large configurations. For more information on database sizing guidelines, refer to "Planning information for setting up and configuring the database" (page 37).

Note: For more information on command options, refer to "Variable definitions" (page 202).

Procedure steps

1 Create the table spaces within the MDM database:

```
$cd $ORACLE_HOME/bin
$sqlplus
```

2 Log in to the Oracle database as the user SYSTEM. Type manager for the password. If the system password has changed, use the new password.

3 At the SQL> prompt, enter the following commands:

```
CREATE TABLESPACE <tablespace_name>
NOLOGGING
DATAFILE
'<data_file_storage_directory>/<tablespace_name>.dbf'
SIZE 1000M REUSE DEFAULT
STORAGE (INITIAL 40K NEXT 40K MINEXTENTS 1 MAXEXTENTS
505
PCTINCREASE 50);
CREATE TEMPORARY TABLESPACE
<temporary_tablespace_name>
TEMPFILE
'<data_file_storage_directory>/<temporary_tablespace_
```

```
name>.dbf>'
SIZE 500M;
AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED;
EXTENT MANAGEMENT LOCAL UNIFORM SIZE 10M;
```

An example of the command follows:

```
SQL> CREATE TABLESPACE mdmtest
2  NOLOGGING
3  DATAFILE ' /data/oracle/oradata/mdm/mdmtest.dbf'
SIZE 1000M REUSE
4  DEFAULT
5 STORAGE (INITIAL 40K MINEXTENTS 1 MAXEXTENTS 505
6 PCTINCREASE 50);
SQL> CREATE TEMPORARY TABLESPACE mdmtemp
2  TEMPFILE '/data/oracle/oradata/mdm/mdmtemp.dbf'
SIZE 500M
3  AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED
4  EXTENT MANAGEMENT LOCAL UNIFORM SIZE 10M;
```

4 Create an MDM administration user for the database. At the SQL> prompt, enter the following commands:

```
CREATE USER <ADMINDB_USER> PROFILE DEFAULT IDENTIFIED
BY <ADMINDB_PASSWORD>
DEFAULT TABLESPACE <tablespace_name>
TEMPORARY TABLESPACE <temporary_tablespace_name>
QUOTA UNLIMITED ON <temporary_tablespace_name>
QUOTA UNLIMITED ON <tablespace_name> ACCOUNT UNLOCK;
GRANT CREATE PUBLIC SYNONYM TO <admindb_user>;
GRANT CREATE ROLE TO <admindb_user>;
GRANT CONNECT TO <admindb_user>;
```

An example of the command follows:

```
SQL> CREATE USER admindb PROFILE DEFAULT IDENTIFIED BY
admindb

2  DEFAULT TABLESPACE mdmtest

3  TEMPORARY TABLESPACE mdmtemp

4  QUOTA UNLIMITED ON mdmtemp

5  QUOTA UNLIMITED ON mdmtest ACCOUNT UNLOCK;

SQL>  GRANT CREATE PUBLIC SYNONYM TO admindb;
```

```
SQL>  GRANT CREATE ROLE TO admindb;

SQL>  GRANT CONNECT TO admindb;
```

5 Connect to the Oracle database as the <admindb_user> created in step 4:

connect <admindb_user>/<admindb_password>

An example of the command follows:

```
SQL> connect admindb/admindb
```

6 At the SQL> prompt, execute the following script to create the admin database:

SQL>
@/opt/MagellanNMS/lib/sql/admindb/oracle/admin_ddl

7 Set the permissions for database users. For more information, refer to “Setting permissions for Database Users” (page 203).

Variable definitions

Variable	Definition
tablespace_name	is the name of the logical storage space of the database
data_file_storage_directory	is the directory path where the datafiles are to be stored
temporary tablespace_name	is the name of the temporary logical storage space of the database
admindb_user	is the Administration Database userid
admindb_password	is the Administration Database userid password
system_password	is the password for the user system within the database
admindb_client	is the Administration Database client userid

(Sheet 1 of 2)

Variable	Definition
admindb_client_password	is the Administration Database client userid password
admindb_report	is the Administration Database report userid
admindb_report_password	is the Administration Database report userid password
login	is the database login for the Administration Database owner

(Sheet 2 of 2)

Setting permissions for Database Users

Procedure steps

1 At the SQL> prompt, execute the following script to create the required roles with the Administration Database:

```
SQL>
@/opt/MagellanNMS/lib/sql/admindb/oracle/admin_roles
```

2 Verify that you are a system user and create an admin service provisioning user for the Administration Database. At the SQL> prompt, enter the following command:

```
CREATE USER <ADMINDB_CLIENT> PROFILE DEFAULT
IDENTIFIED BY
<admindb_client_password>
DEFAULT TABLESPACE <tablespace_name>
TEMPORARY TABLESPACE <temporary_tablespace_name>
QUOTA UNLIMITED ON <tablespace_name>
QUOTA UNLIMITED ON <temporary_tablespace_name> ACCOUNT
UNLOCK;
GRANT CONNECT TO <admindb_client>;
```

An example of the command follows:

```
SQL> CREATE USER admindb_client PROFILE DEFAULT
IDENTIFIED BY
admindb_client
2  DEFAULT TABLESPACE mdmtest
3  TEMPORARY TABLESPACE mdmtemp
```

```
4  QUOTA UNLIMITED ON mdmtemp
5  QUOTA UNLIMITED ON mdmtest ACCOUNT UNLOCK;
SQL>  GRANT CONNECT TO admindb_client;
```

3 Create an admin report user for the Administration Database. At the SQL> prompt, enter the following command:

```
CREATE USER <admindb_report> PROFILE DEFAULT
IDENTIFIED BY
<admindb_report_password>
DEFAULT TABLESPACE <tablespace_name>
TEMPORARY TABLESPACE <temporary_tablespace_name>QUOTA
ACCOUNT UNLOCK;
GRANT CONNECT TO <admindb_report>;
```

An example of the command follows:

```
SQL> CREATE USER admindb_report PROFILE DEFAULT
IDENTIFIED BY
admindb_report
2  DEFAULT TABLESPACE mdmtest
3  TEMPORARY TABLESPACE mdmtemp
4  QUOTA UNLIMITED ON mdmtemp
5  QUOTA UNLIMITED ON mdmtest ACCOUNT UNLOCK;
SQL>  GRANT CONNECT TO admindb_report;
```

4 Grant the appropriate roles to the admin database users. At the SQL> prompt, enter the following command:

```
GRANT ADMIN_ADMIN TO <admindb_user>;
GRANT ADMIN_APPLICATION TO <admindb_client_user>;
GRANT ADMIN_REPORTING TO <admindb_report_user>;
```

An example of the command follows:

```
SQL> GRANT ADMIN_ADMIN TO admindb;
SQL> GRANT ADMIN_APPLICATION TO admindb_client;
SQL>  GRANT ADMIN_REPORTING TO admindb_report;
```

5 Create a public synonym available to all user accounts by executing the following creation script:

```
SQL>
@/opt/MagellanNMS/lib/sql/admindb/oracle/admin_pub_sy
ns
```

OR

Verify that you have connected as a SYSTEM user

```
connect SYSTEM/MANAGER <admindb_password>
```

and create a private synonym for each user that needs access to the database by executing the following script:

```
SQL>
@/opt/MagellanNMS/lib/sql/admindb/oracle/admin_priv_s
yns <user_account_name> <admindb_owner>
```

Note: MANAGER is the default password for new database installations. user_account_name is the user account in which you create the synonyms. admindb_owner is the user account which owns the Admin DB tables.

MDM configuration

This section contains the following procedures you need to perform to configure MDM.

- "Adding servers to the Server Administration tool" (page 205)
- "Configuring the Database Synchronization Controller file" (page 206)
- "Configuring the Database Access" (page 209)

Adding servers to the Server Administration tool

The Administration Database uses the PP Config Server, the Backup Server, the Backup Provider, The DBSyncController, and the Passport Shared Model Server. These servers must be added to the Server Administration tool if they do not already exist.

Procedure steps

1. From the Preside MDM window, select **System** -> **Administration** -> **Server Administration**.

   The **Server Administration** window opens.

2. From the **Security** menu, select **Authorize**.

   The **SVM Enter Authorization Password** dialog opens.

3. Type in the password and click **OK**.

4. Verify that the server is present in the server list.

If the server is present, select it from the server listing. If the process is not running, right-click and select **Start** from the pop-up menu.

5 If the required servers are not present in the server list, add each server one at a time by completing the next steps.

6 From the **Edit** menu, select **New server**.

The **Server Administration** dialog for "SVM New Servers Selection" opens, displaying the following list of servers by category.

Descriptive Name	Startup Command
PP Nodal Provisioning Config Server	/opt/MagellanNMS/bin/pcserver
Backup Server	/opt/MagellanNMS/bin/nsctlbck -notification
Backup Provider	/opt/MagellanNMS/bin/pbckpp
Data Sync Server	/opt/MagellanNMS/bin/dataSyncServer
Shared Model Server	/opt/MagellanNMS/bin/pcms

7 Click on the server you wish to add and select **Select Server**.

The SVM New Server dialog displays with the default information entered in the fields.

8 In the **Startup command** field, enter the appropriate startup command according to the above table.

9 Select the **Automatic startup at reboot time** box.

10 Click **Save** and **Start**.

Note: The Backup Controller and Data Synchronization Server will require further configurations prior to starting. Before starting, perform the procedure “Configuring the Database Synchronization Controller file” (page 206).

Configuring the Database Synchronization Controller file

If you have a database, you must configure the Data Synchronization server. This server is configured via the DataSync.cfg file located in /opt/MagellanNMS/cfg. This section defines the basic customizations. For additional customization instructions, see “Setup and Configuration” (page 35).

Prerequisites

To perform this procedure, you must have root user privileges.

If you are using the Data Synchronization Administration tool, verify that the following servers are running:

- PP Config Server
- MNSDAgent Server
- MDMContext Server
- PP Command Access Server

Procedure steps

1. To edit the DBSynch Controller options, start the Configuration Editor from the Server Administration tool.

   For more information, refer to 241-6001-400 *Preside MDM Administration Database User Guide*.

2. In the list of servers, select **Data Sync Server**.
3. Right click to select **Edit Configuration -> Server Configuration**.

   The Configuration Editor displays.

4. In the left pane, expand the **Embedded Servers** selection.
5. Select the **DBSyncController** selection.
6. Edit the fields, in the right pane, as follows:
   - Enter a unique name into the **name** field. A typical naming strategy is to use the MDM workstation name on which the process will reside.
   - Do not change the value in the **class** field.
   - The **arguments** field is used to configure the DBSyncController. Arguments are -help (to display command usage information), -cfg <configFile> (to specify the configuration file to be used) and -log <logFile> (to enable logging to be written to a specified file).
   - Set the **enabled** field to true. The Data Synchronization server must be enabled even if the database is not being used.
7. Select **File>Save** to save your changes and close the dialog.
8. While **Data Sync Server** is still selected, in the Server Administration tool, right click to select **Edit Configuration->DBSync Controller**.

9 Select **Authentication** in the left pane and, in the right pane, enter the database username and password. If you want to use a password file, set **usePasswordFile** to 'true' and enter a full path in the **passwordFile** field.

10 Select **AutoDiscovery** in the left pane.

The ATM, FR and IP_VPN options are displayed in the left pane.

11 Select one of these options and select the appropriate values in the right pane. For more information on these values, refer to "Data Synchronization Configuration file parameters" (page 65).

Note: If you wish to have the circuits in the network auto-discovered each time the configuration data for a device is loaded, enter **True** in the **AutoDiscovery** field.

12 At this point, you must configure the Backup Server. For more information, refer to "Configuring backup information for an alarm driven backup" (page 46).

13 Restart the Data Sync Controller server to active the changes to the DataSync.cfg file.

Starting the DBSynchController server

Use the Server Administration tool to restart the DBSynchController to active your changes to the DataSync.cfg file.

Procedure steps

1 From the Preside MDM window, select **System** -> **Administration** -> **Server Administration**.

The **Server Administration** window opens.

2 From the **Security** menu, select **Authorize**.

The **SVM Enter Authorization Password** dialog opens.

3 Type in the password and click **OK**.

4 Select Data Sync from the server listing. If the process is running, right-click on the server, and select **Stop** from the pop-up menu.

5 When the state shows **Stopped**, right-click the server again, and click **Start** from the pop-up menu.

If Data Synch is not in the server listing, see "Adding servers to the Server Administration tool" (page 205).

See "Setup and Configuration" (page 35) for more information on other configuration options.

Configuring the Database Access

To configure database access on the workstation and all the client applications that the workstation shares, use the following procedures.

Note: These changes are stored in the dbaccess.cfg file.

Procedure steps

1 From the **Options** menu of MDM Database Administration, select **Configuration**.

The **Configuration Options** dialog opens.

2 For the **Database** tab, complete the following parameters for database connectivity:

- For **Database Vendor:** parameter, specify that Oracle is to be used to support circuit management.
- For the **Database Host** parameter, specify the IP address of the workstation where the database is installed.
- For the **Database Name** parameter, specify the database name recognized by the server. For Oracle, the database name is a registered name (called a SID or database ID).
- For **Database Port** parameter, specify the TCP port on which the database server listens for connections.
- For **Database Disabled**, set the value to **False**.

3 Save the configuration changes by clicking **OK**.

Post installation procedures

This section contains the following topics:

Initial database loading

After you install the Administration database schema, you must load the existing network configuration into the database and perform an initial discovery which discovers the layer-2 and layer-3 services implemented in the network.

Note: When you start the Backup Server, all devices that have the on-alarm flag enabled will be discovered. To discover any other device, you must run the backup on-demand command or a current view backup using the Backup and Restore tool.

Prerequisites

The latest configuration view and journals must be available in the Backup Server system. The Backup Server must be started. For more information, refer to "Starting the Backup Server (Backup Controller)" (page 59).

Procedure steps

1. Disable circuit discovery and IP VPN discovery using the no discovery (-noDiscovery) option command in the DBSyncController startup command.

   For more information, refer to "Disabling discovery" (page 211).

2. Start the Backup Server.

3. Perform a backup using the on-demand command.

   For more information, refer to "On demand" (page 72).

   OR

   Start the Backup and Restore application and perform the next steps.

4. Select **Tools ->Backup Current Configuration**.

   The Backup Current Configuration window displays

5. Click **Add**.

   The Add Group window displays.

6. Select one or more groups.

7. Click **OK**.

   The groups you wish to backup are displayed in the Group List.

8. Click **Backup**.

   After the groups have completed backing up, you must enable the discovery option.

9. Remove the no discovery (-noDiscovery) option from the DataSync Server.

   For more information, refer to "Enabling discovery" (page 211).

Note 1: For RFC 2547 VPNs, after discovery has discovered all 2547 VPNs based on the route targets, all the discovered VPNs are assigned to the Default Customer. The IP VPN SP tool can then be used to re-assign route targets to the appropriate customer.

Note 2: In order for discovery to properly associated the discovered access points with discovered circuits, you must provision the following links onswitch:

- TolpLogicalInterface (under static dlcis)
- TolpLogicalInterface (under FrConn)

10 Restart the Data Sync Server to update the changes you have made to the DBSyncController.

Note: You can now enable circuit discovery for each service as required. If you wish to perform manual circuit discovery, refer to the procedures in "Circuit discovery" (page 109)"Manual and automatic discovery" (page 109).

Disabling discovery

Use the following procedure to disable circuit and IP VPN discovery.

Procedure steps

1 Start the Server Administration application and complete the required authorization.

For more information, refer to 241-6001-303 *Preside MDM Administrator Guide*.

2 In the list of servers, select **Data Sync Server**.

3 Right click to select **Edit Configuration** -> **Server Configuration**.

4 Expand the **Embedded Servers** selection.

5 Select **DBSyncController**.

6 In the arguments field, add

```
-noDiscovery
```

7 Select **File>Save** to save your changes.

8 Restart the Data Sync Server.

Enabling discovery

Use the following procedure to enable circuit and IP VPN discovery.

Procedure steps

1. Start the Server Administration application and complete the required authorization.

   For more information, refer to 241-6001-303 *Preside MDM Administrator Guide*.

2. In the list of servers, select **Data Sync Server**.
3. Right click to select **Edit Configuration** -> **Server Configuration**.
4. Expand the **Embedded Servers** selection.
5. Select **DBSyncController**.
6. In the arguments field, remove

   ```
   -noDiscovery
   ```

7. Click **Apply**.
8. Select **Save** from the **File** menu.

Troubleshooting aids

This section contains troubleshooting information on the following topics:

Viewing the synchronization status of a device

Use the following procedure to view the synchronization status of a specific device.

Procedure steps

1. Start the Data Synchronization Administration tool. For more information, refer to "Launching the Data Synchronization Administration tool" (page 86).
2. Search for devices.

   For more information, refer to "Searching for devices" (page 86).

3. In the **Devices(s) Results** section, select the **Diagnostics** tab.
4. Select a single device from the devices list.

If no devices are listed, perform a search using the procedure “Searching for devices” (page 86).

5 In the **Details** section, select the **Summary** tab.

6 Click **Refresh**.

A summary displays the views and journals on this device, the backup repository and the database.

Enabling Database synchronization debug logs

The following steps can be used to enable debug logs from the DBSyncController. This results in a large number of logs and should not be left on for an extended period of time.

Procedure steps

1 Start the Server Administration tool. For more information, refer to “Launching the Data Synchronization Administration tool” (page 86).

2 Select **Data Sync Server>Edit Configuration>DBSyncController** from the **Options** menu.

The **Configuration Editor** opens.

3 Select **Logging** in the left pane.

4 Right click to select **Add Attribute**.

5 From the **Add Attribute** dialog, select **logDebugToFile**.

6 In the right pane, verify the following settings:

- Set logErrorToFile to **True**.
- Set logFileName to the path to the log files. The default is /opt/MagellanNMS/data/dbsync/dbsync.log.
- Set LogDebutToFile to **True**.

7 From the **File** menu, select **Save**.

Deleting a node

Use a script to delete nodes in the following situations, only if necessary:

- when a node is deleted from the network, the script purges the node's information in the database.
- when a node is renamed, the script purges the node's information in the database. Database Synchronization will reload the renamed node.

ATTENTION	Perform this procedure only on a Release 14.3 Administration database. This procedure corrupts the Administration database of all other releases.

ATTENTION	This script will delete all information related to the specified node. There is no method of recovering this information.

ATTENTION	Prior to performing this procedures, backup your entire Administration database. This backup allows you to recover the database if this procedure causes a database corruption.

Procedure steps

1 Verify that no users are accessing the database.

2 Type the following command:

```
/opt/MagellanNMS/bin/admdbldr -u <db_username> -p
<db_password> -n <nodename> -t <current_time> -delete
<loglevel>
```

Variable definitions

Variable	Definition
db_username	database user name
db_password	database password
nodename	node name (for example, LAKEPLACID)

(Sheet 1 of 2)

Variable	Definition
current_time	current system time with the format yyy-mm-dd-hh:mm:ss (for example, 2003-09-11 10:00:00)
loglevel	level of log (for example -loginfo, -logdebug)

(Sheet 2 of 2)

Enabling loader and discovery logs

Use the following procedure to enable loader and discovery logs to be saved in the admindb.log file.

Procedure steps

1. Start the Server Administration application and complete the required authorization.

   For more information, refer to 241-6001-303 *Preside MDM Administrator Guide*.

2. In the list of servers, select **Data Sync Server**.

3. Right click to select **Edit Server**.

4. In the Startup Command field, add the following option to the startup command:

   `-Dadmindb.loglevel=info`

   Note: You can set the log level to one of the following specifications, in order of increasing detail: debug, info or warn.

Preside Multiservice Data Manager
Administration Database

R14.3

Publication: 241-6001-400
Document status: Standard
Document version: 14.3RSUP
Document date: December 2003
Printed in Canada

NORTEL NETWORKS