NORTEL NETWORKS

Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks

Security and Administration

PT-AAL1/UA-AAL1/UA-IP

NN10180-611

NORTEL NETWORKS

Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks

Security and Administration

PT-AAL1/UA-AAL1/UA-IP

Publication: NN10180-611
Document status: Standard
Document version: (I)SN07S1
Document date: December 2004

Printed in Canada

Publication history

December 2004

(I)SN07S1 Standard
Contains Standard information for the SN07 FVS release.

Contents

Appendix
Preside MDM security and administration tools 99

List of figures

List of tables

About this document

This document provides the procedures for performing security and administration tasks on Nortel Networks Multiservice Switch 15000 / Media Gateway 15000 nodes in Succession Networks. Most of these procedures can be performed using either Nortel Networks Preside Multiservice Data Manager tools, or Multiservice Switch command line interface (CLI).

The following topics are discussed in this section:

Who should read this document and why

This document is intended for people who are responsible for performing security and administration functions on Nortel Networks Preside Multiservice Data Manager workstations and Multiservice Switch 15000 nodes in PT-AAL1 and UA-AAL1 Succession Network solutions, and on Preside MDM workstations, Multiservice Switch 15000 nodes, and Media Gateway 15000 nodes in UA - IP Succession Network solutions.

What you need to know

Before you read this document, it would be helpful to have a general understanding of the concept of Succession Networks, the solutions within that portfolio, and the role that the Multiservice Switch and Media Gateway can play in these solutions. For more information, see:

- NN10300-111 *IP Solutions Basics*
- NN10320-111 *ATM Solutions Basics*
- NN10028-111 *Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP*

Some familiarity with the operating principles of Multiservice Switch systems and ATM is also beneficial. For more information, see NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview* and NN10600-700 *Nortel Networks Multiservice Switch 7400/15000/20000 ATM Technology Fundamentals*.

You should also have some familiarity with security and administration operations of Nortel Networks Preside Multiservice Data Manager (MDM) toolset. For more information, see:

- NN10600-605 *Passport - MDM Network Security: Operations*
- NN10600-606 *Passport - MDM Network Security: User Access Configuration*
- NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration*
- 241-6001-303 *Preside MDM Administrator Guide*

How this document is organized

This document contains a high-level description of Nortel Networks Preside Multiservice Data Manager (MDM) tools and tasks for performing security and administration functions on Nortel Networks Multiservice Switch 15000 / Media Gateway 15000 nodes and Preside MDM workstations in Succession Networks. This document provides an overview of the implementation of distributed computing environment (DCE) for PT-AAL1 and UA-AAL1 solutions, and procedures for performing user access administration tasks

using both CLI and Preside MDM tools. Procedures are included for using the Network Model to administer Multiservice Switch nodes, for performing Preside MDM server file management and Multiservice Switch node software backup and restore, and for viewing Multiservice Switch command logs.

This document contains the following sections:

What's new in this document

The following feature was added to this document:

Preside MDM workstation synchronization

One of the pair of redundant Nortel Networks Preside Multiservice Data Manager (MDM) server workstations in a Succession Network may have a failure that requires the data on the disk drive to be restored. After the failed server has been recovered, it will be necessary for the operator to synchronize the recovered workstation with the operational workstation.

The data synchronization procedure may also be useful when installing a new redundant Preside MDM workstation or after upgrading the workstation.

The following sections were add or modified for this feature:

- "Types of data on a Preside MDM workstation" (page 72)
- "Understanding impacts of Preside MDM workstation outages" (page 76)
- "Backing up and restoring Preside MDM workstation software" (page 78)
- "Synchronizing Preside MDM workstations" (page 80)

Other changes to this document are listed below:

- The terms Passport 15000 and Packet Voice Gateway (PVG) have been rebranded in conjunction with the new Nortel Networks' brand simplified naming format.

  The Passport 15000 is now referred to as the Nortel Networks Multiservice Switch 15000. The Packet Voice Gateway (PVG) is now referred to as Nortel Networks Media Gateway 15000.

  The Multiservice Switch 15000 and Media Gateway 15000 network elements continue to share common hardware and software aspects. Hybrid systems can combine these network elements' capabilities, despite the fact that no specific brand exists for such hybrids.

  For more information on the product rebranding, refer to NN10600-000 *Nortel Networks Multiservice Switch 7400/15000/20000 What's New in PCR6.1*.

- "Security and administration overview" (page 21) was modified as follows:
  - "Multiservice Switch node and Preside MDM security management" (page 22) was updated to include reference to FMIP.
  - "Security and access tasks for Multiservice Switch 15000 nodes" (page 26) was modified to clarify the information about logging in to perform emergency functions.
  - "Secure FTP authentication" (page 27) was modified to clarify text and update the NTP references.

— "Administration of Preside MDM servers and Multiservice Switches using Preside MDM" (page 27) was created to combine information about administration of the Preside MDM and the Multiservice Switch 15000.

- "DCE implementation overview" (page 29) was modified to add a note explaining that the optional Distributed Computing Environment applies to PT-AAL1 and UA-AAL1 solutions only.
- "Configuring the root user as a Preside MDM user" (page 37) was modified to clarify the application of mdmuser, and provide other minor clarifications.
- "Multiservice Switch user access administration" (page 41) has been modified as follows:
  - "Access control components and attributes" (page 42) has been modified to update the Userid attributes.
  - "CLI provisioning mode" (page 45) was modified to clarify the wording in the Note
  - "Adding a user using the CLI" (page 46) was modified to update the definitions for the <scope> and <impact> variables, and provide minor wording changes to steps 6 and 9.
- Step 7 of "Collecting and applying network module data" (page 57) was modified to remove reference to the "CSLAN (if Passport 6480)" node name.
- "Using the Network Model tool to perform network surveillance" (page 57) was modified to correct input parameters in step 6 and add reference to MG15000 in step 10 of procedure for"Collecting and applying network module data" (page 57)
- Chapter 6 was renamed to "File Management on the Preside MDM server" (page 65), and wording in the file changed to remove references to the term "clean up". Information on managing MDP and historical alarm files was added.
- "Backing up the current view using Service Data Backup/Restore tool" (page 86) and "Service Data Backup/Restore tool" (page 104) were modified to reflect the updated name and operation of the tool.

- "Viewing command logs" (page 91) was added to include information about how to use Preside MDM Data Viewer tool to view Multiservice Switch 15000 / Media Gateway 15000 command logs when required.
- "Preside MDM security and administration tools" (page 99) was modified as follows:
  - "Service Data Backup/Restore tool" (page 104) was updated to reflect the updated name and operation of the tool.
  - "Rebooting the Preside MDM server" (page 107) in "Preside MDM security and administration tools" (page 99) was changed to improve the reboot command sequence.
- This section was updated as follows:
  - "What you need to know" (page 14) was updated to add additional reference documents.
  - "Related documents" (page 20) was updated for documents related to Viewing command logs

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 Nortel Networks Preside Multiservice Data Manager, 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

  Nortel Networks Multiservice Switch system 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

You may need to refer to the following documents while performing security tasks on Nortel Networks Multiservice Switch 15000 / Media Gateway 15000 nodes or Preside Multiservice Data Manager (MDM) servers:

- 241-6001-023 *Preside MDM Configuration Management for Passport User Guide*
- NN10600-605 *Passport - MDM Network Security: Operations*
- NN10600-606 *Passport - MDM Network Security: User Access Configuration*
- NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration*

You may need to refer to the following documents while performing administrative tasks on Multiservice Switch 15000 / Media Gateway 15000 nodes or Preside MDM servers:

- 241-6001-309 *Preside MDM Management Data Provider User Guide*
- 241-6001-011 *Preside MDM Fault Management User Guide*
- 241-6001-015 *Preside MDM Network Model Administrator Guide*
- 241-6001-303 *Preside MDM Administrator Guide*
- 241-6001-810 *Preside MDM MDP Data Formats Reference*
- NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*

How to get more help

For information on training, problem reporting, and technical support, see "Nortel Networks support services" section in NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

Chapter 1
Security and administration overview

For overview information on security and administration, see:

- “Preside MDM Security management” (page 21)
- “Preside MDM security management for Multiservice Switch nodes” (page 24)
- “Administration of Preside MDM servers and Multiservice Switches using Preside MDM” (page 27)

Preside MDM Security management

Nortel Networks Multiservice Switch nodes and Preside Multiservice Data Manager (MDM) use a two-tier authentication system. The first tier provides access to Preside MDM network management software. This level of authentication allows the operator to run Preside MDM tools, perform surveillance on the network, and passively administer Preside MDM or UNIX. It does not allow the operator to make any changes to the Multiservice Switch network. The second tier connects the operator to the Multiservice Switch nodes through the login to Preside MDM. Once connected by this method, the operator can perform network element maintenance or configuration tasks.

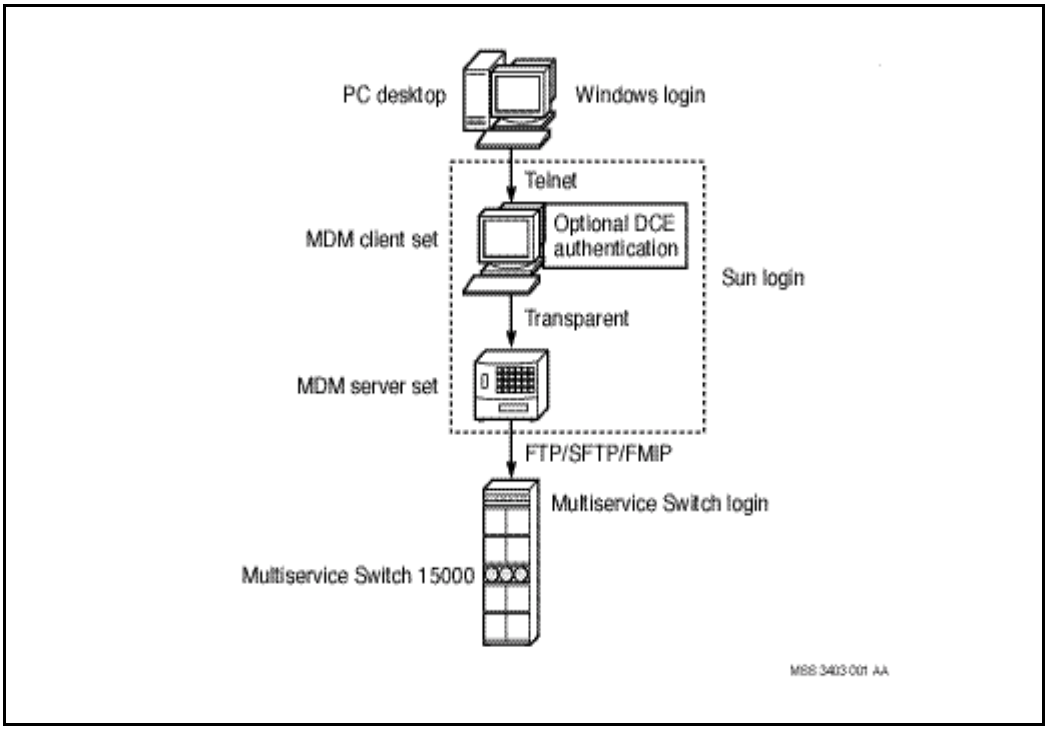
Operators who directly log in to Preside MDM require standard Preside MDM authentication (valid UNIX user ID and password). This level of authentication provides access to the UNIX platform only, and permits the user to launch Preside MDM servers and to run scripts.

For the Preside MDM client-server set, security is provided by UNIX authorization on the client-set machine, and during the configuration of the multi-nodal name server domains (MNSD). For client-set configuration, MNSD is configured with a list of the server-set workstations that are available for selection.

Preside MDM security tools monitor the status of various Preside MDM processes. For information on the monitored processes, see “MDM security and access tasks” (page 23). For more information about the security tools, see “Preside MDM security and administration tools” (page 99).

The figure “Multiservice Switch node and Preside MDM security management” (page 22) shows the levels of security.

Figure 1
Multiservice Switch node and Preside MDM security management



MDM security and access tasks

The table "Preside MDM security and access tasks" (page 23) defines the OAM security procedures required for MDM.

Table 1
Preside MDM security and access tasks

Task performed	When used	Required permissions	Notes
System administration functions	As needed.	Unix "root" user ID and password.	
Regular UNIX maintenance functions	According to the regular maintenance schedule or as needed.	Defined by the system administrator.	
Network surveillance and maintenance	As needed.	UNIX user ID and password.	Also requires a valid node user ID for maintenance.
Configuration	As needed.		Also requires a valid node user ID.
Viewing node security logs	As needed.	Preside MDM user ID which is a member of the MDP Group.	Secured using UNIX security (see Note).
MDP sysadmin	As needed.	mdpadmin.	
Preside MDM sysadmin	As needed.	Unix "root" user ID and password.	
Note: DCE is an optional security package that can govern login.			

Preside MDM security management for Multiservice Switch nodes

When an operator tries to access a Nortel Networks Multiservice Switch node through a Preside Multiservice Data Manager (MDM) tool or utility, a valid Multiservice Switch user ID and password is required. Authentication is performed by a common security function, which allows many tools to share the same authentication and network node connections.

A Multiservice Switch maintains a user profile, which consists of optional attributes that include an impact level that permits different categories of commands to be entered. The type of incoming access (for example, access over FMIP, Telnet, or serial) is configurable.

> ***Note:*** The Distributed Computing Environment (DCE) is an optional package that provides security, authentication, and shared data for the MDM toolset. For information, see "DCE implementation overview" (page 29).

For more information on the security requirements, see the following:

- "User profile impact levels" (page 24)
- "Security and access tasks" (page 26)
- "Secure FTP authentication" (page 27)

User profile impact levels

Each user profile is assigned permissions for access and an impact level that permits different categories of commands to be entered. The various categories of impact levels is determined by the impact these permitted commands could have on the node (for example, issuing a reset command requires a higher impact level than a display command).

The table "Impact levels for Multiservice Switch 15000 nodes" (page 25) identifies the impact levels available on Nortel Networks Multiservice Switch 15000 nodes within a Succession Network.

Table 2
Impact levels for Multiservice Switch 15000 nodes

Impact level	Description
Passive	Allows user read-only access and ability to issue display and list commands only
Service	Allows user to issue commands for diagnostics and maintenance purposes but not for provisioning and configuration
Configuration	Allows user to issue Service-level commands as well as provisioning and configuration commands but not commands that change user access privileges
System administration	Allows user to issue any Service or Configuration-level commands including those that change user access privileges
Debug	Allows user to issue all existing commands

Security and access tasks

The table "Security and access tasks for Multiservice Switch 15000 nodes" (page 26) identifies the security and access tasks required for Nortel Networks Multiservice Switch 15000 nodes within a Succession Network.

Table 3
Security and access tasks for Multiservice Switch 15000 nodes

Use case title and description	Frequency or time of use	Required input	Notes
Log in to perform system administration functions	As needed	Multiservice Switch user ID and password with impact of at least system administration	Access from Preside MDM tools
Log in to perform configuration functions (for example, software upgrade)	According to customer upgrade schedule or as needed	Multiservice Switch user ID and password with impact of at least configuration.	Access from Preside MDM tools
Log in to perform regular maintenance functions	According to regular maintenance scheduled or as needed	Multiservice Switch user ID and password with impact of at least service	Access from Preside MDM tools
Log in to the node to perform emergency functions requiring operating system-level commands	As needed	Multiservice Switch user ID and password with impact of at least debug	Access from Telnet or local (serial) interfaces; access from Preside MDM tools is not possible
Multiservice Switch security audits	As needed	Preside MDM UNIX user ID and password.	Use the Preside MDM Data Viewer to view the node security logs.

Secure FTP authentication

This optional security feature needs to be configured during a software upgrade. It provides a mechanism for encrypting passwords used during FTP communications between Nortel Networks Multiservice Switch nodes and Preside Multiservice Data Manager (MDM) servers.

When a Multiservice Switch node initiates an FTP session with a Preside MDM server, the type of FTP connection used depends on the configuration of the node. If the node is running PCR4.2 software or later, secure FTP is used by default. If the node uses a secure FTP connection, then the workstation must have an FTP daemon configured to ensure that secure FTP authentication is used. FTP sessions are used to download software from the Preside MDM server and upload spooled data to the workstation.

For more information about secure FTP authentication, see the following NTPs:

- NN10600-605 *Passport - MDM Network Security: Operations*
- NN10600-606 *Passport - MDM Network Security: User Access Configuration*
- NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration*

For information about installing secure FTP authentication during a Succession software upgrade, see the following NTPs:

- NN10070-461 *Upgrading Passport 15000 in Succession Networks (PT-AAL1/UA-AAL1)*
- NN10185-461 *Upgrading Preside MDM in Succession Networks*
- NN10419-461 *Upgrading Nortel Networks Multiservice Switch 15000 and Media Gateway 15000/20000 in Succession IP Solutions*

Administration of Preside MDM servers and Multiservice Switches using Preside MDM

Nortel Networks Preside Multiservice Data Manager (MDM) administration tools allow you to:

- monitor the status of various Preside MDM processes and servers

- administer Multiservice Switch equipment
- review Preside MDM and Nortel Networks Multiservice Switch log messages

For more information on these tools, see either the "Preside MDM security and administration tools" (page 99) or 241-6001-303 *Preside MDM Administrator Guide*.

For more information on auditing Multiservice Switch configuration commands, see the following section:

- "Viewing command logs" (page 91)

Chapter 2
DCE implementation overview

This module summarizes the operational and maintenance tasks to support the optional Distributed Computing Environment (DCE), Version 3.1.

> ***Note:*** The optional Distributed Computing Environment (DCE) is supported in PT-AAL1 and UA-AAL1 solutions only.

Information is provided in the following sections:

- "Succession Network node configuration with DCE" (page 30)
- "Displaying DCE account profiles" (page 32)
- "Changing your DCE operator account password" (page 33)
- "Creating new user accounts using DCE" (page 33)

For additional information on DCE in a Succession Network, see NN10170-611 *CS 2000 Core Manager Administration and Security*.

Nortel Networks Preside Multiservice Data Manager (MDM) servers can be installed with DCE Version 3.1 software and configured to use integrated login for user authentication. Individual tools accessed through Preside MDM do not use DCE for data sharing or communication.

DCE can be configured so that authentication is invoked only when the operator logs into Preside MDM. Separate user authentication is still required for logging in to Nortel Networks Multiservice Switch nodes when not logging in using DCE. However, to ensure that DCE authentication is not

bypassed for normal access, IP-based access to Multiservice Switch 15000 nodes is configured to allow access to only those operators logged in through Preside MDM.

Emergency access through the node's control processor serial port is an exception. This level of access does not fall within the scope of the DCE cell. Because serial port access is available for emergency circumstances only (when Preside MDM servers are unavailable), the administrator must ensure that this level of access is restricted to authorized operators.

Succession Network node configuration with DCE

In the Succession Network, DCE includes several hardware platforms, including the following essential servers:

- DCE master server
- DCE replica server

The figure "Example of network configuration with DCE" (page 31) illustrates an example configuration.

For more information on network node configuration using DCE, see the following sections:

- "Integrated login" (page 30)
- "DCE availability" (page 30)

Integrated login

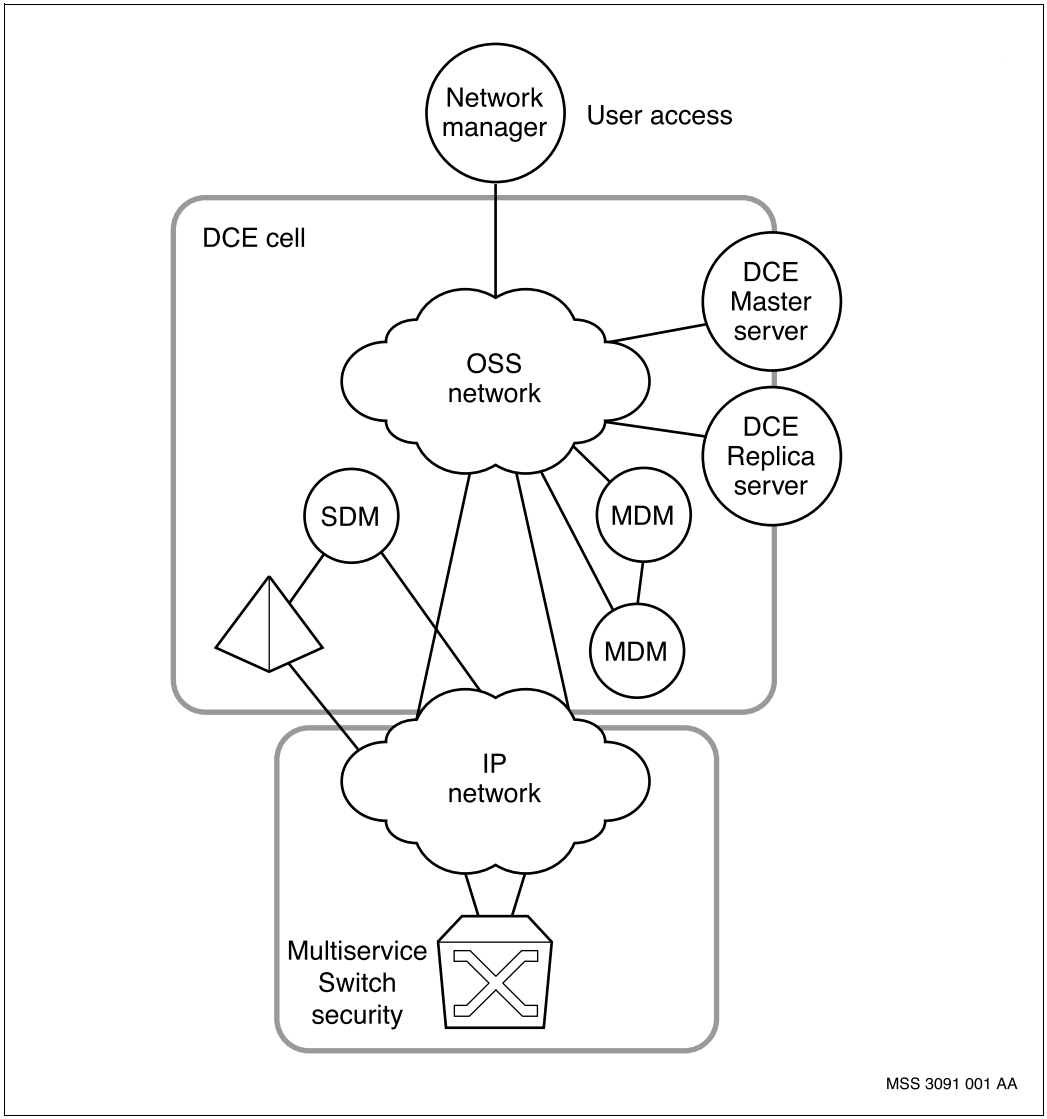
DCE is configured for integrated login, which means the operator need login to Unix only; the DCE login is automatic if the operator is authorized to enter the DCE cell. The administrator configures DCE authentication so that the operator's Unix user ID and password match a DCE user ID and password. Unix root access is a special case in which DCE authentication is always granted.

DCE availability

DCE authentication relies on communication with the DCE servers. If the DCE servers are not available, authentication halts and the operator, including the root user, cannot login to the server. Existing sessions are unaffected by this failure.

Normally, the network configuration includes a minimum of two DCE servers for redundancy.

Figure 2
Example of network configuration with DCE



Displaying DCE account profiles

Perform this procedure to display DCE user account profiles on the SDM application server.

Procedure steps

1 Start the dcecp tool.

```
dcecp
```

2 Display DCE user account profile specifics using the dcecp tool.

```
print show <userid>
```

The dcecp tool displays the account specifics. An example is shown below.

```
# dcecp
dcecp> print show ServProv
{fullname {ServProv Worker}}
{uid 117}
{uuid 00000075-3fdb-21d5-a600-2f09f436aa77}
{alias no}
{quota unlimited}
{groups 101}
```

3 Quit the dcecp tool.

```
quit
```

Variable definitions

Variable	Definition
<userid>	is the user ID you entered at step 3 in the section “Creating new user accounts using DCE” (page 33)

Changing your DCE operator account password

You can change your operator password for DCE using the Unix `passwd` utility. Use the following steps to change your operator account password.

Procedure steps

1. On the SDM application server, change your password using the Unix `passwd` utility. This utility changes both the Unix and the DCE passwords.
2. On each client workstation that you use, change your password using the Unix `passwd` utility.

Creating new user accounts using DCE

Creating a user account with integrated login involves creating a Unix account and DCE user account on the application server, and then a Unix account on all client machines that the operator has access to.

Note: The Unix user names and IDs must be the same as the DCE user names and ID for all platforms.

Use the following steps to create a DCE user account for an operator who requires integrated login.

Procedure steps

1. Start the `create_dce_user` tool on the SDM application server.

   `/sdm/bin/create_dce_user`

2. Enter the administrator user ID and password when prompted.
3. Enter the following information at the prompts:
   - **a.** user ID for the operator
   - **b.** full name of the operator
   - **c.** user group for this user ID
   - **d.** password for this user ID (re-type the password when prompted to confirm)

     Upon re-entering the password, the utility creates the DCE user account.

4 Create a UNIX account using the `admintool`. Create one of these accounts on the SDM application server and on each client workstation that the operator uses.

`admintool`

Note: You must have root privileges to create a Unix account.

5 Select add from the menu.

6 Enter the following information at the prompts:

a. user name

b. user ID

This ID is the value in the uid field when you display DCE account profiles. See step 2 in the section “Displaying DCE account profiles” (page 32).

c. user group

d. shell for this user ID

e. password

f. home directory

7 Select OK to complete the add operation.

Chapter 3
Preside MDM user access administration

Access to a server running Nortel Networks Preside Multiservice Data Manager (MDM) software requires UNIX user ID and password authorization. When the operator logs in with a valid user ID and password, the Preside MDM toolset is available.

User IDs, passwords, and permissions are managed through the Solaris admintool or through UNIX commands entered through an xterm window. Both the admintool and UNIX commands are described in the documents that come with the server platform and the Solaris operating system. For more information, see the *Sun Fire V480 Server Administration Guide* and the Solaris documentation.

The table "Explanation of the user IDs configured on the Sun Fire™ V480 servers" (page 35) lists all of the user IDs and passwords that were configured during the Preside MDM software installation. The names of the user IDs are recommended, but you can use your own names. As well, you will need to determine the passwords for all of your user IDs.

Table 4
Explanation of the user IDs configured on the Sun Fire™ V480 servers

Userid	Purpose	Group	Preside MDM user
root	Preside MDM root user		Yes
mdpadmin	administrative user ID for the MDP application	mdpgroup	Yes

(Sheet 1 of 2)

Table 4 (Continued)
Explanation of the user IDs configured on the Sun Fire™ V480 servers (Continued)

Userid	Purpose	Group	Preside MDM user
mdpprobe	probe user ID for the MDP application	mdpgroup	Yes
pp15ksw	user ID for the Multiservice Switch 15000 node Software Distribution Site		Yes
<>	surveillance and maintenance	mdmgroup	Yes
Note: The user ID mdm and its associated password (mdmpassword) are also used during this software installation. The mdm user ID must be defined on the Communications Server LAN and Multiservice Switch 15000 nodes during each of their software installations. This user ID and password are a suggested convention to follow, you can determine your own user ID and password if you wish.			
(Sheet 2 of 2)			

For more information, see the following sections:

- "Adding additional users" (page 36)
- "Adding additional groups" (page 37)
- "Configuring the root user as a Preside MDM user" (page 37)

Adding additional users

Perform the following procedure to add additional users to the system.

Procedure steps

1. Login to the Preside MDM server as the *root* user.
2. Add the new user:

   ```
   useradd -g <groupname> -d /localdisk/<userid> -m
   <userid>
   ```

   Note: The *useradd* command will create the new user's home directory.
3. Create a password for the new user:

   ```
   passwd <userid>
   ```

4. Enter a password for the new user at the prompt.

5 Make the new user a Preside MDM user:

```
/opt/MagellanNMS/bin/nmsuser <userid>
```

Variable definitions

Variable	Definition
<groupname>	is the group to which the new user belongs to.
<userid>	is the user's ID. This user ID must be unique.

Adding additional groups

Perform the following procedure to add additional groups to the system.

Procedure steps

Note: Do not perform this procedure on a system that is running disk mirroring.

1 Log in to the Preside MDM server as the *root* user.

2 Add a new group:

```
groupadd <groupname>
```

Variable definitions

Variable	Definition
<groupname>	is the name of the new group. This group name must be unique.

Configuring the root user as a Preside MDM user

A Nortel Networks Preside Multiservice Data Manager (MDM) user runs in the user environment provided with Preside MDM software. A Preside MDM user is able to access the default toolset. Perform the following procedure to configure the root user as a Preside MDM user.

Note: The root user is not typically configured as the Preside MDM user, but can be modified using this procedure.

1. Log in to the Preside MDM server as the *root* user.
2. Execute the following command:

   /opt/MagellanNMS/bin/nmsuser root

   Note: If you are running disk mirroring, or other systems that have customized root login scripts, you should not execute this command against the root user. It will replace the logon scripts with Preside MDM login scripts, and will result in other applications not working.
3. Verify the type of shell that is running on the server:

   echo $SHELL

   The system response lets you know which shell is being used: Bourne (`sh`), C-shell (`csh`), or Korn shell (`ksh`).
4. If the account is running Bourne or Korn shell: Right-click on the desktop and select File Manager from the menu to open the File Manager window

   If the account is running C-shell, go to step 11.
5. Click View to open another window.
6. Click Show hidden objects to ensure that the /.profile file is displayed.
7. Click on /.profile in order to open the folder. It may be necessary to scroll to the bottom of the window to find this folder.
8. Add text to the end of the /.profile file:

   . /opt/MagellanNMS/bin/nmssh

   /opt/MagellanNMS/bin/nmstool &

   Note: A space is required between the period and the slash in the command.
9. Save and close the .profile file using these options from the File menu.
10. Logout and then log back in to automatically restart the Preside MDM application.

    If the account is running Bourne or Korn shell, you are finished.
11. If the account is running C-shell, type the command:

    vi /.cshrc
12. Right-click on the desktop and select Files and then File Manager from the menu to open the File Manager window.

13 Perform step 5, step 6, and step 7, and then complete step 14.

14 Add text to the end of the /.profile file:

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

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

Note: A space is required between the word “source” and the slash in the command.

15 Save and close the .profile file using these options from the File menu.

16 Log out and then log in to automatically restart the Preside MDM application.

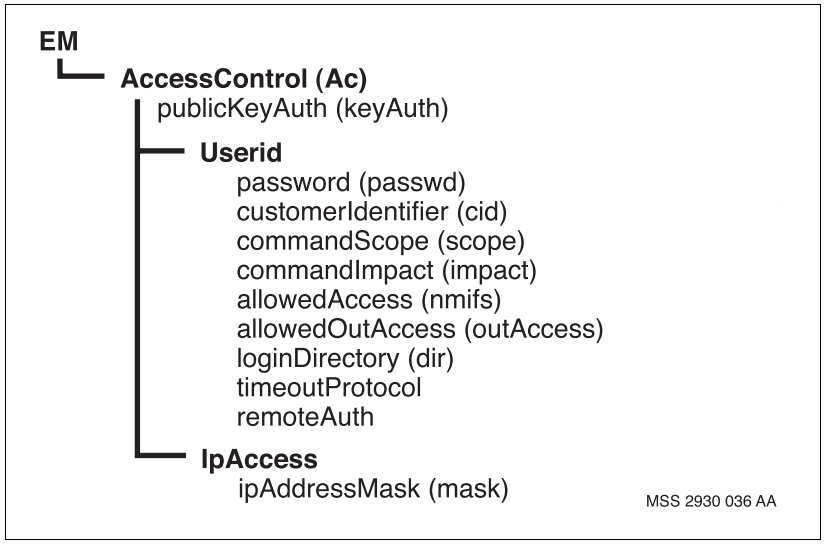
Note: After completing this procedure, you can launch the Preside MDM application on your desktop by entering the nmstool & command in a terminal window.

Chapter 4
Multiservice Switch user access administration

Nortel Networks Multiservice Switch access control restricts access to network nodes through user IDs, passwords, and authorized remote IP addresses. Operators must enter a valid user ID and password to access a node. Optionally, the operator may be required to access a node from a device with a specific IP address.

Access control is set through configuration of the *AccessControl* component (and its sub-components) on the node. The figure "Access control components and attributes" (page 42) summarizes the associated components and attributes.

Figure 3
Access control components and attributes



Access control configuration can be done through the following tools:

- Nodal Provisioning tool (see 241-6001-610 *Preside MDM Nodal Provisioning User Guide*)
- Command Console tool (see 241-6001-804 *Preside MDM Workstation Utilities User Guide*)

The table "Summary of user access tasks" (page 42) summarizes the OAM tasks required for node security and access.

Table 5
Summary of user access tasks

OAM tasks	Relevant section
Adding a new user (after initial installation and commissioning is complete)	"Adding a new user"
Using the profile of one user as the template for the profile of another user	"Copying an existing userID for a new user"

Table 5
Summary of user access tasks (Continued)

OAM tasks	Relevant section
Changing a user password	"Changing a password"
Setting a password using a secure method	"Setting a password using a secure method"
Changing a user profile	"Changing user attributes"
Deleting a user profile, including its ID and password	"Deleting a userID"
Note: All references in the Relevant section column are to the Configuring user access section of NN10600-605 *Passport - MDM Network Security: Operations*.	

For complete information on access controls, see all sections of NN10600-605 *Passport - MDM Network Security: Operations*.

For basic command line interface information, see "Command line interface basics" (page 43). For specific procedures for performing user access administration on nodes, see the following:

- "Adding a user using the CLI" (page 46)
- "Copying an existing user ID for a new user using the CLI" (page 48)
- "Adding an IPAccess component using the CLI" (page 50)
- "Setting a password using a secure method" (page 51)
- "Changing a user profile and password using the CLI" (page 53)
- "Deleting a user profile using the CLI" (page 54)

Command line interface basics

For information on the basics of Nortel Networks Multiservice Switch command line interface (CLI), see the following:

- "Logging into CLI" (page 44)
- "CLI operational mode" (page 44)
- "CLI provisioning mode" (page 45)

Logging into CLI

Follow these steps to log in to CLI. For user IDs and passwords, see the system administrator.

Procedure steps

1. Open an xterm window on a UNIX workstation or server that has LAN\WAN access to the node.
2. Start a local session on the node by using the xterm window.

   ```
   telnet <ip_addr> <port>
   ```

   Note: If a previous user has not logged out, the current user logs into the same session. The previous user must log out first.
3. Enter a valid user ID at the user ID prompt.
4. Enter the password at the password prompt.

   You are now logged into CLI operational mode.

Variable definitions

Variable	Definition
<ip_addr>	is the IP address or domain name of the terminal server.
<port>	is the port number for the link to the node.

CLI operational mode

Procedures contained within this document can either be performed in operational mode or provisioning mode. When you initially log into a Nortel Networks Multiservice Switch node, you are in operational mode. Multiservice Switch systems use the following command prompt when you are in operational mode:

```
#>
```

where:

is the current command number

In operational mode, you work with operational components and attributes. In operational mode, you can:

- list operational components and display operational attributes to determine the current operating parameters for the node
- control the state of parts of the node by locking and unlocking components
- set certain operational attributes and enter commands to perform diagnostic tests

CLI provisioning mode

To change from operational mode to provisioning mode, use the start Prov command. Only one user can be in provisioning mode at a time. Nortel Networks Multiservice Switch systems use the following command prompt whenever you are in provisioning mode:

```
PROV #>
```

where:

is the current command number

Note: The prompt does not change when you are using Preside MDM Command Console. To find out the mode, issue the ““network”” command.

In provisioning mode, you work with the provisionable components and attributes which contain the current and future configurations of the node. You can add and delete components, as well as display and set provisionable attributes. You can also verify your changes and then activate them as the new node configuration. To end provisioning mode and return to the operational mode, use the end Prov command.

For information on operational and provisionable attributes, see NN10600-060 *Nortel Networks Multiservice Switch 7400/15000/20000 Component Reference*.

Adding a user using the CLI

Perform this procedure in provisioning mode to configure a new user on the node.

Procedure steps

1 Add the *Userid* component:

```
add AccessControl Userid/<userID>
```

Note: StartUp adds the *AccessControl* component when you reset the control processor's software in StartUp.

2 Set the password:

```
set AccessControl Userid/<userID> password <password>
```

Note 1: Passwords are case-sensitive. After it is set, the password cannot be displayed.

Note 2: Ensure that the command recall buffers are cleared of the commands to set the password. See "Risks" (page 53).

3 Set the customer identifier (CID):

```
set AccessControl Userid/<userID> customerIdentifier
<identifier>
```

The CID is used in Customer Network Management (CNM) and limits the user to receiving commands from a CNM operator belonging to the same CID.

4 Set the command impact for the user:

```
set AccessControl Userid/<userID> commandScope <scope>
```

5 Set the command impact for the user:

```
set AccessControl Userid/<userID> commandImpact
<impact>
```

6 Set the allowed network management interfaces:

```
set AccessControl Userid/<userID> allowedAccess
<interface>
```

Review the following to determine which interface to use for each tool:

- serial port connection—local (for example, connection by terminal server, modem, directly connected terminals, PC and others)
- MDM application /user—FMIP (for example, Command Console)

- standard telnet—Telnet
- standard FTP—FTP

If you want to prevent access on an interface, you can type the interface name preceded by a tilde (~) character. For example, to allow access to all interfaces except FTP, enter the following:

```
set AccessControl Userid/<userID> allowedAccess local
fmip telnet ~ftp
```

7 Set the user's login directory for file system commands or FTP commands:

```
set AccessControl Userid/<userID> loginDirectory
<directory>
```

8 Verify the configuration of the new user:

```
display AccessControl Userid/<userID>
```

9 Verify that at least one user exists with system administration impact:

```
display AccessControl Userid/(commandImpact =
systemAdmin)
```

10 Complete the configuration changes. See "Completing configuration changes" in Configuration information.

Variable definitions

Variable	Definition
<userid>	On first reference, it identifies the new user you want to add and is from one to eight characters. On subsequent references, is the new user you just added.
<password>	Identifies the user's password from five to eight characters.
<identifier>	Is any number between 0 and 8191.

(Sheet 1 of 2)

Variable	Definition
<scope>	Identifies the importance of the components on which the user can perform the commands. The command scope is one of the following: • network, which means the user can adjust components that affect the operation of the network • device, which means that the user can adjust components that affect the operation of a Multiservice Switch module • application, which means that the user can adjust components that affect the operation of a single component. The command scope is automatically set to application if you do not enter this command In Succession Networks, Nortel Networks recommends always using a scope of "network". For more information on this attribute, see NN10600-606 *Passport - MDM Network Security: User Access Configuration*.:
<impact>	identifies the importance of the commands that the user can perform. Table 2, "Impact levels for Multiservice Switch 15000 nodes," (page 25) lists the impact levels that apply. The command impact is automatically set to passive if you do not enter this command.
<interface>	Identifies how the user will be allowed to access the node and limits the user to the specified interface types. The allowed network management interfaces must be one or more of the following: local, FMIP, Telnet or FTP. The allowed interface is automatically set to local if you do not enter this command.
<directory>	Is the directory where the user will be placed after logging into the node. This value is automatically set to "/" if you do not enter this command. "/" is the root directory.
(Sheet 2 of 2)	

Copying an existing user ID for a new user using the CLI

You can copy an existing user ID and all of its attributes, except password attributes. This is useful if you have a large number of user IDs that will have the same attributes except for the password. This technique reduces the need to specify attributes every time you add a new user. Once you copy a *userID*

component, you only need to change the password. If you want to change other attributes, see “Changing a user profile and password using the CLI” (page 53).

To copy an existing user ID, you must be logged in with a user ID with a command impact of *system Administration*.

Use the following procedure to copy an existing user ID. Perform the following steps in provisioning mode. For information on working in provisioning mode, see NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

Procedure steps

1. Copy the *userID* component:

   ```
   copy -s(Ac userID/<olduserID>) -d(Ac userID/
   <newuserID>) Prov
   ```

2. Set the password for the new user ID:

   ```
   set Ac userID/<newuserID> password <password>
   ```

   Note 1: When you set a password, it displays on the user interface. After it is set, the password cannot be displayed again.

   Note 2: Ensure that the command recall buffers are cleared of the commands to set the password. See “Risks” (page 53).

3. To change the attributes of the new *userID* component, use the *set* command.

Variable definitions

Variable	Definition
<olduserID>	Is the existing user ID
<newuserID>	Is the new user identifier. It must be one to eight characters.
<password>	Is the initial password for the new user identifier. It must be five to eight characters.

Adding an *IPAccess* component using the CLI

The *IpAccess* component is a security mechanism that applies to Nortel Networks Multiservice Switch node access using FMIP, FTP, and Telnet. It is not available for local or serial access. The *IpAccess* component prevents users from logging into a node from an unauthorized device by defining a list of devices that have permission to access the node. A device is specified by its IP address. You can specify an entire IP subnetwork using an IP address and a subnetwork mask. Adding an *IpAccess* component is optional. If you do not add this component all devices are permitted to access the node, regardless of their IP address. Perform this procedure in provisioning mode.

Procedure steps

1. Add an *IpAccess* component:

   ```
   add AccessControl IpAccess/<address>
   ```

2. To enable access to a subnetwork, set the subnetwork mask:

   ```
   set AccessControl IpAccess/<address> IpAddressMask
   <mask>
   ```

3. Verify the configuration of the *IPAccess* component:

   ```
   display AccessControl IpAccess/*
   ```

4. Complete the configuration changes. See “Completing configuration changes” in Configuration information.

Variable definitions

Variable	Definition
<address>	Is the IP address of the device that you want to be able to access the node
<mask>	Indicates which byte of the IP address to ignore when evaluating an incoming IP address. For example, setting the mask to 255.255.255.0 tells the node to ignore the last byte in the address. This allows all devices with its first three bytes identical to the IP address set in the previous step to access the node. The mask combined with the IP address defines a subnetwork.

Setting a password using a secure method

Use the following procedure to minimize the security risk when setting a password. It assumes that you have a physically secure node where you can make password changes and that you need to change a password on another, non-secure node. It also assumes that the user ID associated with the changed password exists on both the secure and the non-secure node.

Only the system administrator (with a user ID with a command impact of *systemAdministration*) can change a password.

Procedure steps

1. Log into a secure node. Access this node from a workstation in a physically secure area using a local VT100 session. You can also use a Telnet session as long as you use a secure connection. Do not establish a Telnet session across a public network.

2. Start provisioning mode.

   ```
   start Prov
   ```

3. Set the password.

   ```
   set Ac userID/<userID> password <password>
   ```

4. Save the *userID* component with the changed password.

   ```
   save -component(Ac userID/<userID>) -file(<name>) Prov
   ```

   Note: To save a partial view to the file system, use its complete name in the form <name>.part.<num>, where <num> is an automatically generated sequence number. The *save Prov* command responds with the complete name of the view, for example, UserRoot.part.001.

5. End provisioning mode.

   ```
   end Prov
   ```

6. Log out of the secure node to clear the command recall queue.

   ```
   logout
   ```

7. Transfer the partial saved view containing the *userID* component from the secure node to an non-secure node using FTP. You must use the complete name of the view, which is in the form <name>.part.<num>.

   Note: If the FTP session to transfer the view is not via an Preside MDM application such as Backup & Restore, do not use the same user ID since FTP does not have a secure login mechanism.

a. Transfer the partial saved view from the secure node to a workstation using FTP. You can find the partial saved view you created in the /provisioning directory of the node.

b. Transfer the partial saved view from the workstation to the non-secure node using FTP. Put it in the /provisioning directory.

8 Log into the non-secure node using Preside MDM Command Console tool.

9 Start provisioning mode.

```
start Prov
```

10 Load the partial saved view.

```
load -file(<viewname>) Prov
```

11 Verify that the provisioning changes you have made are acceptable.

```
check Prov
```

Correct any errors, then verify the provisioning changes again.

12 If you want these changes as well as other changes made in the edit view to take effect immediately, activate and commit the provisioning changes.

```
activate Prov
confirm Prov
commit Prov
```

For more information, see NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

13 End provisioning mode.

```
end Prov
```

Variable definitions

Variable	Definition
<userID>	Is name of the user ID for which you are setting the password, or the name of the user ID with the changed password.
<password>	Is the new password. The password must be five to eight characters.

(Sheet 1 of 2)

Variable	Definition
<name>	Is a descriptive name for the partial saved view.
<viewname>	Is the complete name of the partial saved view, which is in the form <name>.part.<num>.
(Sheet 2 of 2)	

Risks

When setting an initial password for a user or changing an existing password, there are the following security risks:

- The actual characters of the password appear on the user interface.
- When you are using a session type other than local, the password travels over the network in easy-to-read ASCII format. Even local sessions transmit passwords in ASCII format if the connection is made using a terminal server.
- Local and Telnet sessions have a command recall queue, which stores the last 10 commands. The command in which you set the password can be recalled from the queue using the Up-Arrow and Down-Arrow keys.
- After setting passwords, ensure that the command recall buffers are cleared of such commands.

Changing a user profile and password using the CLI

Individual users cannot change their own profile or password. Only the system administrator (with a user ID with a command impact of *systemAdministration*) can change a profile or password.

When you change a password, the actual characters of the password appear on the user interface. To keep passwords private, make sure your workstation is in a secure area before changing a password. For more information on password security, see “Setting a password using a secure method” (page 51) and “Risks” (page 53).

Use the following procedure to change the user attributes of an existing *userID* component. The following procedure needs to be performed in provisioning mode. For information on working in provisioning mode, see NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

Procedure steps

1 Change the attributes of the *userID* component:

```
set Ac userID/<userID> <attribute> <value>
```

2 Set the password:

```
set Ac userID/<userID> password <password>
```

Variable definitions

Variable	Definition
<userID>	Is name of the user ID with the attributes to be changed.
<attribute>	Is any attribute of the *userID* component.
<value>	Is any valid value for the chosen attribute
<password>	Is the new password. This password must be five to eight characters.

Deleting a user profile using the CLI

To delete a user, you must be logged in with a user ID with a command impact of *systemAdministration*.

Perform the following command in provisioning mode. For information on working in provisioning mode, see NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

Procedure steps

1 Remove the *userID* component:

```
delete accessControl userID/<userID>
```

Variable definitions

Variable	Definition
<userID>	Is the user ID to be deleted.

After the user profile is deleted, the system ensures that at least one user ID still exists with a minimum of system administration impact. After the user profile deletion is activiated, active user sessions that employed that user ID are permitted to stay logged in. After these user sessions end by logging out, subsequent logins will require the use of a different user ID.

Chapter 5
Using the Network Model tool to perform network surveillance

For information on performing network surveillance using Nortel Networks Preside Multiservice Data Manager (MDM) Network Model tool, see the following sections:

- “Collecting and applying network module data” (page 57)
- “Configuring the Ethernet links in the network model” (page 61)
- “Copying the network model from one Preside MDM server to another” (page 62)

Collecting and applying network module data

To collect the data about network components and apply this data to your network model, perform the following procedure.

Procedure steps

1. Enter edit mode in the Network Viewer. See the section on entering edit mode in 241-6001-015 *Preside MDM Network Model Administrator Guide*.
2. Create a new organization called *Succession* within the network model. See the section on creating an organization in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Set the . . .	to . . .
Organization type	Generic
Organization name	Succession

3 Create a new region called *Succession* within the Succession organization. See the section on manually creating components and subcomponents in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Set the . . .	to . . .
Node Name	Region/Succession
Parent	Generic/Succession

4 Create a new site called *MDM* and then sites for the Multiservice Switch 15000 nodes using the office identifier (for example, the CS2000 site name). Make one site for each of the offices that will contain a node within the Succession Network office. See the section on manually creating components and subcomponents in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Set the . . .	to . . .
Node Name	Site/MDM Site/office1, office2, office3 Site/OTHER
Parent	Region/Succession

5 Click *Close* to close the *Create/Edit Component* dialog.

The two sites and the nodes representing the Preside MDM servers and the Succession offices are visible in the *Network Viewer* window.

6 Collect the network module data. See the section on collecting the network module data in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Set the . . . to . . .

Collection Name	<customer defined>
Equipment Type	Multiservice Switch
Passport Group	ACCESS
User ID	<mssuserid>
Password	<msspassword>

Options that must be activated:

Collect all Modules under Group

Complete Collection

Collect Customer ID Data

Notify Upon Completion

Note: Wait for the collection of network module data to finish before continuing with the next step of this procedure.

7 Create a new node for the Succession Network component. See the section on manually creating components and subcomponents in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Set the . . .	to . . .
Node Name	GEN/<name of Succession component>
Parent	Site/OTHER
MG4000	GEN/MG4K-<SPMID>-<CLLI>
SAM21	GEN/SAM-<SPMID>-<CLLI>
UAS	GEN/UAS-<SPMID>-<CLLI>
XA-Core	GEN/CS2K-<SPMID>-<CLLI>
MG9000	GEN/MG9K-<SPMID>-<CLLI>
IWSPM	GEN/IWSPM-<SPMID>-<CLLI>
DPTSPM	GEN/DPTSPM-<SPMID>-<CLLI>
CSLAN (if Passport 8600)	PP8600/<name>
CSLAN (if not Passport 8600	BB/CSLAN-<CLLI>
OAM LAN	BB/OAM_LAN

8 Click *Close* to close the *Create/Edit Component* dialog.

The new node is visible in the *Network Viewer* window.

9 Apply the collection data to your network model. See the section on applying collection results to the Network Model in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

10 Drag and drop all the remaining device icons (Multiservice Switch 15000, Passport 8600, Media Gateway 15000, MDM) to the

appropriate site: the icon representing the Preside MDM servers onto the *MDM* site, and the icons representing the Multiservice Switch and Media Gateway nodes onto the correct Succession Network office site. See the sections on assigning modules to sites and sites to regions, and moving new components into sites in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Note: Media Gateway 15000 nodes are used only in UA - IP solutions.

11 Move the icons as required to create a functional layout.

12 Save the network model. See the section on saving and distributing network model files in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Note: You can save the network model under the same name if you do not want to create a history of versions. If you do want a history of versions, save it under a different name, but ensure that you clean up the saved network models regularly.

Configuring the Ethernet links in the network model

Perform the following procedures to configure the Ethernet links that Nortel Networks Preside Multiservice Data Manager (MDM) does not add automatically. You can find all the sections referenced in the following procedure in the 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Procedure steps

1 Enter edit mode In the Network Viewer. See the section on entering edit mode to enable editing in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

2 For each of the Multiservice Switch 15000 nodes, create Ethernet links between the node and the Communications Server LAN (CS LAN). See the section on using menu commands to create and edit links in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Set the . . .	to . . .
Link Type	EL - for ethernet link
Component	EM/<name of the CS LAN> LA/<the LanApplication component instance value>
Component	EM/<name of the Multiservice Switch 15000 node>

3 For the CS LAN, create Ethernet links between the node and Preside MDM servers. See the section on using menu commands to create and edit links in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Set the . . .	to . . .
Link Type	EL - for Ethernet link
Component	EM/<name of the CS LAN> LA/<the LanApplication component instance value>
Component	NMS/<name of the Preside MDM server>

4 Configure the link between the BB/CSLAN and BB/OAM_LAN.

5 Save the network model. See the section on saving and distributing network model files in 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Note: You can save the network model under the same name if you do not want to create a history of versions. If you do want a history of versions, save it under a different name, but ensure that you clean up the saved network models regularly.

Copying the network model from one Preside MDM server to another

Perform the following procedure to copy the network model from one Nortel Networks Preside Multiservice Data Manager (MDM) server to another.

Procedure steps

1 Login to the second server:

```
telnet <MDM_name>
```

2 Enter the root user ID and the root password at the prompt.

3 Change directories to the */opt/MagellanNMS/data/model/nmf/* directory:

```
cd /opt/MagellanNMS/data/model/nmf
```

4 Make the directory that will contain the model:

```
mkdir /opt/MagellanNMS/data/model/nmf/<modelname>
```

5 Change directories to the newly created model directory:

```
cd <modelname>
```

6 Change the permissions of the directory so that all users can write to it:

```
chmod a+rwx .
```

7 Connect to the first server using the file transfer protocol (FTP):

```
ftp <privmdm1>
```

8 Enter the root user ID and the root password at the prompt.

9 Change directories to the */opt/MagellanNMS/data/model/nmf/<modelname>* directory:

```
cd /opt/MagellanNMS/data/model/nmf/<modelname>
```

10 Transfer the model files from the first server to the second server:

```
get instances.nidf
get instances.lidf
get instances.oidf
```

Note: Do not copy the *instances.image* file if it is present. This is the fast load format file which is not portable.

11 Close the FTP connection to the first server:

```
quit
```

12 Activate the network model on the second server:

```
makecurrent <modelname>
```

13 Commit the network model on the second server:

```
commitmodel <modelname>
```

14 Close the Telnet connection to the second server:

```
exit
```

Variable definitions

Variable	Definition
<MDM_name>	Is the name of the second Preside MDM server
<modelname>	Is the name of the model. In the example, the model name is Succession.
<privmdml>	Is the host name of the interface on the top port (qfe0) of the 4-port Ethernet card on the first Preside MDM server

Chapter 6
File Management on the Preside MDM server

The basic strategy for managing files on Nortel Networks Preside Multiservice Data Manager (MDM) servers is to set appropriate file retention times using the various tools provided by Preside MDM. Determination of appropriate retention times must consider the amount of Preside MDM disk space available for storing files.

For more information on recommended disk partition sizes for Preside MDM server configurations, refer to NN10028-111 *Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP*.

For more information on managing various types of files stored on Preside MDM servers, see the following sections:

Managing retention times for MDP files

File retention times for MDP data files are managed using the Disk Manager in the MDP Configuration tool. When the Disk Manager is selected from the MDP Configuration tool menu, a list of data files and retention times is displayed for editing.

Perform the following procedure to change MDP data file retention times.

Procedure steps

1. Login in to the server.
2. Using the MDP Configuration tool, select the **Disk Manager** from the tool menu.

   The **Disk Manager Configuration** window opens with a list of files and current retention times.
3. Review the file retention times and edit as required.
4. Click on **Save** to save the changes to the configuration file.

For more information, refer to "Configuring data file retention" in 241-6001-309 *Preside MDM Management Data Provider User Guide*.

Managing retention times for historical alarm files

The collection and storage of short-term alarms is done by the real-time alarm collection server (RTACCOL). Each day, RTACCOL creates a file for the collection of alarms and stores this file in the directory defined in the RTAC.cfg configuration file.

Perform the following procedure to start the RTACCOL server with a specified file retention time of 30 days.

Procedure steps

1. Login in to the server.
2. Open a Preside MDM window by entering the following:

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

   The copyright dialog and the window opens.
3. Click **OK** to close the copyright dialog.
4. From the window, select **System** -> **Administration** -> **Server Administration**.

   The **Server Administration** window opens.
5. From the Security pull-down menu, select **Authorize**.

   The **SVM Enter Authorization Password** dialog opens.

6 Enter the password into the **Password** field and click **OK**.

7 Select the **Real Time Alarm Col** from the list of servers.

8 From the **Options** menu, select **Stop**.

Note: The server must be in **Running** or **Exited** state before it can be stopped.

In the server list, the server's state changes to stopped. In the activity log, a log appears showing the time and date at which the server was stopped.

9 From the Edit pull-down menu, select the **Edit** server.

The **SVM Edit Server** dialog opens, displaying the current information for the server.

10 If the "-filecleanup 30" option is not specified, append it.

11 Click **Save and Restart**.

For more information on using the Server Administration tool, refer to 241-6001-303 *Preside MDM Administrator Guide*. For more information on the RTACCOL server, refer to 241-6001-310 *Preside MDM Server Reference Guide*.

Managing temp PMSP files

Perform the following procedure to create a cron job that will remove the temp PMSP files that have been stored on the system for more than a day. This cron job is set to perform daily file removal.

Procedure steps

1 Login to the server as the *root* user.

2 Set the EDITOR environment variable to use the vi editor when creating the cron job:

```
EDITOR=vi; export EDITOR
```

3 Create a cron job that will regularly remove the saved PMSP files:

```
crontab -e
```

The cron file is opened with a text editor.

4 Add the following information to the cron file:

```
30 0 * * * (cd '/opt/MagellanNMS/data/pmsp'; /bin/rm
`find . -name "*.csv" -mtime +1 -print`)
```

5 Save and close the cron file.

Managing the 5-minute network traffic management files

Perform the following procedure to create a cron job that will remove the 5-minute Network Traffic Management (NTM) statistics files that have been stored on the system for more than 5 days. This cron job is set to perform daily file removal.

Procedure steps

1 Login to the server as the *root* user.

2 Set the EDITOR environment variable to use the vi editor when creating the cron job:

```
EDITOR=vi; export EDITOR
```

3 Create a cron job that will regularly remove the saved NTM statistics files:

```
crontab -e
```

The cron file is opened with a text editor.

4 Add the following information to the cron file:

```
50 0 * * * (cd '/opt/MagellanNMS/data/pmsp'; /bin/rm
`find . -name "*.FIVE.CSV" -mtime +5 -print`)
```

5 Save and close the cron file.

Managing the 30-minute network traffic management files

Perform the following procedure to create a cron job that will remove the 30-minute Network Traffic Management (NTM) statistics files that have been stored on the system for more than 10 days. This cron job is set to perform daily file removal.

Procedure steps

1 Login to the server as the *root* user.

2 Set the EDITOR environment variable to use the vi editor when creating the cron job:

```
EDITOR=vi; export EDITOR
```

3 Create a cron job that will regularly remove the saved NTM statistics files:

```
crontab -e
```

The cron file is opened with a text editor.

4 Add the following information to the cron file:

```
40 0 * * * (cd`/opt/MagellanNMS/data/pmsp`; /bin/rm
`find . -name "*.THIRTY.CSV" -mtime +10 -print`)
```

5 Save and close the cron file.

Chapter 7
Preside MDM software backup, restore, and synchronization

Configuring a Succession Network with redundant paired Nortel Networks Preside Multiservice Data Manager (MDM) workstations, and using good backup policies, provides the most reliable method of maintaining surveillance data flow and access to network management tools in the event that a Preside MDM workstation experiences a service outage.

For more information about software backup, restore, synchronization, and the ability to recover workstations, see the following sections:

- "Types of data on a Preside MDM workstation" (page 72)
- "Understanding impacts of Preside MDM workstation outages" (page 76)
- "Backing up and restoring Preside MDM workstation software" (page 78)
- "Synchronizing Preside MDM workstations" (page 80)

Types of data on a Preside MDM workstation

Nortel Networks Preside Multiservice Data Manager (MDM) workstations maintain several types of data.

Preside MDM dynamic data

Dynamic data consists of:

- active Nortel Networks Multiservice Switch and Preside MDM alarms
- Multiservice Switch and Preside MDM network element states used by the network model

This memory-based information changes from one moment to the next so it cannot be simply protected by a backup strategy.

Preside MDM collected data

Collected data is collected from Nortel Networks Multiservice Switch nodes that are managed by Preside Multiservice Data Manager (MDM) workstations. Preside MDM collected data includes:

- performance data such as 5 and 30 minute performance management (PM) data
- historical alarms collected to support the Query Historical Alarms application
- Multiservice Switch service data
- processed Multiservice Switch spooled data such as log files, historical alarms and state change notices (SCNs)

Performance management data is collected in real time and is not protected by any backup strategy. Redundant pair workstations do not synchronize this information. The downstream higher level management systems or OSS applications deal with any redundant data feeds.

Alarm data is collected in real-time and stored in files for use by the Query Historical Alarms application. Because of the real-time nature of the data, it cannot be protected by any backup strategy. Redundant pair workstations do not synchronize this information.

In Succession Networks, Multiservice Switch service data is static. Multiservice Switch backup data on a Preside MDM workstation is synchronized with the node. If the node backup data stored on the workstation is suspect, then a node backup should be re-executed for each node in the network.

> ***Note:*** Only one of the redundant pair of Preside MDM workstations can be configured to act as the backup site for the Multiservice Switch nodes in the network. For more information, refer to "Multiservice Switch software backup and restore" (page 83).

Multiservice Switch spooled data is synchronized with the nodes. If a Preside MDM workstation is out of service, the spooled data remains on the node until the workstation is recovered. At this time, the node spools the data to the workstation.

Preside MDM configuration data

Configuration data is created when you configure a Nortel Networks Preside Multiservice Data Manager (MDM) workstation and make subsequent changes. Configuration data includes:

- Preside MDM services
- the network model that includes the Network Elements (NEs) and their subcomponents. Note that the network model active states are retained in the memory-based model.

In a Succession Network solution, Preside MDM configuration data is static and can be protected with a good backup procedure.

Generally the network model data only changes when new Nortel Networks Multiservice Switch nodes or subcomponents are added to the network, or when you introduce a new feature on the workstation. This data needs to be synchronized with other Preside MDM workstations.

UNIX configuration data and core software

UNIX configuration data consists of the specific UNIX configuration data set up at workstation initialization. It includes user IDs and passwords, user data, network host addresses, and cron jobs. This data is reasonably static and can

be protected with a good backup procedure. Since the data is local to each workstation, the data is not synchronized with other Nortel Networks Preside Multiservice Data Manager (MDM) workstations.

Cron files are used to support:

- seasonal time of day time change (**root crontab**)
- data collection by MDP (**mdpadmin crontab)**
- PMSP file management (**root crontab**)

  Note: It is essential that the crontab files are included in the workstation backup procedures so that they will be available during a workstation restore. These files are located in the directory **/var/spool/cron/crontabs**.

The UNIX core software consists of the Solaris operating system and Solaris configuration files. The configuration files are static and can be protected by a good backup procedure. The operating system can either be restored from backup or by other methods recommended by the supplier.

Preside MDM core software

Nortel Networks Preside Multiservice Data Manager (MDM) core software is provided for a client-set workstation configuration or a server-set/stand-alone workstation configuration which functions as both a client and a server. Preside MDM software is static and can be protected with a good backup procedure. The software can be restored from backup or from the supplied source files.

"Data mapping for Preside MDM workstation configurations" (page 75) shows the data relevant to each type of Preside MDM workstation configuration.

Table 6
Data mapping for Preside MDM workstation configurations

Server-set / stand-alone workstation	Client-set workstation
Preside MDM dynamic data • Preside MDM and Multiservice Switch alarms • network model states	
Preside MDM collected data • 5 and 30 minute performance measurements • Alarms to support the Query Historical Alarms application • Multiservice Switch backup and restore data • Processed Multiservice Switch spooled data	
Preside MDM configuration data • Preside MDM services • network model	
UNIX configuration data and core software • user Ids and passwords • network host addresses • user data • cron files • Solaris operating system and configuration files	UNIX configuration data and core software • user Ids and passwords • network host addresses • user data • cron files (seasonal time of day change only) • Solaris operating system and configuration files
Preside MDM core software • server-set software • client-set software	Preside MDM core software • client-set software

Understanding impacts of Preside MDM workstation outages

When two Nortel Networks Preside Multiservice Data Manager (MDM) workstations are running in redundant pair mode, the data between the two must be kept consistent so that each can continue to provide network surveillance data and network management functions if the other one experiences an outage. The operational workstation will continue to feed data to the higher level management system and to the OSS, and to collect data from Nortel Networks Multiservice Switch nodes.

Types of outages

A simple outage is one where the workstation is out of service for a short period of time, there is no loss of hard disk data, and no changes have been made to the operational workstation during the outage. Examples of simples failures are power outages, and workstation rebooting.

A complex outage is one that either forces the restore of disk data due to a disk failure, or the Preside Multiservice Data Manager (MDM) administrator is unsure if changes have been made to the operational Preside MDM workstation and not applied to the out of service workstation.

“Impacts of workstation outages on Preside MDM data” (page 76) lists the impacts of workstation outages on Preside MDM data.

Table 7
Impacts of workstation outages on Preside MDM data

Data type	Impact to data
Preside MDM dynamic data	Active alarms and network model states are lost. The data will automatically resynchronize with the operational Preside MDM workstation data after the workstation is rebooted. [1]
Preside MDM collected data	
• 5 and 30 minute PMs	5 and 30 minute PMs will have a gap for the PM records generated during the out of service period. The data cannot be recovered.
(Sheet 1 of 2)	

Table 7 (Continued)
Impacts of workstation outages on Preside MDM data

Data type	Impact to data
• Preside MDM backup data	For a simple outage, there is no impact to Multiservice Switch backup data. For a complex outage, Multiservice Switch backup data is lost and must be restored from Preside MDM backup. [2]
• Historical alarms	Historical alarm data will have a gap for the alarms generated during the out of service period. The data cannot be recovered.
• Multiservice Switch spooled data	Multiservice Switch spooled data processing is deferred until the Preside MDM workstation has returned to service. Information will be retrieved from the node at the next collection interval.
• Preside MDM Configuration data	For a simple outage, no data is lost. For a complex outage, data is lost and must be restored from backup. Since the data is not synchronized with the operational Preside MDM workstation, changes since the last backup must be applied manually.
UNIX configuration data and core software	For a simple outage, no configuration data is lost, and there is no impact to the Solaris operating system. For a complex outage: • Configuration data is lost and must be restored from backup. Since data is not synchronized with the operational Preside MDM workstation, changes made since the last backup must be applied manually. • Solaris operating system software is lost and must be restored from backup or from supplier sources.
Preside MDM core software	For a simple outage, there is no impact to Preside MDM software. For a complex outage, the software is lost and must be restored from backup or from Preside MDM source files.

(Sheet 2 of 2)

Note 1: Synchronization between Preside MDM workstations takes place when the recovered workstation's GMDR service connects to the FMDRs of the operational workstation. The workstation will also

synchronize with Multiservice Switch nodes at this time, and any redundant data will be rejected. If both workstations were out of service, they will synchronize with the nodes.

Note 2: If Multiservice Switch service data was changed since the last backup, then a Multiservice Switch backup should be executed for each node in the network after the Preside MDM workstation is recovered.

Backing up and restoring Preside MDM workstation software

Back up strategies

There are two strategies for backing up data:

1 Treat the whole system as a single unit, and do system backups monthly with incremental backups on a weekly basis. If you are planning to use this strategy, it is advisable to get a third-party product designed to do backups.

2 Use the following logical splits, do selected backups on the data that changes, and retain an operating system backup to initiate the restore.

Preside MDM configured data

Using the “tar” command, backup the following set of files to a secure, offline storage location. Perform this task prior to any system migration. As this data is stable, backing it up weekly or monthly is sufficient.

- /opt/MagellanNMS/cfg
- /opt/MagellanNMS/data
- /opt/Nortel/EPIC/cfg
- /opt/Nortel/WMS/cfg
- /opt/Nortel/DVR/cfg
- /opt/MagellanMDP/cfg
- /opt/MagellanMDP/data

User data

Use the “tar” command to copy the following set of files to a secure, offline storage location. Perform this task prior to any system migration. As this data is stable, backing it up weekly or monthly is sufficient.

- /localdisk/~

Unix configured data

Use the “tar” command to copy the following set of files to a secure, offline storage location. Perform this task prior to any system migration. As this data is stable, backing it up weekly or monthly is sufficient.

- /etc/hosts
- /etc/passwd
- /var/spool/cron/crontabs

Unix core software

Use the ufsdump command to create a backup of the operating system partitions. Backing up on a monthly basis is sufficient. For the root partition to be correctly backed up, the workstations should be booted in single user mode, ensuring that the root partition is not being modified during the backup.

Restoring Preside MDM workstation software

Nortel Networks Preside Multiservice Data Manager (MDM) workstation software should be restored according to the instructions of the third-party product used to backup the software.

CAUTION

When restoring software to a Preside MDM workstation, make sure that a server-set/stand-alone workstation is restored only from the server-set/stand-alone backup, and a client-set workstation is restored only from the client-set backup.

Synchronizing Preside MDM workstations

A Nortel Networks Preside Multiservice Data Manager (MDM) workstation may be unavailable to the network for a short period of time such as in the case of a system re-boot, loss of network connectivity, or loss of power. As long as a disk restore was not required because of the outage, synchronization of the recovered workstation's dynamic data with the operational workstation's dynamic data is handled automatically. No administrator intervention is required to initiate the synchronization.

If the workstation outage requires a restore procedure to be performed to recover data, or if data changes have been made to the operational workstation during the interval that the recovered workstation has been out of service, the data on the two workstations may no longer match. In this case, the two workstations must be manually synchronized. Refer to "Restoring Preside MDM workstation software" (page 79).

Perform the following procedure to synchronize the recovered workstation with the operational workstation.

Note: This procedure should only be performed for server-set/stand-alone workstation configurations.

Note: Refer to "Impacts of workstation outages on Preside MDM data" (page 76) to review the data that will be synchronized by this procedure.

Procedure steps

Before performing the synchronization procedure, make sure that the recovered Preside MDM workstation has had the fault fully repaired, and that the workstation has been fully restored from the latest backup.

1. Login to the operational workstation as the *root* user.
2. Use the "tar" command to consolidate the following files on the operational workstation, and then copy them to the recovered workstation:
   - /opt/MagellanNMS/cfg/SVMList.cfg
   - /opt/MagellanNMS/cfg/HGDS.cfg
   - /opt/Nortel/DVR/cfg/dvrRes.txt
   - /opt/Nortel/PMR/cfg/pmrRes.txt

- /opt/MagellanNMS/cfg/ANP_Nodal.cfg
- /opt/MagellanNMS/cfg/DCS.cfg
- /opt/MagellanNMS/cfg/GMDR.cfg
- /opt/MagellanNMS/cfg/RTAC.cfg
- /opt/MagellanNMS/cfg/SFM.cfg

3 Use the procedure “Copying the network model from one Preside MDM server to another” (page 62) to synchronize the network model on the recovered workstation with the operational workstation.

4 Restart the recovered workstation:

```
sync; sync; sync; init 6
```

Note: The recovered workstation will connect immediately to the operational workstation and automatically synchronize and refresh the memory-based data (alarms and network states).

Chapter 8
Multiservice Switch software backup and restore

For more information about software backup and restore on Nortel Networks Multiservice Switch 15000 nodes, see the following sections:

Backup site creation

Configuring the backup site

Perform this procedure to configure Nortel Networks Preside Multiservice Data Manager (MDM) server as a Nortel Networks Multiservice Switch 15000 backup site.

> ***Note:*** Only configure the node backup site on the first Preside MDM server.

Procedure steps

1 Login to the server as the *root* user.

2 Add a new node backup user:

```
useradd -d /localdisk/ppbackup -m ppbackup
```

3 Create a password for the *ppbackup* user:

```
passwd ppbackup
```

4 Enter a password for the new user at the prompt.

5 Make the *ppbackup* user a Preside MDM user:

```
/opt/MagellanNMS/bin/nmsuser ppbackup
```

6 Login to the server as the *ppbackup* user.

7 Open the *PPBackup.list* file with a text editor:

```
vi $HOME/PPBackup.list
```

This file lists the Multiservice Switch 15000 nodes that the server needs to back up.

8 Add the following information to the *PPBackup.list* file:

```
-target <s1pp15k1> <s1pp15k2> <s1pp15k3>
```

9 Save and close the *PPBackup.list* file.

Variable definitions

Variable	Definition
<s1pp15k1>	is the name of the first Multiservice Switch 15000 node.
<s1pp15k2>	is the name of the second Multiservice Switch 15000 node.
<s1pp15k3>	is the name of the third Multiservice Switch 15000 node.

Configuring automatic backups to the backup site

When the Nortel Networks Multiservice Switch backup site is created, perform the following procedure to configure the automatic backups of the node data to this backup site.

Procedure steps

1 Login to the Preside MDM server as the *ppbackup* user.

2 Set the EDITOR environment variable to use the vi editor when creating the cron job:

```
EDITOR=vi; export EDITOR
```

3 Create a cron job that will perform the automatic backup of the nodes listed in the *PPBackup.list* file:

```
crontab -e
```

The cron file is opened with a text editor.

4 Add the following information to the cron file:

```
32 1 * * 0 /opt/MagellanNMS/bin/cmcwrap -gp
/opt/MagellanNMS/bin/pbackup -full -pds localhost
ppbackup <ppbackuppassword> -auth ACCESS mdm
<mdmpassword> -f $HOME/PPBackup.list >
$HOME/pbackup.log.`date +%Y%m%d`
32 1 * * 1-6 /opt/MagellanNMS/bin/cmcwrap -gp
/opt/MagellanNMS/bin/pbackup -pds localhost
ppbackup <ppbackuppassword> -auth ACCESS mdm
<mdmpassword> -f $HOME/PPBackup.list >
$HOME/pbackup.log.`date +%Y%m%d`
```

The first line of text added to the cron job tells the system to perform a full backup on Sundays at 01:32. The second line of text tells the system to perform an incremental backup every other day at 01:32.

5 Save and close the cron file.

Variable definitions

Variable	Definition
<mdm>	is the Preside MDM user ID that has yet to be defined on the Multiservice Switch 15000 nodes.
<mdmpassword>	is the password defined for the Preside MDM user ID.
<ppbackuppassword>	is the password defined for the ppbackup user ID.

Software backup

- “Backing up the current view using Service Data Backup/Restore tool” (page 86)
- “Backing up the current view using CAS” (page 87)

Backing up the current view using Service Data Backup/ Restore tool

The Service Data Backup/Restore tool enables you to copy service data and application version (AV) information from a Nortel Networks Multiservice Switch 15000 node to a reliable data storage site. The backup site can be a Nortel Networks Preside Multiservice Data Manager (MDM) server or another node. It can also be a Software Distribution Site (SDS) configured to store backed-up node service data. Performing a backup allows you to restore the node to its operational state.

Procedure steps

1. Login to the server if you are not already logged in.
2. Open a Preside MDM window by entering the following:

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

   The copyright dialog and the window opens.
3. Click *OK* to close the copyright dialog.
4. From the window, select **Configuration > Passport > Administration > Passport Service Data Backup/Restore**.

   The Backup and Restore window opens.
5. Select the **Backup Configuration** tab.

   The devices to be backed up are listed in the Device list area of the Backup Configuration panel.
6. If additional devices need to be backed up, click on the **Add** button to bring up the Add Device dialog window.
7. In the Add Device dialog window, select the Multiservice Switch group or the specific node to be backed up, fill in the default mode and authentication information, and click **OK** to return to the Backup Configuration panel.

   The devices to be backed up are listed in the Device list area.
8. From the **Mode** pull-down menu for each device, select either incremental, full or selective for the type of backup required.
9. Click **Backup**. To stop the backup, click **Cancel**.

   When the backup completes successfully, a message is displayed in the Message area. If the backup is unsuccessful, an error dialog is displayed that specifies the devices and the reason for the failure.

10 To exit the Backup/Restore tool, select **File > Exit** from the menu bar.

About local disk usage

The Service Data Backup tool uses the */tmp* directory to perform some of its file processing, for example, archive, compress, and uncompress. Your local disk needs to have twice the amount of space as the actual size of the files you are transferring for back up. You need to clean up the local disk if errors are raised (for example, *"No space left on device"*). In this case, you can mount the */tmp* directory from a lower-usage disk on a selected file server.

About backup site disk usage

The Service Data Backup tool transfers all back up files to the FTP home directory on the back up site. To change the directory for these back up files on the back up site, you need to re-configure the FTP home directory on the back up site. Contact your administrator for information on how to configure your FTP home directory.

Backing up the current view using CAS

To backup the current view using CAS, you need to make the current view the committed view and save this view to another location. Perform the following procedure in operational mode.

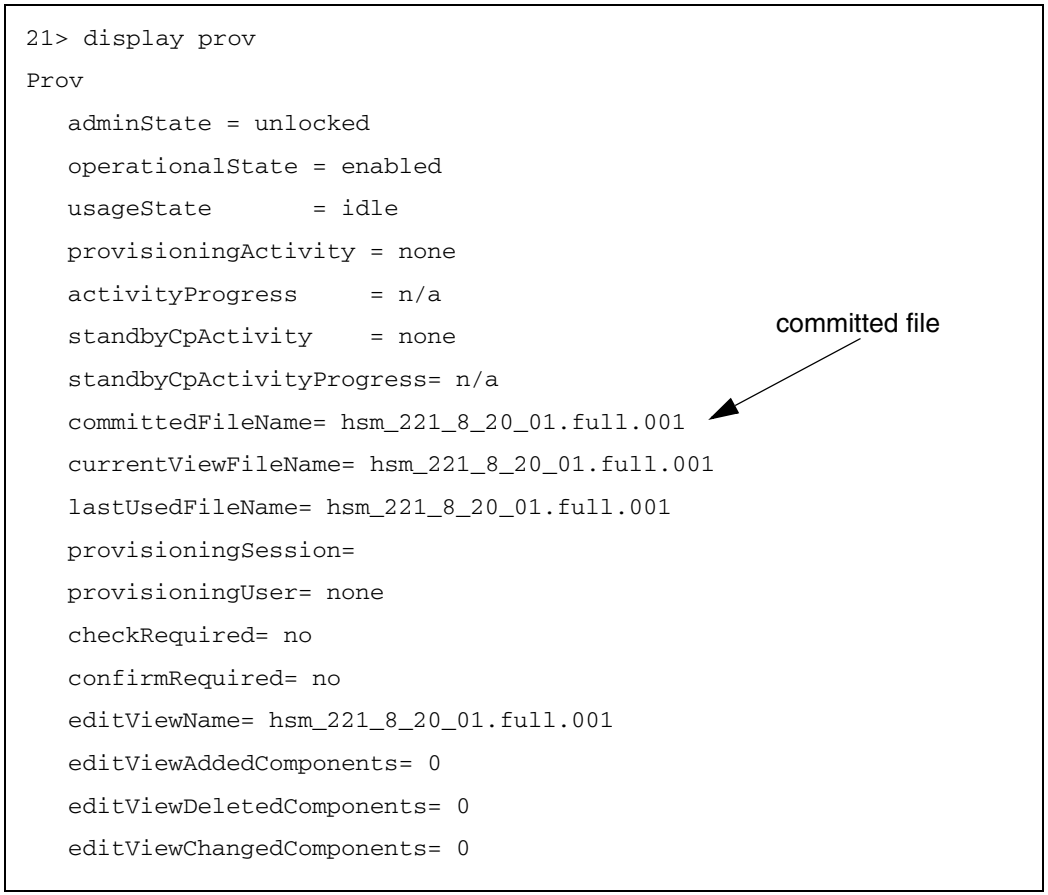
> ***Note:*** The Nortel Networks Preside Multiservice Data Manager (MDM) server has been configured to regularly backup the provisioning files from Nortel Networks Multiservice Switch nodes. By creating a backup of the committed file now, you ensure that you have the most current committed file you can have before beginning the migration.

Procedure steps

1 Display the committed view and the current view:

```
display prov committedFileName, currentViewFileName
```

Figure 4
Sample output



If the current view is the committed view, then the attribute values for the displayed attributes are the same.

2 If the current view is not the committed view, set the committed view to the current view:

commit prov

3 Verify that the provisioning changes you have made are acceptable:

check prov

The system responds with a warning that indicates that the processors may reboot when the new provisioning data is activated.

4 Save the current view with portable formats:

```
save -current -file(<filename>) -portable prov
```

5 Transfer the saved file to the server using the File Transfer Protocol.

Variable definitions

Variable	Definition
<filename>	is the name of the file in which the current view is saved.

Restoring software

When used:	Following corruption of a configuration view.
Scope:	Current configuration view.
Tools used:	Service Data Backup/Restore
Reference:	See 241-6001-807 *Preside MDM Network Backup and Restore*.

Using the Service Data Restore tool

Configuration files that have been backed up to the data storage site can be restored to the node using the Restore Configuration panel in the Service Data Backup/Restore tool. You complete a full restore based on the most recent backup or a specific time stamp, or you can restore specific views.

Chapter 9
Viewing command logs

Nortel Networks Preside Multiservice Data Manager (MDM) Data Viewer tool can be used to examine Nortel Networks Multiservice Switch 15000 command logs to audit node configuration changes.

Each node maintains a log of operator activities, such as logging in and out, password changes, and configuration changes. The File Prober tool transfers these logs to the Preside MDM server. File Prober is part of the Preside MDM Management Data Provider (MDP) application.

When a configuration change is activated on the node, the node raises a 7000 0007 SET alarm. When the activation is confirmed, the node raises a 7000 0007 CLEAR alarm. The SET and CLEAR alarms are sent to the higher level management system for insertion into the SCC2 data stream which is sent on to the OSS. These alarms can alert the OSS operator that configuration changes have been performed on the node.

Using information contained in the SCC2 alarm record, OSS operators with Preside MDM access can use the Data Viewer tool to examine the node's command log files for configuration operations. In particular, the information in the node's logs can be used to establish who performed the change and the nature of the change.

For more information on viewing command logs using the Data Viewer tool, see the following sections:

- "Viewing the command logs" (page 92)
- "Reading the command log" (page 95)

- "Obtaining the alarm timestamp and node identifier from the SCC2 record" (page 96)

Viewing the command logs

Perform the following procedure using Nortel Networks Preside Multiservice Data Manager (MDM) Data Viewer tool to view Nortel Networks Multiservice Switch 15000 command logs.

Note: Access to the command logs on the Preside MDM server is controlled by UNIX permissions on the MDP dump directories. Ensure that the permissions are set correctly so that the operator's user ID can access the directories.

For more information about using the Data Viewer tool, see 241-6001-031 *Preside MDM Performance Management User Guide*.

Procedure steps

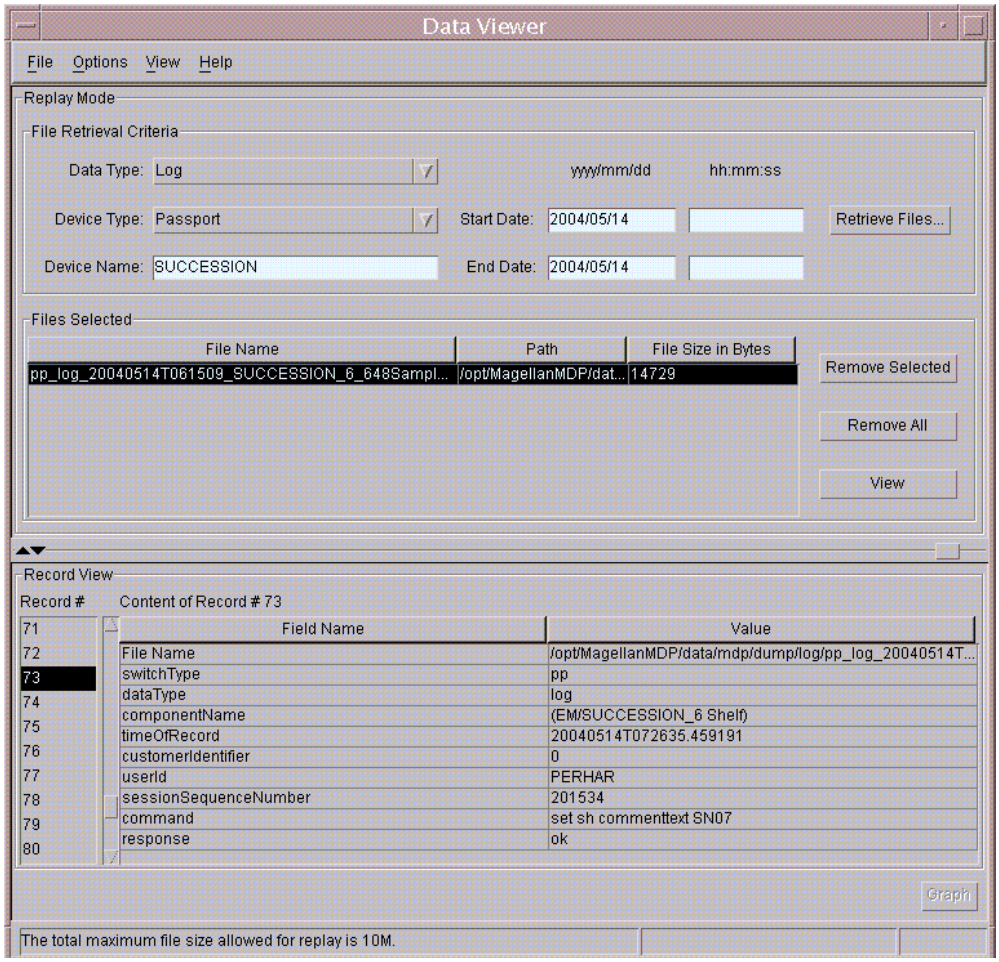
1. Log in to the Preside MDM server.
2. Open the **Data Viewer** tool from the tool launcher.

   From the window, select **Performance** and then select **Data Viewer** from the cascading menu.
3. In the Data Viewer screen, select **Options** from the menu bar. From the **Options** menu, select **Replay Mode**.

   Replay Mode brings up the Data Viewer window to allow you to replay data collected by the MDP.

   "Data Viewer window layout" (page 93) shows the layout of the Data Viewer Replay Mode Window for use in the following steps.

Figure 5
Data Viewer window layout



4 In the File Retrieval Criteria area of the Replay Mode window, complete the following actions:

a. From the **Data Type** pull-down menu, select **Log**

b. From the **Device Type** pull-down menu, select **Passport**

c. In the **Device Name** field, enter the name of the node that you recorded from the SCC2 log. This can be an exact match (e.g.

Succession6) or a partial wildcard (e.g. Succession*). Leaving the field blank is equivalent to a full wildcard search. (e.g. *)

d. Enter the start and end times of the interval to be viewed. The times provided by configuration change alarm records in the SCC2 data stream can be used to identify intervals of configuration activity. This will limit the file retrieval to the time period of interest. To obtain the start and end times from the SCC2 alarm record, see “Obtaining the alarm timestamp and node identifier from the SCC2 record” (page 96).

5 Click the **Retrieve Files** button.

The File Selection browser opens at the directory containing the log files: /opt/MagellanMDP/data/mdp/dump/log

6 In the browser window, select the files of interest and click on OK.

The Files Selected area of the Data Viewer window displays a listing of the files that you retrieved. The files are displayed in tabular format. You can click and drag a column heading to reorder the columns.

7 Select a file from the Files Selected section of the window. The log file data will appear in the Record View area of the window.

8 In the Record View area of the window, use the scroll bar to view the available command log records, and select the desired record for viewing.

The data fields for the command log record are displayed in the Record View area of the Data Viewer window.

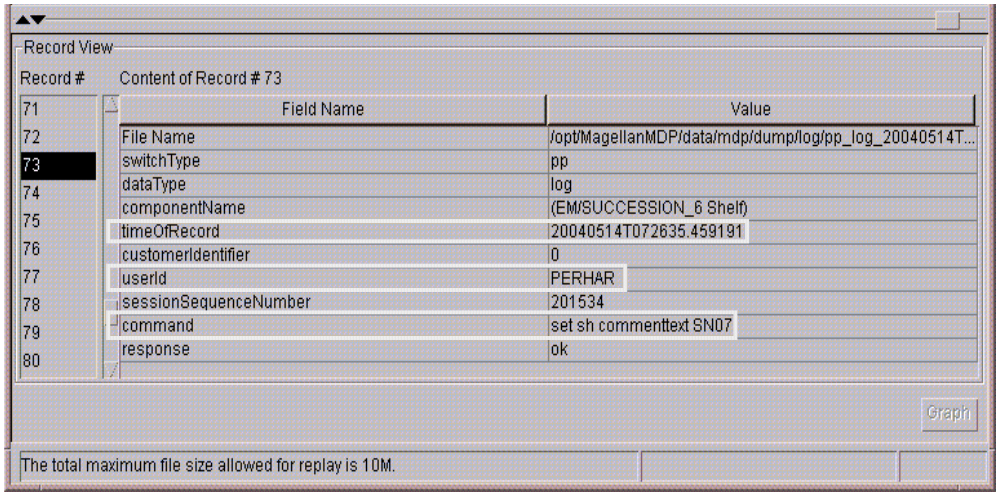
Refer to “Reading the command log” (page 95) to interpret the command log information.

Reading the command log

"Data Viewer window layout" (page 93) shows a sample command log. The following fields have been highlighted:

- timeOfRecord: the date and time the command log record was generated
- userid: the ID of the user who performed the command
- command: the command that was performed

Figure 6
Sample Command Log



For more information on the command log format, see 241-6001-810 *Preside MDM MDP Data Formats Reference*.

For a description of common operator commands and component-specific commands and responses, refer to the Nortel Networks Multiservice Switch documents.

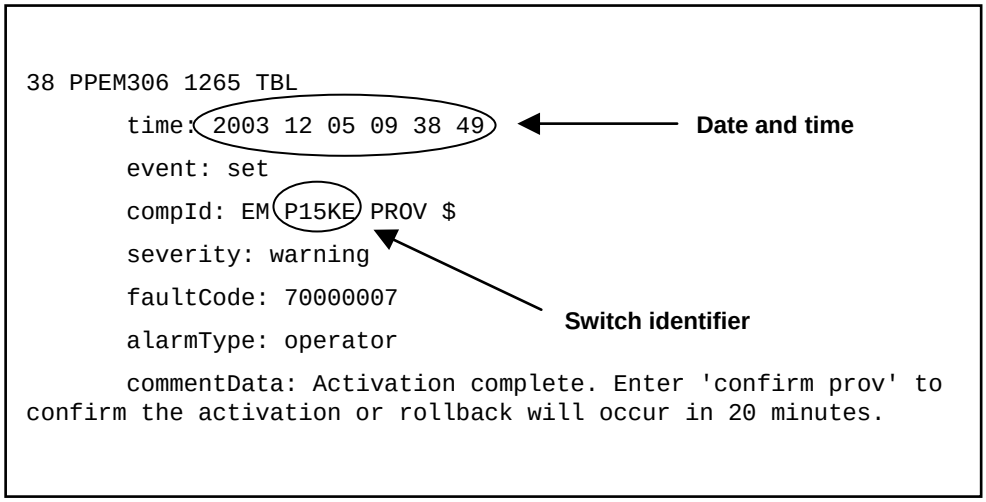
Obtaining the alarm timestamp and node identifier from the SCC2 record

Since the number of command logs received by Nortel Networks Preside Multiservice Data Manager (MDM) server can be large, information from the SCC2 record can be used to limit the search of the logs to a reasonable number. The timestamp of the alarm and the Nortel Networks Multiservice Switch 15000 node identifier contained in the SCC2 record for the 7000 0007 alarm can be used to select command logs for the time interval of interest.

Procedure steps

1. Locate the SCC2 log entry for the provisioning alarm.
2. Record the time of the alarm and the node identifier contained in the SCC2 log entry.

   A sample SCC2 log entry for a 7000 0007 alarm is shown below.



- The time field contains the date and time of the alarm (yyyy mm dd hh mm ss).
- The event field contains the SET/CLEAR values.
- The compID field contains the node ID and the component altered on the node. **EM** precedes the node ID.
- The faultCode field contains the alarm code.

For more information, see NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.

3 Use the time field to determine the start and end times for the set of command logs to be reviewed.

Note: Command logs are retrieved from nodes periodically by the MDP application. This collection interval is configurable for each node. Depending on the collection interval, there may be a delay between when the SET/CLEAR alarms are raised and when the log files arrives on the server. For more information on collecting data and scheduling data collection, see 241-6001-309 *Preside MDM Management Data Provider User Guide*.

Note: During normal disk maintenance, the MDP application will remove command log files. The recommended retention time is seven days. However, this interval is user configurable. If the logs are not viewed before the retention time has expired, the logs will have been lost For more information on setting the file retention time, see 241-6001-309 *Preside MDM Management Data Provider User Guide*.

Appendix
Preside MDM security and administration tools

Preside MDM security

Nortel Networks Preside Multiservice Data Manager (MDM) tools are password protected to protect Preside MDM configuration. Accessing a Preside MDM tool requires a valid user ID and password. The passwords are secured in the Server Administration tool by password encryption. Passwords are required to access the following tools and tasks:

- Network Model
- Service Selection
- GMDR Administration
- Server Administration
- Preside MDM userids
- Secure FTP daemon
- Command Console (for setting up Nortel Networks Multiservice Switch user IDs and passwords)

Multiservice Switch security log audits

Nortel Networks Multiservice Switch 15000 nodes maintain a log of operator activities, such as logging in and out, password changes, and configuration changes. The File Prober tool transfers these logs to Nortel Networks Preside Multiservice Data Manager (MDM) server. File Prober is part of Preside MDM Management Data Provider (MDP) application. Operators with

Preside MDM access can also use the Data Viewer tool to view the Security Logs by either using the Data Viewer GUI or the command line tool that can be invoked with a log file name as argument.

As a prerequisite, the MDP must be configured for BDF conversion of raw node data files.

Data Viewer tool

Accessible through:	Preside MDM window
Primary FCAPS scope:	security and performance management
Secondary FCAPS scope:	fault management
Where to find more information:	241-6001-031 *Preside MDM Performance Management User Guide*

The Data Viewer tool is used to display Nortel Networks Multiservice Switch node security logs. The log files are stored in the directory `/opt/MagellanMDP/data/mdp/dump/log` on both MDMs.

The Data Viewer tool is also a diagnostic tool that allows you to collect, display, and analyze performance information in real-time and replay modes.

For information on the Data Viewer tool, see 241-6001-031 *Preside MDM Performance Management User Guide*.

Solaris admintool

Accessible through:	UNIX command line: `admintool` (xterm window)
Primary FCAPS scope:	Preside MDM configuration and administration, security management
Secondary FCAPS scope:	none
Where to find more information:	Solaris product documentation

The Solaris admintool provides function for administering and maintaining workstation resources, such as CPU usage, disk and file administration, user permissions, and others.

Preside MDM administration tools

Administering Nortel Networks Preside Multiservice Data Manager (MDM) is performed by using the following tools and tasks:

Management Data Provider (MDP) Configuration tool

Accessible through:	Preside MDM window
Primary FCAPS scope:	security and administration
Secondary FCAPS scope:	performance
Where to find more information:	241-6001-309 *Preside MDM Management Data Provider User Guide*

In Succession Networks, Nortel Networks Preside Multiservice Data Manager (MDM) Management Data Provider (MDP) performs security log collection. MDP collects security logs from Nortel Networks Multiservice Switch nodes and then converts the data into an ASCII-based bulk data format (BDF).

Server Administration tool

Accessible through:	Preside MDM window
Primary FCAPS scope:	all
Secondary FCAPS scope:	none
Where to find more information:	Server Administration tool section in 241-6001-303 *Preside MDM Administrator Guide*

The Server Administration tool lets you monitor and control Preside MDM servers. The tool has two modes of operation, a view mode and an edit mode.

In view mode the tool lets you do the following:

- choose a host (workstation) on which to monitor or control Preside MDM servers
- select a server, then start it, stop it, or view its restart parameters
- print or refresh the contents of the main window

In edit mode, the tool lets you perform all of the tasks in view mode plus the following:

- select a server, then edit the startup command and automatic restart parameters for the server
- add or remove a server

The tool also displays a log of all server activity that has occurred since the last system restart.

GMDR Administration tool

Accessible through:	Preside MDM window
Primary FCAPS scope:	all
Secondary FCAPS scope:	none
Where to find more information:	GMDR Administration tool section in 241-6001-303 *Preside MDM Administrator Guide*

The General Management Data Router (GMDR) Administration tool lets you do the following to a GMDR server running on the local workstation:

- configure the GMDR server to collect surveillance data from the surveillance servers. The surveillance servers gather raw surveillance information from Nortel Networks Multiservice Switch 15000 nodes (FMDR) and from the MDM (IMDR).
- identify the servers that communicate with the GMDR on a workstation including the list of the FMDRs and IMDRs that receive workstation alarms (in a redundant configuration or deployment the FMDRs and IMDRs belonging to the other MDM workstations are also defined by the GMDR Administration tool)
- monitor connections between the GMDR server and the surveillance servers from which it collects surveillance data
- view and reset a GMDR database that contains statistics gathered by the GMDR server
- view a list of components and subcomponents that are being monitored by a GMDR server
- view logs about changes in the states of connections to the surveillance servers and about database resets
- trigger a state walk to obtain the current states of one or all Multiservice Switch modules that are managed by an FMDR server

Network Model

The Network Model stores a modeled view of the managed elements in the network and makes this view available to Nortel Networks Preside Multiservice Data Manager (MDM) tools. The Network Model provides applications with access to a repository of network state and configuration data. Element states calculated from network information and propagated throughout the network are essential to the Preside MDM fault management applications.

The Network Model is used to prepare accurate and efficient representations of the network, distribute workloads among network operators, and for network planning.

The Network Model is a database of your network's components, which stores a modeled view of the managed elements in a network and makes it available to the Preside MDM applications. The Network Model provides applications with access to network topology, as well as state and configuration data. You can use the Network Viewer to see your network model. The Network Model is useful when the network topology changes, typical during commissioning or when the network increases in size.

For more information on creating, maintaining, and deploying a Network Model, see the 241-6001-015 *Preside MDM Network Model Administrator Guide*.

Service Data Backup/Restore tool

Accessible through:	Preside MDM window
Primary FCAPS scope:	configuration and administration
Secondary FCAPS scope:	none
Where to find more information:	241-6001-807 *Preside MDM Network Backup and Restore*

The Service Data Backup/Restore is a stand-alone tool for backing up and restoring the service data on selected devices. A backup is required when the network topology changes, typically during commissioning and when the network increases in size. A restore is required on an as-needed basis. You can perform full, incremental, and selective backups and restores. Additionally, this tool can be used to back up and restore the committed view and journal log files in case the node fails or is destroyed. This functionality applies to Multiservice Switch equipment only. For more information, see “Backing up the current view using Service Data Backup/Restore tool” (page 86)

The current supported platform of the Service Data Backup/Restore tool is SPARC Solaris.

You can perform the following backup functions with Service Data Backup:

- full backup of service data for a single device or for multiple devices
- incremental backup of service data for a single device or for multiple devices

- backup of selected data for a single device or for multiple devices

You can perform the following node recover functions with Service Data Backup:

- recover and restore the current view
- restore the associated journal log files
- download the software and activate it so that the latest current view runs on the replacement node

You can perform the following restore functions with Service Data Restore:

- full restore of service data for a single device or for multiple devices
- incremental restore of service data for a single device or for multiple devices
- restore of selected service data for a single device or for multiple devices

Nodal Provisioning tool

Accessible through:	Preside MDM window
Primary FCAPS scope:	configuration and administration
Secondary FCAPS scope:	security management
Where to find more information:	241-6001-610 *Preside MDM Nodal Provisioning User Guide* and 241-6001-611 *Preside MDM Nodal and Service Provisioning Reference Guide*

Nortel Networks Preside Multiservice Data Manager (MDM) Nodal Provisioning tool is used to set up user IDs and passwords on Nortel Networks Multiservice Switch nodes. See 241-6001-610 *Preside MDM Nodal Provisioning User Guide* and 241-6001-611 *Preside MDM Nodal and Service Provisioning Reference Guide* for more information about the Nodal Provisioning tool.

Command Console tool

Accessible through:	Preside MDM window
Primary FCAPS scope:	fault management
Secondary FCAPS scope:	configuration and administration, performance management, and security management
Where to find more information:	241-6001-011 *Preside MDM Fault Management User Guide* and 241-6001-804 *Preside MDM Workstation Utilities User Guide*

Nortel Networks Preside Multiservice Data Manager (MDM) Command Console lets you access the Nortel Networks Multiservice Switch node command interface, and its corresponding command set. The Command Console can also be used for setting up user IDs and passwords on nodes using CLI commands.

System Log Display tool

Accessible through:	Preside MDM window
Primary FCAPS scope:	administration
Secondary FCAPS scope:	none
Where to find more information:	241-6001-303 *Preside MDM Administrator Guide* and 241-6001-310 *Preside MDM Server Reference Guide*

Nortel Networks Preside Multiservice Data Manager (MDM) System Log Display lets you display and print logs produced by Preside MDM servers, and by the actions of Preside MDM tools.

For information about the logs produced by the actions of Preside MDM tools, see 241-6001-303 *Preside MDM Administrator Guide*. For information about the logs produced by Preside MDM servers, see 241-6001-310 *Preside MDM Server Reference Guide*.

Preside MDM user IDs and passwords

Accessible through:	UNIX command line or Sun's admintool
Primary FCAPS scope:	administration
Secondary FCAPS scope:	security
Where to find more information:	241-6001-303 *Preside MDM Administrator Guide*

Creating a UNIX group dedicated to Preside MDM user accounts prevents unauthorized use of Preside MDM tools. The groupadd command or Sun's admintool can be used to create a UNIX group dedicated to Preside MDM users, and create new user accounts that run the default user environment provided with Preside MDM software.

Rebooting the Preside MDM server

Perform the following procedure to reboot Preside MDM servers.

1 Reboot the server:

```
sync; sync; sync; init 6
```

Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks

Security and Administration

PT-AAL1/UA-AAL1/UA-IP

(I)SN07

Publication: NN10180-611
Document status: Standard
Document version: (I)SN07S1
Document date: December 2004
Printed in Canada

NORTEL NETWORKS