NORTEL

Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks

Security and Administration

PT-AAL1/UA-AAL1/UA-IP

NN10180-611

Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks

Security and Administration

PT-AAL1/UA-AAL1/UA-IP

Publication: NN10180-611
Document status: Standard
Document version: (I)SN08 and up S1
Document date: June 2005

Printed in Canada

Publication history

May 2005

(I)SN08 and up S1 Standard
Contains standard information for the SN08 FVS release.

Contents

List of figures

List of tables

About this document

This document provides the procedures for performing security and administration tasks on Nortel Multiservice Switch 15000 / Media Gateway 15000 nodes in Carrier Voice over IP Networks. Most of these procedures can be performed using either Nortel Multiservice Data Manager (MDM) 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 Multiservice Data Manager (MDM) workstations and Multiservice Switch 15000 nodes in PT-AAL1 and UA-AAL1 Carrier Voice over IP Network solutions, and on Multiservice Data Manager workstations, Multiservice Switch 15000 nodes, and Media Gateway 15000 nodes in UA-IP Carrier Voice over IP 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 Carrier Voice over IP 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:

- NN10441-100 *PT-AAL2 Solution-level Basics*
- NN10443-100 *UA-AAL1 Solution-level Basics*
- NN10446-100 *Universal Access - IP Solution-level Basics (UA-IP)*
- NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP 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 Multiservice Switch 7400/15000/20000 Overview* and NN10600-700 *Nortel Multiservice Switch 7400/15000/20000 ATM Technology Fundamentals*.

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

- NN10600-605 *Nortel Multiservice Data Manager Network Security Fundamentals*
- NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*
- NN10600-607 *Nortel Multiservice Data Manager Network Security: Secure Communications Configuration*
- 241-6001-303 *Nortel Multiservice Data Manager Customization and Administration*

How this document is organized

This document contains a high-level description of Nortel Multiservice Data Manager (MDM) tools and tasks for performing security and administration functions on Nortel Multiservice Switch 15000 / Media Gateway 15000 nodes and Multiservice Data Manager workstations in Carrier Voice over IP

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

This document contains the following sections:

- "Mapping of Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000 access privileges to Integrated EMS groups in VoIP networks" (page 171)
- "IPSec administration procedures for VoIP networks" (page 179)

What's new in this document

The following features were added to this document:

- "Centralized user administration in an Operator Client environment" (page 20)
- "Security audit logs" (page 20)
- "New security features for VoIP networks" (page 21)

Centralized user administration in an Operator Client environment

In VoA networks, user administration through the MDM Admin Server allows you to assign access privileges to Operator Client users. You create user accounts and assign roles that restrict operator access according to access controls, set in configured policies. The policies are configured to limit access to specific tools and the ability to perform specific actions within specific tools. The Policy Manager defines the access that a user or role can have to the tools and the network. Multiple users and roles can be associated with a policy. See "Multiservice Data Manager centralized user administration in a VoA solution with the Operator Client application" (page 39).

Security audit logs

"Security audit logs" (page 87) was added to describe the security audit logs capability for VoA and VoIP networks. The security audit log collector (SALC) server on the Multiservice Data Manager server collects security logs from MSS/MG15000 nodes and the MDM workstation in real time, and stores them locally for later access using the Log Browser tool. For VoIP networks, the security audit logs are sent to the Integrated EMS. For VoA networks, the security audit logs are sent to the CS2000 Core Manager.

New security features for VoIP networks

The following sections were added or modified to provide information on operating a VoIP network that has the new security features in operation:

- "Centralized user access management using Integrated EMS" (page 61) provides information on the use of Integrated EMS to provide central authentication, authorization and accounting (AAA) service for Multiservice Data Manager workstations and MSS/MG15000 nodes.
- "Communications security management" (page 71) provides information on using IPSec and SSH security protocols to protect management data communications.
- "Platform security management" (page 83) describes the changes made to the Multiservice Data Manager and MSS/MG15000 platforms to secure them.
- "Multiservice Data Manager local user access administration" (page 103) had the following procedures modified or added:
  - "Adding additional local users" (page 105)
  - "Changing the password for a local userid" (page 106)
- "File Management on the Multiservice Data Manager server" (page 133) had the following procedures added:
  - "Managing MDM log files" (page 137)
  - "Managing MDM syslog files" (page 139)
- "Multiservice Data Manager software backup, restore, and synchronization" (page 141) has been modified to include disaster recovery information for workstations and switches secured in a VoIP network.
- Appendix "Summary of MDM tools and Operator Client application tools" (page 167) has been updated to summarize the MDM tools available through the MDM Toolset and Operator Client environments.
- Appendix "Mapping of Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000 access privileges to Integrated EMS groups in VoIP networks" (page 171) was added to provide information about mapping MDM and MSS/MG15000 access privileges onto Integrated EMS user groups.

- Appendix “IPSec administration procedures for VoIP networks” (page 179) was added to provide miscellaneous IPSec administration procedures.

Other changes to this document are listed below:

- “Local user access management” (page 31) provides information on the operation of userids defined locally to the Multiservice Data Manager and to the MSS/MG15000 node. This information previously resided in the Security and administration overview section.
- Chapter on “Viewing command logs” has been removed as it is no longer required. The Log Browser tool is now used to view security audit logs.
- The term Succession has been rebranded Carrier Voice over IP (CVoIP).
- The term Preside Multiservice Data Manager (Preside MDM) has been rebranded to Multiservice Data Manager (MDM) in conjunction with the new Nortel brand simplified naming format.
- Passport 8600 (PP8600) has been rebranded to Ethernet Routing Switch 8600 (ERS 8600).

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.

Multiservice Data Manager

- UPPERCASE, lowercase

  In Nortel Multiservice Data Manager (MDM), 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 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 Multiservice Switch 15000 / Media Gateway 15000 nodes or Nortel Multiservice Data Manager (MDM) servers:

- 241-6001-023 *Nortel Multiservice Data Manager Configuration Management Tools*
- NN10600-605 *Nortel Multiservice Data Manager Network Security Fundamentals*
- NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*
- NN10600-607 *Nortel Multiservice Data Manager Network Security: Secure Communications Configuration*
- NN10600-601 *Nortel Multiservice Switch 7400/15000/20000 Security Management*

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

- 241-6001-309 *MDM Management Data Provider User Guide*
- 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*
- 241-6001-015 *Nortel Multiservice Data Manager Network Model Administration*
- 241-6001-303 *Nortel Multiservice Data Manager Customization and Administration*
- 241-6001-810 *Nortel Multiservice Data Manager Management Data Provider Data Formats*
- NN10600-500 *Nortel Multiservice Switch 6400/7400/15000/20000 Alarms Reference*

How to get more help

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

Chapter 1
Security and administration overview

Note: For the purpose of this document, the term VoIP refers to UA-IP and PT-IP solutions only.

For overview information on security and administration, see:

- "Security management for Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000" (page 27)
- "Administration of Multiservice Data Manager servers and Multiservice Switches using Multiservice Data Manager" (page 30)

Security management for Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000

Security measures in a network are required to ensure the integrity and confidentiality of data. In particular, use of IP networks for transporting management data introduces additional risks.

MDM workstations and MSS/MG15000 switches can be protected by setting up good security practices and applying security measures to the following areas:

Platform security

In VoIP networks, securing the platform involves protection of the operating system and applications running on a workstation or switch. This can involve:

- controlling the remote systems that are allowed to access the node or workstation (MDM, MSS/MG15000)

- removing unused system functions (MDM)
- restricting access to critical system functions (MDM)
- using passwords to access system functions, and enforcing good password habits (MDM)
- monitoring user sessions and ending inactive ones (MSS/MG15000)

For more information, see “Platform security management” (page 83).

Communications security

Communications between MDM workstations and MSS/MG15000 nodes can be protected in various ways:

- FTP sessions between MSS/MG15000 nodes and MDM workstations utilize password authentication. For VoIP solutions, this feature should be disabled as IPSec is used to protect FTP sessions. For more information, see “Secure FTP authentication” (page 72).
- For VoIP solutions only, X11 sessions between the desktop and MDM workstations use the Secure Shell (SSH) protocol to encrypt all data, including login passwords. For more information, see “Secure Shell (SSH) protocol for VoIP solutions” (page 73).
- For VoIP solutions only, sessions between two MDM workstations use the IP Security (IPSec) protocol to provide data encryption and authentication. For more information, see “IP Security (IPSec) protocol for VoIP solutions” (page 74).
- For VoIP solutions only, sessions between MDM workstations and MSS/MG15000 nodes use the IPSec protocol to provide data encryption and authentication.
- For VoIP solutions only, sessions between MDM workstations and Integrated EMS workstations use SSH to encrypt all data including passwords. For more information, see “Secure Shell (SSH) protocol for VoIP solutions” (page 73).
- Authentication sessions are protected by using RADIUS, IPsec (VoIP only), obsfucation, HTTPS and SAML protocols.

User access security

User access security involves making sure that only approved personnel have access to the node or workstation (authentication of userids and passwords), and that they have access to only the functions required to do their tasks (authorization of access levels). The following user authentication and authorization capabilities are supported:

- MDM and MSS/MG15000 local user authentication and authorization. Userids and passwords are authenticated and authorized by the system on which they were created. Access to the MDM Toolset environment requires use of a local userid. For more information, see "Local user access management" (page 31).
- MDM centralized authentication and authorization for VoA solutions. The MDM Admin Server provides user authentication and authorization for Operator Client userids for access to MDM tools and utilities and to associated MSS/MG15000 nodes. For more information, see "Multiservice Data Manager centralized user administration in a VoA solution with the Operator Client application" (page 39).
- Integrated EMS centralized authentication and authorization for VoIP solutions. A specified Integrated EMS workstation provides user authentication and authorization for all userids for MDM workstations and MSS/MG15000 nodes associated with it. For more information, see "Centralized user access management using Integrated EMS" (page 61).

Security audit logs

An essential part of managing a secured network is the monitoring and auditing of security activities in the network to look for security breaches or unwanted or unauthorized access so that corrective action can be taken.

MDM and MSS/MG15000 security audit logs are collected by the Multiservice Data Manager and stored on the MDM workstation. The logs can be sent either to the Integrated EMS (for VoIP solutions) or to the CS2000 Core Manager (for VoA solutions) for central access and storage. For more information, see "Security audit logs" (page 87).

Administration of Multiservice Data Manager servers and Multiservice Switches using Multiservice Data Manager

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

- monitor the status of various Multiservice Data Manager processes and servers
- administer Multiservice Switch equipment
- review Multiservice Data Manager and Nortel Multiservice Switch log messages
- administer user access for Operator Client (VoA solutions only)

For more information on these tools, see either the "Summary of MDM tools and Operator Client application tools" (page 167) or 241-6001-303 *Nortel Multiservice Data Manager Customization and Administration*.

Chapter 2
Local user access management

Local user authentication and authorization is applied to userids defined locally on the Multiservice Data Manager server or on a Multiservice Switch 15000 or Media Gateway 15000 switch.

In VoA solutions, access to the MDM Toolset environment requires local user authentication and authorization. Access to the MDM Operator Client environment uses central authentication and authorization services provided by the MDM Admin Server. For more information on the MDM centralized user access, see “Multiservice Data Manager centralized user administration in a VoA solution with the Operator Client application” (page 39).

In VoIP solutions, access to a subset of MDM Toolset functionality requires local user authentication and authorization. Access to the MDM Operator Client environment and most of the MDM Toolset environment requires central authentication and authorization provided by the Integrated EMS. For more information on using Integrated EMS for central user authentication and authorization, see “Centralized user access management using Integrated EMS” (page 61).

For more information on local user access management, see:

- “Multiservice Data Manager local user authentication and authorization” (page 32)
- “Multiservice Data Manager local user authentication and authorization for Multiservice Switch nodes” (page 35)

Multiservice Data Manager local user authentication and authorization

Nortel Multiservice Switch nodes and the Multiservice Data Manager Toolset use a two-tier authentication system. The first tier provides access to Multiservice Data Manager network management software. This level of authentication allows the operator to run Multiservice Data Manager tools, perform surveillance on the network, and passively administer Multiservice Data Manager 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 log in to Multiservice Data Manager. Once connected by this method, the operator can perform network element maintenance or configuration tasks.

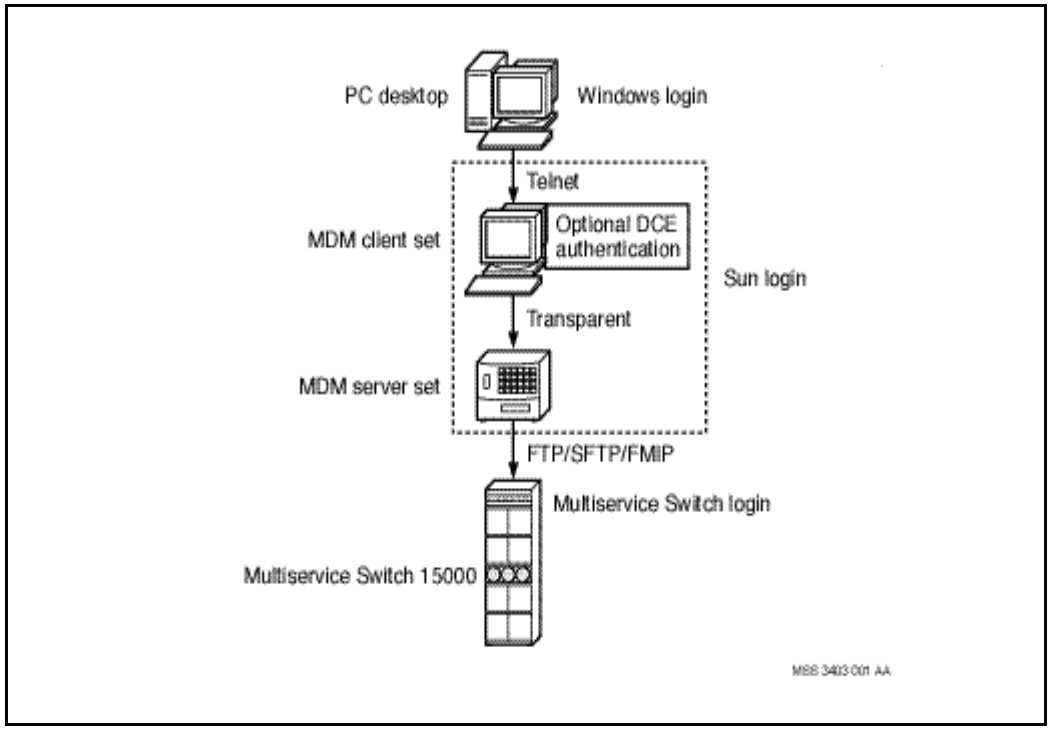
Operators who directly log in to Multiservice Data Manager require standard Multiservice Data Manager authentication (valid UNIX userid and password). This level of authentication provides access to the UNIX platform only, and permits the user to launch Multiservice Data Manager servers and to run scripts.

For the Multiservice Data Manager client-server set, security is provided by UNIX authorization on the client-set machine.

Multiservice Data Manager security tools monitor the status of various Multiservice Data Manager processes. For information on the monitored processes, see “Multiservice Data Manager security and access tasks” (page 33). For more information about the security tools, see “Summary of MDM tools and Operator Client application tools” (page 167).

The figure “Multiservice Switch node and Multiservice Data Manager security management” (page 33) shows the levels of security.

Figure 1
Multiservice Switch node and Multiservice Data Manager security management



Multiservice Data Manager security and access tasks

The table “Multiservice Data Manager security and access tasks” (page 34) defines the OAM security procedures required for MDM.

Table 1
Multiservice Data Manager security and access tasks

Task performed	When used	Required permissions	Notes
System administration functions	As needed.	UNIX “root” userid 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 userid and password.	Also requires a valid node userid for maintenance.
Configuration	As needed.		Also requires a valid node userid.
Viewing node security logs	As needed.	Multiservice Data Manager userid	Secured using UNIX security (see Note).
MDP sysadmin	As needed.	mdpadmin.	
Multiservice Data Manager sysadmin	As needed.	UNIX “root” userid and password.	
Note: DCE is an optional security package for VoA solutions that can govern log in.			

Multiservice Data Manager local user authentication and authorization for Multiservice Switch nodes

When an operator tries to access a Nortel Multiservice Switch node through a Nortel Multiservice Data Manager (MDM) tool or utility, a valid Multiservice Switch userid and password is required. Authentication is performed by a common security function, which allows many MDM 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 97).

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

- "User profile impact levels" (page 35)
- "Security and access tasks" (page 37)
- "Secure FTP authentication" (page 72)

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 36) identifies the impact levels available on Nortel Multiservice Switch 15000 nodes within the 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 37) identifies the security and access tasks required for Nortel Multiservice Switch 15000 nodes within the 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 userid and password with impact of at least system administration	Access from Multiservice Data Manager tools
Log in to perform configuration functions (for example, software upgrade)	According to customer upgrade schedule or as needed	Multiservice Switch userid and password with impact of at least configuration	Access from Multiservice Data Manager tools
Log in to perform regular maintenance functions	According to regular maintenance scheduled or as needed	Multiservice Switch userid and password with impact of at least service	Access from Multiservice Data Manager tools
Log in to the node to perform emergency functions requiring operating system-level commands	As needed	Multiservice Switch userid and password with impact of at least debug	Access from Telnet or local (serial) interfaces; access from Multiservice Data Manager tools is not possible
Multiservice Switch security audits	As needed	Multiservice Data Manager UNIX userid and password	Use the Multiservice Data Manager Data Viewer to view the node security logs

Chapter 3
Multiservice Data Manager centralized user administration in a VoA solution with the Operator Client application

This section describes the configuration required to deploy and manage user administration with centralized AAA in a VoA solution. To use centralized AAA on an MDM Admin Server in a VoA solution with Operator Client desktops, you must ensure that you have:

- installed the software to deploy the MDM Admin Server and enable Operator Client applications, see NN10185-461 *Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*
- configured the MDM Admin Server for centralized AAA, see NN10114-511 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP*
- configured the RADIUS interface (on MDM) and RADIUS client (on MSS15000/MG15000 nodes) for centralized authentication, see NN10114-511 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP*
- made an Ethernet connection between the Operator Client desktop and the MDM Admin Server
- configured Policies with roles and associated users with those roles on the MDM Admin Server as shown in the rest of this chapter, see “User administration in a VoA solution with MDM centralized AAA overview” (page 40)

- the operator perform an initial launch of Operator Client at the operator's desktop to finish the user access configuration of centralized AAA in your VoA network

The MDM Operator Client can be launched from a web browser on a PC (using Internet Explorer) or from a UNIX workstation (using Netscape). If Operator Client is run on a UNIX workstation, the workstation must be a platform certified by Nortel that supports Solaris 9 operating systems. On a PC, Operator Client can run on both Windows 2000 and Windows XP operating systems.

User administration in a VoA solution with MDM centralized AAA overview

Operator Client interface user accounts are configured on an MDM Admin Server using the MDM Toolset for deployments that use the MDM for centralized authentication, authorization, and accounting. As administrator, you configure policies, roles, and users using the MDM Toolset to enable operators to have access and specified capabilities with certain tools through an Operator Client interface. To govern user access in this way, you must ensure that your operators have access to the network through an Operator Client interface.

Centralized AAA is available when operators access the network using the Operator Client application, however, centralized AAA is not available when you access the network through the MDM Toolset. You can configure users to have access through both the Operator Client interface and the MDM Toolset interface. However, if you want to control what a user can see and do, configure the user's access to be through Operator Client only. This means that once you have configured the policies, roles and users on the MDM Admin Server for Operator Client access, you should remove the local UNIX access to the MDM Toolset for those users.

To control user access, the following user administration tasks must be performed:

- Configure three policies for each of the roles to define access privileges.
- Apply the policies to the roles.
- Associate the users with roles.

- Remove local UNIX user privileges for operators to restrict them to using the Operator Client application only.

Access administration in a VoA solution with MDM centralized AAA

There are four key concepts to understand when you configure user access for Operator Client as follows:

- User: an operator on the system with defined privileges, userid, password etc. A user will be associated with at least one Role.
- Role: a logical entity used to associate users with policies thereby defining the access of a user. This is simply a name and description with no other characteristics.
- Rule: defines the resources and access to that resource (for example, for the Fault resource permit view only)
- Policy: a collection of Rules with an associated Role (or users)

To administer access to the network, you must configure policies, which are applied to roles, to which you associate users. The combination of a policy and a role defines the access permitted to a user. See Figure 2, "Administering policies, roles, and users in a VoA solution with central AAA," (page 42).

The following list is the legend for Figure 2, "Administering policies, roles, and users in a VoA solution with central AAA," (page 42). The numbers correspond to the sequence of tasks that you must perform to administer user access for centralized AAA in a VoA solution:

1 Create three policies for each role that you plan to use in your network workforce.

2 Create each role.

3 Apply each of the three required policies to each role as planned.

4 Associate each user with a role or multiple roles as planned.

See "An example of View Access Configuration Attributes - MDM Application Actions" (page 43) for an example of the values in a configured policy for users that are associated to a view only role.

Figure 2
Administering policies, roles, and users in a VoA solution with central AAA

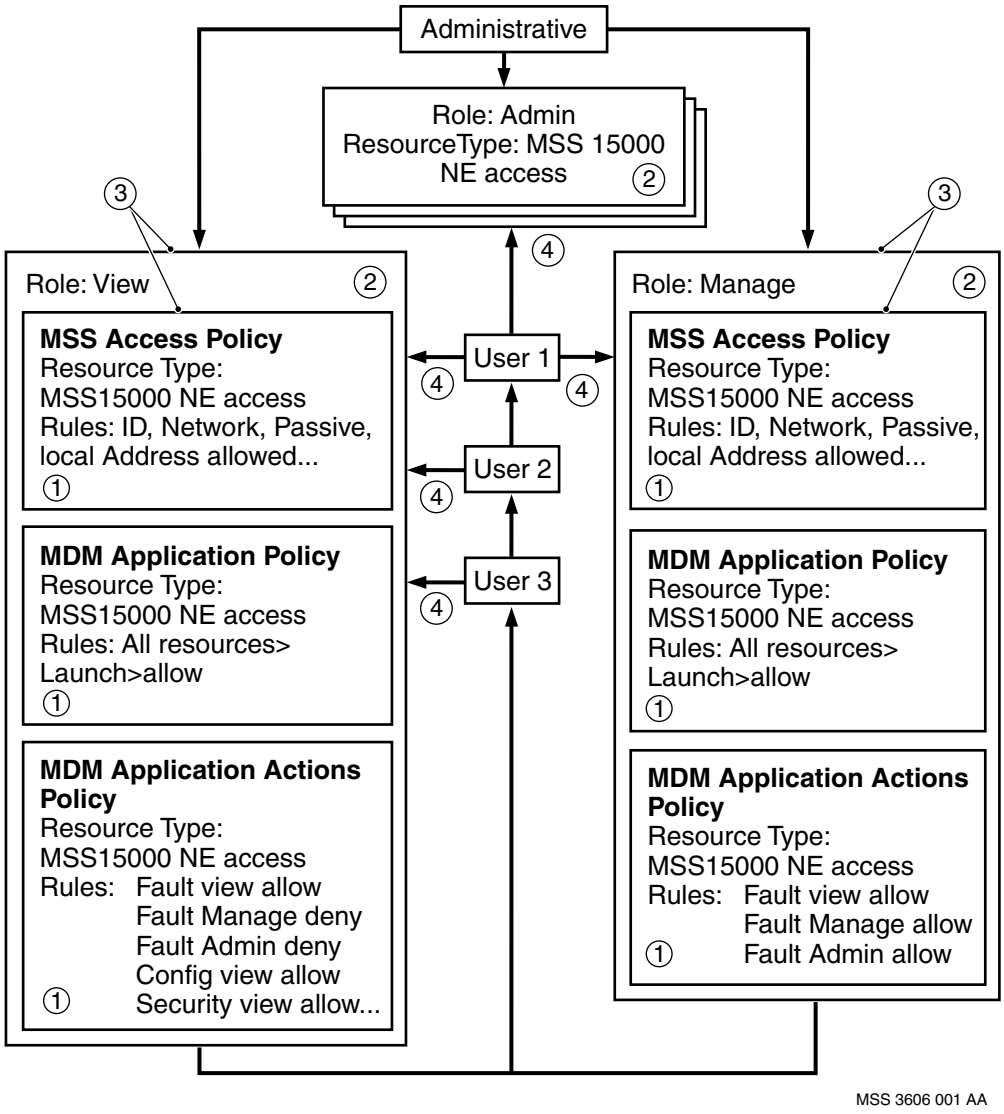


Table 4
An example of View Access Configuration Attributes - MDM Application Actions

Attribute	Value
Policy Name MDM	Application Actions View
Subjects (Role)	View Role
Rule Name: MDM View Actions	Resource Type: Application Actions Resources: All Resources Actions: • Fault View: Allow • Fault Manage: Deny • Fault Admin: Deny • Config View: Allow • Config Manage: Deny • Config Admin: Deny • Accounting View: Deny • Accounting Manage: Deny • Accounting Admin: Deny • Performance View: Allow • Performance Manage: Deny • Performance Admin: Deny • Security View: Allow • Security Manage: Deny • Security Admin: Deny • Operational View: Allow • Operational Manage: Deny • Operational Admin: Deny

Policies in a VoA solution with MDM centralized AAA

The Policy Manager is used to define access for a User or Role to the tools and the network. Multiple Users and/or Roles can be associated with a policy. A user can be associated to a role and the role associated with a policy. This way multiple users can have the same access privileges.

A policy contains a set of policy rules that define the allowable actions that can be performed on a specific resource type. Policies are created by associating action permissions and resource types.

The user administration system has two resource types to define access on MSS and Operator Client: MSS NE Access and a generic resource type labelled Application which is used to control access to Operator Client. Each resource type contains a set of attributes that are used to define a policy rule for logging on to the resource type. Using the Policy Manager application, the administrator creates a policy rule for a resource type by entering unique values in its attribute set. These values define the user permissions for that particular resource.

User access is composed of three separate policies for any given role:

- MSS Access Policy - controls the MSS15000 access allowed
- MDM Application Policy - determines the applications to which a user has access
- MDM Application Actions Policy - determines the actions the user can perform within the scope of a tool for the tools that the user can access

  Note: A single MDM Application policy will be created for all recommended roles. The MSS15000 Access Policy and MDM Application Action Policy controls the access available to the user or role.

When you associate a role to a policy or policies, you grant all the users associated with that Role the same access privileges. A Policy is composed of the following:

- Resource type
- Resources that can be applied to the Resource Type

- Actions that can be applied to the Resources

Resources in a VoA solution with MDM centralized AAA

The Resources depend on the Resource Type selected and the Application Action:

- MSS NE Access
- Applications (MDM applications (tools))
- Application Actions (actions that are allowed for a specific MDM application)

Application actions are the actions a user can perform with each specific system tool. For each tool, there is a set of application actions that can be granted to a user. For example, the actions associated with the Alarm Display tool, are:

- view active alarms
- view alarm history
- acknowledge or unacknowledge alarms
- clear alarms locally
- clear alarms globally

The administrator determines which applications a user is authorized to access through the definition of policies to use of crucial actions. In order to run applications deployed via Operator Client, a user must be authorized for the application's crucial actions. In addition, the administrator can also determine which actions, within applications, a user can access through the use of action categories.

Refer to NN10600-605 *Nortel Multiservice Data Manager Network Security Fundamentals* for information about action categories, crucial actions, and Operator Client user administration.

To see examples of the various policies with the attributes configured for Operator Client in the VoA network, refer to "Policy and role configuration for Operator Client user administration on the MDM" NN10225-512 *Nortel*

Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP.

Roles in a VoA solution with MDM centralized AAA

Roles are used to group users that perform common tasks. A role is a logical entity that is used to associate users with policies and define the access of the user. Use the User Manager application to create, delete, or edit any role in the User Administration system.

A role can be associated with any number of users or policies. For example, an administrator can create the role of Fault Management and associate it with a number of users who have permission to perform Fault Management procedures.

The role name, which you define, is used to group users according to a function. For example, “Ottawa Fault”. The role description describes the function of the role. For example, “all users who perform fault management in Ottawa”. You can edit or delete a role at any time. Refer to NN10600-605 *Nortel Multiservice Data Manager Network Security Fundamentals* for more information about roles.

Users privilege definitions in a VoA solution with MDM centralized AAA

Three user access definitions are recommended:

- View/passive - observe the network but unable to make modifications
- Manage/provisioning - observe the network, take corrective actions and provision
- Administrative - full access to all actions

You can see the policies and rules configured in your system through the Policy manager and User Manager applications.

To see examples of the various policies with the attributes configured for Operator Client in the VoA network, refer to “Policy and role configuration for Operator Client user administration on the MDM” NN10225-512 *Nortel*

Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP.

User administration tools and tasks in a VoA solution with MDM centralized AAA

User administration for centralized AAA on the MDM Admin Server is comprised of the following:

- accessing the MDM Admin Server and configuring user accounts and passwords, see "Accessing the MDM Admin Server User administration tools" (page 47)
- assigning policies to roles and assigning users to roles for centralized AAA
- removing local user privileges for those users that have no need to gain access to the MDM Toolset

Four GUI-based applications, available from the MDM Toolset on the MDM Admin Server, allow you to administer centralized AAA. These interfaces are used to create roles, policies, and application actions that define a user's privileges. The four GUI-based applications are as follows:

- User Manager: used to create centralized user accounts as well as roles, which group the users into common functions
- Policy Manager: used to create policies, which define the allowable actions that the user can perform on a network element and/or allowable applications of Operator Client
- Security Settings: used to configure basic security settings for all centrally defined users
- Session Management: used to view or terminate current user sessions

Accessing the MDM Admin Server User administration tools

1 Log in to the MDM Admin Server with the current administrator userid and password to start the system.

Refer to "Logging in to the User administration system" in NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access*

Configuration for complete procedure and a list of userids and system passwords.

Note: It is recommended that all default passwords given in the documentation for initial access are changed as soon as possible after the initial login for security reasons.

2 Open the MDM Toolset and from the main menu under System, select Security> User Admin.

The User Admin screen opens.

3 Configure the user accounts and passwords in the Security Settings screen. Refer to "User administration system user configuration" in NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration* for procedural information.

Note: This task includes general security settings that are related to user passwords and accounts (for example, length of userid, expiration time for password).

Task flow reference for a VoA solution with MDM centralized AAA

The following table gives the sequence of actions necessary for policy creation and user administration to enable centralized AAA in your VoA network. The actions should be performed in the sequence shown using the references to the procedures that are required to complete each action. See "Tasks reference for Centralized AAA in a VoA solution" (page 49).

Table 5
Tasks reference for Centralized AAA in a VoA solution

Action	See procedure	Reference
Configure the required policies in the Policy Manager screen. ***Note:*** This is where you define Policies composed of Rules applied to Resources and Attributes that control user access (for example, MSS15000 access definition, MDM tool access, and MDM tool actions).	Creating a Policy	NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*
Configure the required roles. ***Note:*** Roles are used to group users that perform common tasks. Refer to NN10600-605 *Nortel Multiservice Data Manager Network Security Fundamentals* for more information about roles.	Creating a role	NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*
Configure those users that you want to have centrally authenticated on the MDM Admin Server in the User Manager screen. ***Note:*** This is where you define Users and Roles. Roles are a means of creating a set of users with the same access privileges.	Creating users	NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*
(Sheet 1 of 5)		

Table 5 (Continued)
Tasks reference for Centralized AAA in a VoA solution

Action	See procedure	Reference
Associate the policy to the users. ***Note:*** This is where you associate users with roles and roles with policies. Remember roles are a means of creating a set of users with the same access privileges.	Adding a Policy to Subjects	NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*
Ensure you have configured the RADIUS interface (on MDM) and RADIUS client (MSS15000/MG15000) for centralized authentication.	Radius configuration for centralized authentication	NN10114-511 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP*
Remove local access privileges from those users with no need to access the MDM Toolset.	For local UNIX users that no longer require access to the MDM Toolset, use the User Manager tool to delete their userid entities which are stored in the LDAP directory on the MDM.	NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*.
Remove local MSS users so that they will be centrally authenticated. ***Note:*** Do not remove local userids from the MSS that are used by the MDP, FMDR, and PMSP surveillance servers. If you remove these userids and the central AAA server goes down, surveillance data may be lost. Ensure you retain the local userids for MDP, FMDR, and PMSP in addition to a debug level userid.	Deleting a userid	NN10600-601, MSS Security Management
(Sheet 2 of 5)		

Table 5 (Continued)
Tasks reference for Centralized AAA in a VoA solution

Action	See procedure	Reference
Monitor active sessions in the User Session Manager screen. ***Note:*** From this interface you can monitor active sessions from the list and terminate any of the sessions as necessary.	Terminating a centrally defined user's session	NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*
(Sheet 3 of 5)		

Table 5 (Continued)
Tasks reference for Centralized AAA in a VoA solution

Action	See procedure	Reference
Ensure that the operator performs an initial log in to the desktop on which the Operator Client application will be running and edits the appropriate files for the initial launch. ***Note:*** All systems should be part of the same DNS. If you are not part of the same DNS, perform the following: • For PC-based Operator Client applications, you must edit the file: c:\WINNT\system32\drivers \etc\hosts • For UNIX-based Operator Client applications, you must edit the file: /etc/hosts	Starting Operator Client	241-6001-122 *Nortel Multiservice Data Manager Using MDM Tool Set and Operator Client Interfaces* for initial log in procedures.
(Sheet 4 of 5)		

Table 5 (Continued)
Tasks reference for Centralized AAA in a VoA solution

Action	See procedure	Reference
Have the operator log in from the Operator Client desktop after the initial launch.	Starting Operator Client	For subsequent launches of Operator Client, begin the launch at step 2 of the Starting Operator Client procedure in: 241-6001-122 *Nortel Multiservice Data Manager Using MDM Tool Set and Operator Client Interfaces* ***Note:*** Ensure you have downloaded the latest Java Runtime Environment (JRE) to allow the JWS files to download. When the JWS files have downloaded and if the files on your desktop are current, you will get the Operator client window and a login screen. Refer to 241-6001-122 *Nortel Multiservice Data Manager Using MDM Tool Set and Operator Client Interfaces*.
(Sheet 5 of 5)		

Managing user administration system accounts for the MDM Admin Server

User account passwords expire, staff join or leave the organization, and staff with existing MDM UNIX user accounts or MSS logins who will now be centrally authenticated must have their accounts migrated to the MDM user administration server. Passwords for system and operator user accounts must be created, maintained, updated, or removed.

For system user accounts, the User Administration System itself defines the system user accounts (that is for example, surveillance users as opposed to operator user accounts). However, as administrator, you will be required to reset these passwords whenever they are about to expire. Refer to the procedure “Changing system account passwords” in NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*.

CAUTION

Allowing a system user password to expire causes major system problems

If a system user password expires, you will be required to re-install the system. Call GNTS at Nortel for assistance. To safeguard against the expiration of system user accounts, set up automatic email notification of expiration in a cronjob. When the administrator is notified of the expiration it is a simple matter of resetting the user account passwords.

Note: The User Administration system consists of four applications that are accessed from Nortel Multiservice Data Manager Toolset. A set of default administration userids provide access to the applications.

The following table lists references to the procedures in NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration* that are required for account maintenance.

Table 6
Managing user administration system accounts task references for MDM Centralized AAA in a VoA solution

Activity	Task	Refer to Procedure	Notes
Configuring the User Administration System	Initial login with system user passwords	"Logging in to the User Administration system"	There are a number of predefined administrator user accounts configured. You must periodically change these passwords. The only password that does not expire is the cn=directory manager userid password.
	Installing trusted certificates	"Changing the Sun ONE IS Web Server admin account"	If trusted certificates are required, this procedure is used to install the trusted certificates for SSL.
	Change the amldapuser password	"Changing the password for amldapuser if the password has not expired"	The amldapuser is the default user for root user bind. It is used to bind to the Directory Server specified in the Primary LDAP Server and Port field as administrator.
		"Changing the password for amldapuser if the password has expired"	
	Change the dsmeuser password	"Changing the password for dsmeuser"	The dsmeuser is used for binding purposes when the Identity Server SDK performs operations on the Directory Server that are not linked to a particular user (for example, retrieving service configuration information). If the password has expired, you must generate a new encrypted password to paste into both the serverconfig.xml file and the IS console.

(Sheet 1 of 5)

Table 6 (Continued)
Managing user administration system accounts task references for MDM Centralized AAA in a VoA solution

Activity	Task	Refer to Procedure	Notes
	Change the puser password	"Changing the password for puser"	Puser is a proxy user that can take on any user privileges. Puser is used by the Identify SDK to establish the LDAP connection pool to the Directory Server. If the password has expired, clients cannot authenticate and you must generate a new encrypted password to paste into both the serverconfig.xml file and the NDS console.
	Change the amService-UrlAccessAgent account password	"Changing the password for the amService-UrlAccessAgent account"	
User access security management	Configure users	"Starting the Sun ONE DS console"	Start the Sun ONE DS console to perform administration procedures on the Multiservice Data Manager LDAP server.
	View the system account userids	"Viewing system account userids"	The User Manager application displays userids. The Policy Manager application displays the permissions associated with userids.
	Change system account passwords	"Changing system account passwords"	Administrators are required to change the passwords on system accounts. A command line password change utility is provided for this purpose.
(Sheet 2 of 5)			

Table 6 (Continued)
Managing user administration system accounts task references for MDM Centralized AAA in a VoA solution

Activity	Task	Refer to Procedure	Notes
	Change the Sun ONE Directory Manager password	"Changing Sun ONE Directory Manager password"	The Sun ONE Directory Manager password does not expire and should be changed regularly to maintain system security. You must also create a local encrypted password file.
	Set the validation period for system account passwords	"Setting validation period for system account password"	Specify the number of days before the system account passwords expire. If the value is specified as zero (0), the system account password will not expire.
Managing user accounts	Configure users	"Setting validation period of user account password"	The validation period for individual users is set using the Security Settings interface.
	Set up a cron job to check for password expiry and email notification of expiries	"Setting up a cron job to check for password expiry"	This script is run hourly to check for expiring passwords. When expiring passwords are found an email is sent to notify the user. If you have enforced password expiry in the Security Settings window, set up this cron job.
	Change centrally authenticated passwords	"Changing centrally authenticated passwords"	Users can use Nortel Multiservice Data Manager Operator Client environment to change their own centrally authenticated passwords.
(Sheet 3 of 5)			

Table 6 (Continued)
Managing user administration system accounts task references for MDM Centralized AAA in a VoA solution

Activity	Task	Refer to Procedure	Notes
User access security management	Change centrally defined userid attributes	"Changing centrally defined user ID attributes"	Modify userid attributes for a centrally defined user are in the User Manager application of the User Administration system.
	Delete a centrally defined user	"Deleting a centrally defined user"	Delete userid and associated privileges of a centrally defined user from the Sun ONE Identify server. Externally authenticated users are added automatically as users in the MDM LDAP directory and must be deleted periodically by the administrator.
	Reset a centrally defined user password	"Resetting a centrally defined user password"	If you do not know a current centrally defined user password and want to change it, reset the password.
User administration system user configuration	Create centrally authenticated users through the User Administration system	"Creating centrally authenticated user through the User Administration system"	Use the User Manager application to create a user that is centrally authenticated.
(Sheet 4 of 5)			

Table 6 (Continued)
Managing user administration system accounts task references for MDM Centralized AAA in a VoA solution

Activity	Task	Refer to Procedure	Notes
	Change an existing user to be centrally authenticated and locally authorized from the MSS/ MG15000	"Changing an existing user to be centrally authenticated and locally authorized - MSS/MG"	Use the Nortel Multiservice Switch 15000 command line to create a userid that has access defined by the RADIUS server.
	Change a userid to be centrally authenticated from the MSS/MG15000	"Changing a user ID to be centrally authenticated - MSS/MG"	You can edit an existing userid that has its access defined locally on a node, to having access defined by the RADIUS server centrally authenticated.
(Sheet 5 of 5)			

Chapter 4
Centralized user access management using Integrated EMS

In VoIP solutions, Integrated EMS maintains a single set of userids for access to all the Multiservice Data Manager workstations, Multiservice Switch 15000 switches and Media Gateway 15000 switches in the associated regional office. This centralization promotes ease of managing the userids across multiple switches and workstations, and reduces the time to make necessary changes.

Integrated EMS user access management

Integrated EMS provides detailed access authorization by setting the scope for the operations assigned to a group. This scope defines the restricted access for the operation in that group. Integrated EMS procedures provide for:

- configuring user settings
- configuring scope and group settings

For details on using Integrated EMS to manage user access, refer to NN10336-611 *Integrated EMS Security and Administration*.

Local access requirements

Some MDM userids and groups must be maintained locally on the MDM Server. Local userids are used to access MDM functionality if the connection to the Integrated EMS is not available. MDP tools can only be accessed using local userids. “MDM local userids” (page 62) and “MDM local groups”

(page 62) lists the userids and groups that remain as local userids and groups after the migration of userids to the Integrated EMS. Other userids may be maintained locally as required.

When changing the password for a locally defined MDM userid, use the command: **`passwd -r files <userid>.`**
Otherwise, the password change request is sent to Integrated EMS.

Table 7
MDM local userids

root:Super-User	noaccess:No Access User
daemon:x:1:1::/:	wpms:Workstation Performance Monitoring System
bin:x:2:2::/usr/bin:	Nortel:nortel from NNswmgmt
sys:x:3:3::/:	sshd:sshd privsep
adm::Admin	<mdpadmin>:mdp administor
nobody:Nobody	
Note: For <mdpadmin>, use the MDP administrator userid set during installation.	

Table 8
MDM local groups

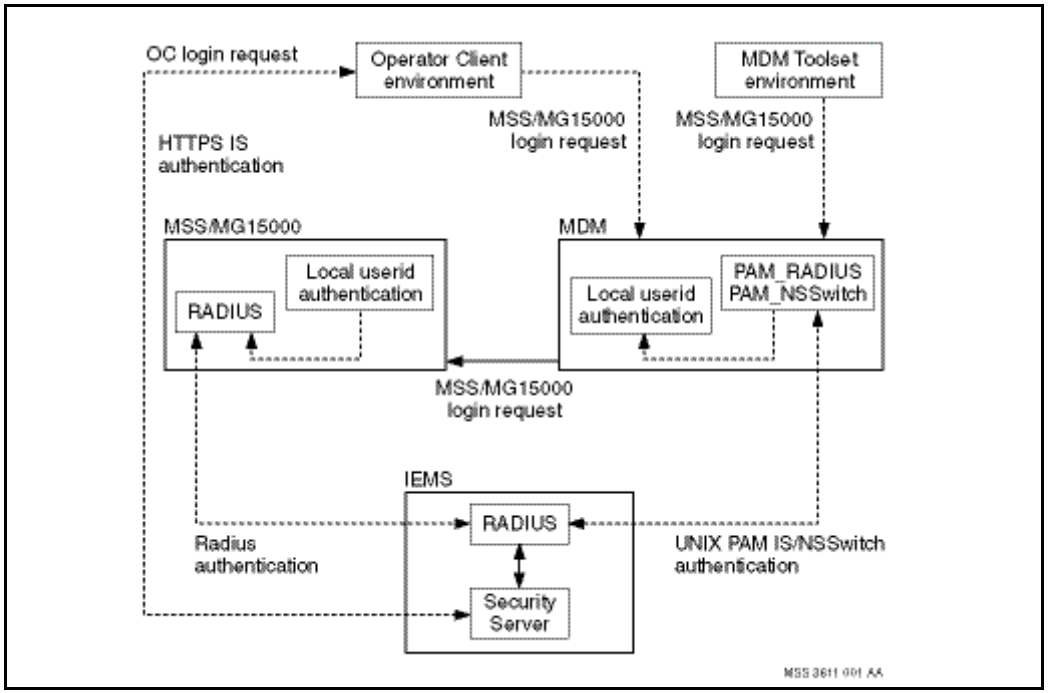
root	adm	staff	noaccess
other	uucp	daemon	nogroup
bin	tty	sysadmin	nortel
sys	nuucp	nobody	<mdpgroup>
Note: For <mdpagroup>, use the MDP administrator group set during installation.			

Some MSS/MG15000 userids must also be maintained as local userids. In case that the connection to Integrated EMS is unavailable, userids for GMDR and PMSP access are required, as well as a local userid with an impact of debug.

Authentication data flow using Integrated EMS central AAA service

"User authentication and authorization data flow with Integrated EMS" (page 63) shows the data flow for user authentication and authorization in VoIP solutions using Integrated EMS central AAA service.

Figure 3
User authentication and authorization data flow with Integrated EMS



MDM Toolset environment

The MDM sends an MDM Toolset login message via the PAM_RADIUS interface to the Integrated EMS security server for authentication. When the Integrated EMS security server authenticates a valid userid, it returns

information on the authorization level associated with the userid to the MDM. The MDM uses the PAM_NSSwitch interface to determine the associated user information for the MDM system, such as valid groups, shell, and other UNIX information. If the userid is not found on the Integrated EMS system, then MDM local user authentication is invoked.

Operator Client environment

Once the Operator Client application on the desktop is launched, a login window appears. If Integrated EMS has a security certificate configured, the certificate window appears before the login information can be entered. The login information is sent from the desktop to the Integrated EMS security server where the userid/password is authenticated. If the userid is valid, the associated group information is returned to the Operator Client application where the authorized tools are activated.

MSS/MG15000

MSS/MG15000 login requests are sent to the node where they are first compared with the local userids. If the userid is not found locally, it is sent via a RADIUS client interface to the Integrated EMS system. When the Integrated EMS security server authenticates the userid, it sends the group's authorization information back to the MSS using the RADIUS interface. The MSS/MG15000 switch maps this information onto the associated access control components (scope, impact, etc).

Integrated EMS user group mappings

The Integrated EMS user groups and the mapping of the MDM and MSS/MG15000 access privileges onto these groups are shown in "Mapping of Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000 access privileges to Integrated EMS groups in VoIP networks" (page 171).

For more information on administering Integrated EMS groups, see NN10336-611 *Integrated EMS Security and Administration*.

Administration procedures for Integrated EMS central AAA service

The following administration procedures are used on the MDM Server and MSS/MG15000 switches:

- "Updating the MDM Server when the Integrated EMS amadmin password changes" (page 65)
- "Updating the MDM Server when the Integrated EMS RADIUS shared secret changes" (page 66)
- "Updating the MSS/MG15000 switch when the Integrated EMS RADIUS shared secret changes" (page 66)

Updating the MDM Server when the Integrated EMS amadmin password changes

If the password for the Integrated EMS userid *amadmin* changes, the PAM_NSSwitch software on the MDM Server must be updated with the new password.

Note: Make sure that the new password for the Integrated EMS *amadmin* userid is distributed to the MDMServer site using a secure method.

Procedure steps

1 Log in to the MDM Server as root.

2 Execute the following commands:

```
cd /opt/nortel/applications/security/current_nssaml/
swmgmt/bin

./configure_nssaml.sh -subcomponent password
```

3 At the prompt, enter the new Integrated EMS *amadmin* password.

The following shows a sample output for the *configure_nssaml.sh* command:

```
Note:  Configuring component nssaml
Note:  Configuring password subcomponent
      Enter the password: <IEMS_admadmin_password>
```

Variable definitions

Variable	Definition
<IEMS_amadmin_pwd>	is the new password for the Integrated EMS *amadmin* userid.

Updating the MDM Server when the Integrated EMS RADIUS shared secret changes

If the Integrated EMS RADIUS shared secret changes, the PAM_RADIUS software on the MDM Server must be updated with the new RADIUS shared secret.

Note: Make sure that the new RADIUS shared secret is distributed to the MDM Server site using a secure method.

Procedure steps

1. Log in to the MDM Server as root.
2. Execute the following commands:

```
cd /opt/nortel/applications/security/
current_pamradclt/swmgmt/bin

./configure_pamradclt.sh -subcomponent servers
```

3. Enter the Integrated EMS RADIUS shared secret as prompted.

Updating the MSS/MG15000 switch when the Integrated EMS RADIUS shared secret changes

If the Integrated EMS RADIUS shared secret changes, the RADIUS client software on the MSS/MG15000 switch must be updated with the new RADIUS shared secret.

Note: Make sure that the new RADIUS shared secret is distributed using a secure method.

Procedure steps

1. Log in to the MSS/MG15000 switch as system administrator.
2. Enter provisioning mode:

```
start prov
```

3 Obtain the provisioning file:

```
copy prov
```

4 Change the RADIUS shared secret:

```
set Ac Radius Server/0 sharedSecret
<new_shared_secret>
```

5 Verify the provisioning change:

```
check prov
```

6 Save the provisioning change:

```
save prov
```

7 Activate the provisioning change:

```
activate prov
```

8 Confirm the provisioning change:

```
confirm prov
```

9 Commit the provisioning change:

```
commit prov
```

10 Exit provisioning mode after the commit is complete:

```
end prov
```

Variable definitions

Variable	Definition
<new_shared_secret>	is the new Integrated EMS Radius shared secret.

Updating the MDM Server when the Integrated EMS IP address changes

If the Integrated EMS IP address changes, the PAM_RADIUS software on the MDM Server must be updated with the new IP address.

Procedure steps

1. Log in to the MDM Server as root.
2. Execute the following commands:

```
cd /opt/nortel/applications/security/
current_pamradclt/swmgmt/bin

./configure_pamradclt.sh -subcomponent clients
```

3. Enter the Integrated EMS IP address as prompted.

Updating the MSS/MG15000 switch when the Integrated EMS IP address changes

If the Integrated EMS IP address changes, the RADIUS client software on the MSS/MG15000 switch must be updated with the new IP address.

Procedure steps

1. Log in to the MSS/MG15000 switch as system administrator.
2. Enter provisioning mode:

```
start prov
```

3. Obtain the provisioning file:

```
copy prov
```

4. Change the Integrated EMS IP address:

```
set Ac Radius Server/0 serverIpAddress
<new_IEMS_IPaddr>
```

5. Verify the provisioning change:

```
check prov
```

6. Save the provisioning change:

```
sav prov
```

7 Activate the provisioning change:

```
activate prov
```

8 Confirm the provisioning change:

```
confirm prov
```

9 Commit the provisioning change:

```
commit prov
```

10 Exit provisioning mode after the commit is complete:

```
end prov
```

Variable definitions

Variable	Definition
<new_IEMS_IPaddr>	is the new Integrated EMS IP address.

Updating JWS software when the MDM Server host name changes

If the host name of the MDM Server changes, the JWS software must be configured to launch to the new host name.

Procedure steps

1 Log in to the MDM Server as root.

2 Edit the configuration file:

```
vi /opt/nortel/config/applications/desktop/jws/mft/
resources/desktop/DesktopGUI.jnlp
```

Change the host name references to the new host name.

Save and close the file.

Updating the MDM Server when the Integrated EMS host name changes

If the Integrated EMS host name changes, the MDM Server must be updated with the new host name.

Procedure steps

1. Log in to the MDM Server as root.
2. Execute the following commands:

   ```
   cd /opt/nortel/applications/security/
   current_isclient/swmgmt/bin

   ./configure_isclient.sh
   ```

3. Enter the Integrated EMS host name as prompted.

Chapter 5
Communications security management

In a VoIP network, security measures are applied to OAM Ethernet connections and to MG15000 signalling connections that carry management information to provide integrity and confidentiality of data transmitted across untrusted network connections. “VoIP management connections and protection methods” (page 71) shows the various management connections between MDM workstations, MSS/MG15000 nodes, and the Integrated EMS workstation, and the protection method used for each connection. See “IP Security (IPSec) protocol for VoIP solutions” (page 74) for more information about MG15000 signalling connections.

Table 9
VoIP management connections and protection methods

connections between		types of data	protection method
MDM server	X11 desktop	authentication data management commands management data (logs, etc)	encryption using SSH
MDM server	Operator Client desktop	authentication data limited management commands and data responses	password protection
MDM server	Integrated EMS	authentication data	PAM_RADIUS and PAM/NSSwitch
MDM server	Integrated EMS	fault and performance data	encryption using SSH

(Sheet 1 of 2)

Table 9 (Continued)
VoIP management connections and protection methods

connections between		types of data	protection method
MDM server	CS2000 Core Manager	performance data	
MDM server	MDM server		data authentication and encryption using IPSec
MSS/MG15000 node	MDM server	FTP data software downloads	data authentication using IPSec
MSS/MG15000 node	MDM server	all other connection types (FMIP, NTP, FTP control)	data authentication and encryption using IPSec
Integrated EMS security server	MSS/MG15000	authentication data	RADIUS
Integrated EMS security server	Operator Client desktop	authentication data	HTTPS, JAAS

(Sheet 2 of 2)

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 Multiservice Switch nodes and Nortel Multiservice Data Manager (MDM) servers. This feature is not recommended for VoIP networks where IPSec is being used.

When a Multiservice Switch node initiates an FTP session with a Multiservice Data Manager 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 Multiservice Data Manager server and upload spooled data to the workstation.

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

- NN10600-601 *Nortel Multiservice Switch 7400/15000/20000 Security Management*

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

- NN10070-461 *Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1*
- NN10185-461 *Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*
- NN10419-461 *Upgrading Nortel Multiservice Switch 15000 and Media Gateway 15000/20000 in Carrier Voice over IP Networks*

Secure Shell (SSH) protocol for VoIP solutions

Secure Shell (SSH) is a protocol supported by the Solaris 9 operating system software. SSH software is installed with the Solaris 9 operating system. For information on the Solaris 9 installation procedure, see NN10185-461 *Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*. For more information on activating SSH when securing the network, see NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*

Secure Shell (SSH) provides:

- data authentication in which keys are used to ensure that both participants in the connection are known to each other
- data encryption which encodes all data, including passwords.

SSH uses a system of dynamically exchanged public and private keys to authenticate the users of the connection, and to encrypt and decrypt the data.

For more information on SSH operation for MDM, see NN10600-607 *Nortel Multiservice Data Manager Network Security: Secure Communications Configuration*.

IP Security (IPSec) protocol for VoIP solutions

The IP Security (IPSec) protocol is supported on MDM workstations by the Solaris 9 operating system and on MSS/MG15000 switches in the SN08 release software. It provides both authentication and encryption of data moving between the two end points of a connection.

IPSec connections require the definition of security policies (SPs) that govern how transmitted and received IP packets will be treated. Security associations (SAs) are defined to assign these policies and a security key to the connection. A separate SA must be created for each end of the connection, and must match SA being applied at the other end of the connection. Security keys are used for data authentication and encryption/decryption.

Since security policies and security associations are statically configured, they will not be lost on a system reboot or restart.

To display the IPSec configuration information for MDM workstations and MSS/MG15000 nodes, see:

- "Viewing MDM IPSec information" located in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*
- "Viewing MSS/MG15000 IPSec information" located in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*

The H.248 call control connection between a Media Gateway 15000 using VSP3-o function processors and the Connection Server 2000 (CS2000) in a VoIP network is also secured using IPSec. For more information about IPSec for the call control connection for the Media Gateway 15000, refer to NN10600-780 *Nortel Media Gateway 7480/15000 Technology Fundamentals*.

To display the IPSec configuration information for MG15000 call control connections, see "Displaying IPSec security association information for call connections on the MG15000 shell interface" (page 179).

For more information on IPSec for MDM workstations, see NN10600-607 *Nortel Multiservice Data Manager Network Security: Secure Communications Configuration*. For more information on IPSec for MSS/MG15000 nodes, see NN10600-601 *Nortel Multiservice Switch 7400/15000/20000 Security Management*.

IPSec key management

The level of authenticity and confidentiality that security keys provide relies on the keys being unique, random, and shared only by the two ends of the connection.

IPSec keys for the MDM workstations and MSS/MG15000 nodes are refreshed manually. It is recommended that keys are refreshed regularly (on a weekly basis, for example) to maintain the security of the keys. See the procedures for:

- "Refreshing IPSec security keys for a link between MDM Servers" (page 76)
- "Refreshing IPSec security keys for the link between an MDM Server and MSS/MG15000 node" (page 78)

Note: When you refresh IPSec security keys, backup the workstations and the nodes to ensure that the keys will be synchronized in the event that a workstation or a node restore is required. Otherwise the security associations for both ends of the connection may have to be re-established. See "Synchronizing IPSec security associations in VoIP networks" (page 156).

To simplify administration and recovery, it is recommended that the same keys are used by an MDM Server to communicate with all its associated MSS/MG15000 switches.

Use of third party firewalls

If a third-party firewall is configured in front of the MSS/MG15000 node or the MDM workstation, refer to NN10114-511 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP* for port information that must be used to configure the firewall.

IPSec key management procedures for VoIP solutions

Use the following procedures to perform administration tasks for IPSec connections:

- "Refreshing IPSec security keys for a link between MDM Servers" (page 76)
- "Refreshing IPSec security keys for the link between an MDM Server and MSS/MG15000 node" (page 78)

Refreshing IPSec security keys for a link between MDM Servers

IPSec connections between MDM Servers are protected by both an authentication key and an encryption key. These keys should be refreshed regularly. These keys are updated manually and must be communicated between MDM Server sites in a secure fashion.

These keys are updated manually and must be communicated between MDM Server sites in a secure fashion.

Security keys can be displayed on the MDM Server. Refer to "Viewing MDM IPSec information" located in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*.

CAUTION
When an IPSec security key is refreshed for the security association at one end of a link, the link is not operational until the security association at the other end of the link is refreshed with the same security key.

Prerequisites

- Before refreshing the IPSec security key for the link between two MDM workstations, ensure there are secure operational connections between the MSS/MG15000 switches and MDM Servers, and between the MDM Servers and the higher level management system to ensure uninterrupted transmission of data.

- To use this procedure, designate one MDM Server as MDM1 and the other as MDM2.
- Use the IPSec configuration record compiled during the security activation phase to obtain the IP addresses and SPIs for security associations for both MDM Servers. Optionally, use the procedure "Viewing MDM IPSec information" located in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements* to determine the security association information.

Using a secure connection from the desktop

1 Log in to MDM1 as root.

2 Type the following command to update the IPSec encryption key for the security association to MDM2:

```
/opt/MagellanNMS/bin/ipsec_keyrefresh <MDM2_IPaddr> -
inSPI <x> -outSPI <y> -enc_alg aes generate
```

This commands updates the security association on MDM1 with a new encryption key, and outputs the security key value <aes_key> that will be entered in step 5.

The connection to the MDM2 is now disabled.

3 Type the following command to update the IPSec authentication key for the security association to MDM2:

```
/opt/MagellanNMS/bin/ipsec_keyrefresh <MDM2_IPaddr> -
inSPI <x> -outSPI <y> -enc_auth sha generate
```

This commands updates the security association on MDM1 with a new authentication key, and outputs the security key value <sha_key> that will be entered in step 6.

4 Log in to MDM2 as root.

5 Type the following command to update the IPSec encryption key for the security association on MDM2, using the value <aes_key> output in step 2:

```
/opt/MagellanNMS/bin/ipsec_keyrefresh <MDM1_IPaddr> -
inSPI <y> -outSPI <x> -enc_alg aes <aes_key>
```

The link between the two MDMs is now operational using refreshed keys.

6 Type the following command to update the IPSec authentication key for the security association on MDM2, using the value <sha_key> output in step 3:

```
/opt/MagellanNMS/bin/ipsec_keyrefresh <MDM1_IPaddr> -
inSPI <y> -outSPI <x> -enc_auth sha <sha_key>
```

The link between the two MDMs is now operational using refreshed keys.

Variable definitions

Variable	Definition
<MDM1_IPaddr>	is the IP address of MDM1
<x>	is the inSPI for the MDM1-based security association for the FTP data channel
<y>	is the outSPI for the MDM1-based security association for the FTP data channel
<aes_key>	is the aes encryption security key
<sha_key>	is the sha authentication security key

Refreshing IPSec security keys for the link between an MDM Server and MSS/MG15000 node

IPSec connections between an MDM Server and an MSS/MG15000 switch are protected by both an authentication key and an encryption key. These keys should be refreshed regularly.

MSS/MG15000 security keys are stored in the provisioning file in an encrypted format and cannot be displayed.

The security keys on both the MDM Server and the MSS/MG15000 switch can be refreshed from the MDM Server as long as a secure connection exists through the redundant MDM Server to the switch. If this connection does not exist, then the security associations on both the MDM Server and the switch for the link will have to be deleted and then re-created. For information on deleting and re-creating the security associations for the link between and MDM Server and MSS/MG15000 switch, refer to step 2 of the procedure

"Restoring an MSS/MG15000 switch in a secured network" in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*.

CAUTION
When an IPSec security key is refreshed for the security association at one end of a link, the link is not operational until the security association at the other end of the link is refreshed with the same security key.

Prerequisites

- Designate the MDM Server requiring the key refresh as MDM1. Designate the other MDM Server as MDM2.
- Make sure a secure operational connection exists between the MSS/MG15000 switch and MDM2 and between MDM1 and MDM2 to ensure uninterrupted transmission of data.
- Have a group, userid and password with a system impact of system administration for the MSS/MG15000 node, and the IP address for the MSS/MG15000 node.
- Use the IPSec configuration record compiled during the security activation phase to obtain the IP addresses and SPIs for the security associations for the link. Optionally, use the procedure "Viewing MSS/MG15000 IPSec information" located in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements* to determine the security association information.

Using a secure connection from the desktop

1 Log in to MDM1 as root.

2 Enter the following command to update the IPSec encryption security key for the FTP data channel on both MDM1 and the MSS/MG15000 switch:

```
/opt/MagellanNMS/bin/ipsec_keyrefresh <MSSMG_IPaddr>
-inSPI <x> -outSPI <y> -enc_auth MD5 generate -pp
<MDM2_IPaddr> <MSSMG_group> <MSSMG_userid> <MSSMG_pwd>
```

At this point, the FTP data channel between MDM1 and the MSS/MG15000 switch is operational.

3 Enter the following command to update the IPSec encryption security key on both MDM1 and the MSS/MG15000 switch for the other traffic channels on the link:

```
/opt/MagellanNMS/bin/ipsec_keyrefresh <MSSMG_IPaddr>
-inSPI <w> -outSPI <z> -end_alg aes generate -pp
<MDM2_IPaddr> <MSSMG_group> <MSSMG_userid> <MSSMG_pwd>
```

At this point, all the links between MDM1 and the MSS/MG15000 node are operational.

4 Enter the following command to update the IPSec authentication security key on both MDM1 and the MSS/MG15000 switch for the other traffic channels on the link:

```
/opt/MagellanNMS/bin/ipsec_keyrefresh <MSSMG_IPaddr>
-inSPI <w> -outSPI <z> -end_auth sha generate -pp
<MDM2_IPaddr> <MSSMG_group> <MSSMG_userid> <MSSMG_pwd>
```

At this point, the link between MDM1 and the MSS/MG15000 switch is fully operational.

Variable definitions

Variable	Definition
<MSSMG_IPaddr>	is the IP address of the MSS/MG15000 switch
<x>	is the inSPI for the MDM1-based security association for the FTP data channel
<y>	is the outSPI for the MDM1-based security association for the FTP data channel
<w>	is the inSPI for the MDM1-based security association for the other data channels
<z>	is the outSPI for the MDM1-based security association for the other data channels
<MDM2_IPaddr>	is the IP address of the redundant MDM Server providing the secure connection from MDM1 to the MSS/MG15000 switch
<MSSMG_group>	is the group name for the MSS/MG15000 switch

(Sheet 1 of 2)

Variable	Definition
<MSSMG_userid>	is the system administration userid for the MSS/MG15000 switch
<MSSMG_pwd>	is the system administration password for the MSS/MG15000 switch
(Sheet 2 of 2)	

Chapter 6
Platform security management

In a secure VoIP network, the MDM and MSS/MG15000 platforms have been hardened. Operating system hardening procedures are used to improve the resistance of commercial operating systems to attacks.

Multiservice Data Manager platform hardening

The Multiservice Data Manager platform has been secured in the following ways:

- The Solaris 9 operating system is hardened using the MDM supplied script. For more information on this script, see NN10600-605 *Nortel Multiservice Data Manager Network Security Fundamentals*.
- The **`traceroute`** commands can be executed only by the root userid.
- The **`ping`** command can be executed only by the root userid and userids belonging to the MDP group.
- **`Telnet`** access to the MDM has been turned off. All access from desktops and the Integrated EMS system must use SSH commands to connect to the MDM.
- The range of dynamically allocated IP ports has been restricted. For more information on the firewall port assignments, see NN10225-512 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP*.
- Access to the MDM by remote systems has been restricted using the /etc/hosts.allow and /etc/hosts.deny files.

Note: Each MSS/MG15000 node and MDM workstation is allowed access using **ftp** instead of **sftp**. All other systems will be required to use **sftp**.

- The Apache server is free of known buffer overflows at the time of the SN08 release.

Message banners, such as message of the day banner, FTP banner and telnet banner, are used to contain information warning users that MDM access has been restricted to authorized users only.

The following MDM local access parameters have been set:

- password length for local access is set to the maximum value of 8 characters
- local access passwords may be changed every 2 weeks, and must be changed every 12 weeks. Users are notified when their password is about to expire.
- a maximum of 3 log in attempts are allowed before the session is locked

Access to MDM software should be kept secure in the following ways:

- Ensure that administration tools can only be accessed by appropriately authorized users. Where supported, enable passwords for tool access For more information, see 241-6001-310 *Nortel Multiservice Data Manager Server Reference*.
- Where supported, use encrypted passwords for additional security. For more information, see “Securing the operating system and server infrastructure” in 241-6001-303 *Nortel Multiservice Data Manager Customization and Administration*.

Multiservice Switch 15000 and Media Gateway 15000 platform hardening

Access to the MSS/MG15000 nodes has been secured by:

- requiring idle local user access sessions to time out after 10 minutes
- requiring idle telnet sessions to time out after 10 minutes

- restricting the remote systems that are allowed access to the node. To view the list of system IP addresses that are allowed access to the node, enter the following command on the node: **`display Ac IpAccess`**
- restricting the remote systems that are allowed access to the node.

  To view the list of system IP addresses that are allowed access to the switch, enter the following command on the switch:
  `display Ac IpAccess`

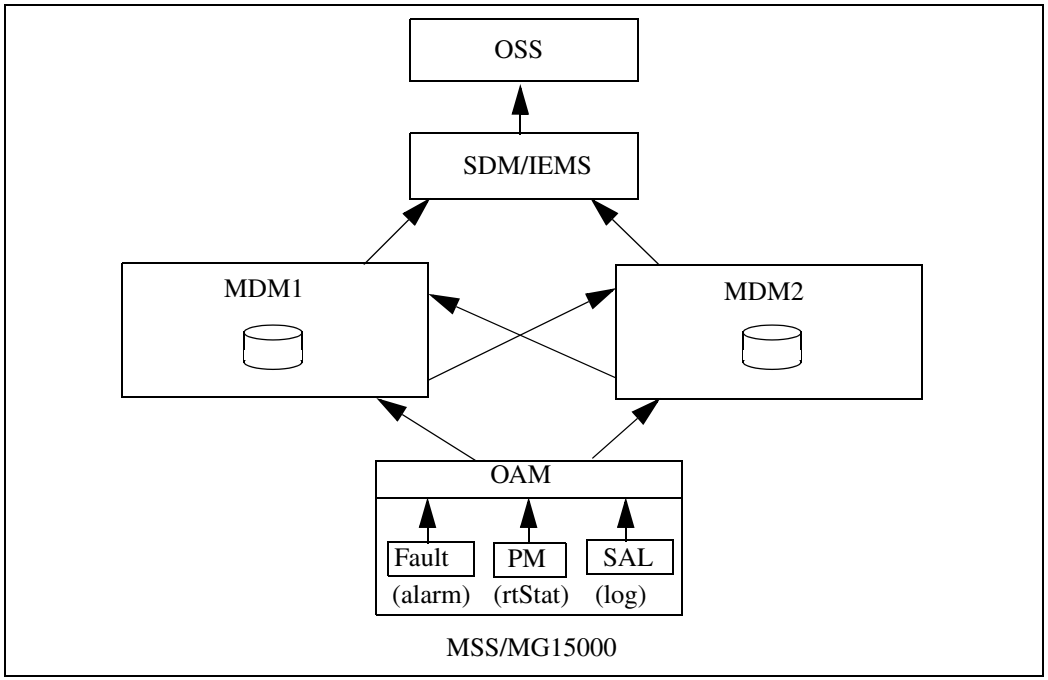
  To add an IP address to the list of system IP addresses that are allowed access to the switch, enter the following command on the switch:
  `set Ac IpAccess <IP_address>`

For more information, refer to NN10600-601 *Nortel Multiservice Switch 7400/15000/20000 Security Management*.

Chapter 7
Security audit logs

The security audit log flow for a single MSS/MG15000 node is shown in Figure 4. When a centralized Multiservice Data Manager (MDM) pair is used to manage multiple nodes, the architecture for security audit log interworking is maintained.

Figure 4
Security audit log (SAL) flow interworking architecture (1 node)



Audit log refers to an event that tracks (audits) user activity including logins/ logouts, commands executed, and/ or actions such as GUI-initiated actions. Audit log is synonymous with command log and is considered to be a subset of security logs.

Security log refers to audit logs as well as to some alarm logs that are classified as impacting security. In addition to user activity, some alarm logs are duplicated into the "security log" stream as they are classified as directly impacting security (for example, too many invalid login attempts). Specifically, this includes alarm logs where the alarm type is security or operator.

Nortel Multiservice Data Manager (MDM) Log Browser tool can be used from the MDM Toolset to statically view security audit logs stored in files on the MDM.

Types of security audit logs

Security audit logs that originate on MDM and MSS/MG15000 can be categorized as follows:

- Logging a direct human user/administrator action. Most of the different instances of a security audit log fall into this category and it is often a one-to-one (or one-to-a-few) mapping of an action to a security audit log. Some examples include:
  - — Logging in to an MSS/MG15000
  - — Acknowledge an alarm in the MDM alarm display
- Logging a user/administrator-initiated background activity. In MDM and MSS/MG15000, these activities can cause many security audit logs to be generated, although such activities do not typically occur on a regular basis. The set of activities includes:
  - — Commissioning a switch via NP Templates. Applying each template causes a security audit log and when the commands are sent to the MSS/MG15000, each add/set command causes its own security audit log. This would come in small bursts of roughly 10-100 commands per template.
  - — Retrieving the spooled historical files from MSS/MG15000 by MDP (i.e., historical alarms, SCN's, security audit logs). This would

typically involve only a few files of each type per day, assuming the recommended retrieval schedule is used. Security audit logs are issued for logins/logouts and for each retrieved file.

— When using SASM/SISM upgrade tools on MDM, the logins/logouts plus the actual provisioning commands are logged. However, the pre-checks and post-checks are not logged. The reason is that pre- and post-checks consist of Display commands, which are passive impact, and thus are not logged.

— When using MSS Backup and Restore tools on MDM, security audit logs are issued for logins/logouts and for each retrieved file on backup. On restore, a security audit log is issued for each restored prov file, but not for any downloaded software.

— When using software/patch downloading to MSS/MG15000 only the "Start" download command itself causes a security audit log on MSS/MG15000. Downloading does not cause per-file security audit logs.

— MDM auto-patching scripts generate security audit logs for logins

— Data Sync journaling

- Logging a machine-generated set of activities. Typically, this too is bursts of activity over short periods and there are not many of these in MDM and MSS/MG15000. The set of activities includes:

  — MDM automatically and continuously trying to regain connectivity to an MSS/MG15000. Any normal failover on loss of connectivity recovers in less than 1 minute, but within that time, multiple MDMs can be retrying multiple times.

  — MDM application having the wrong password for a MSS/MG15000 to which it is trying to connect. In this case, it will not connect until the configuration error is fixed. This should not occur except during initial setup or during regular maintenance when personnel are on hand to note and resolve such errors.

  — state-walks done by MDM after re-gaining connectivity do not generate security audit logs on the MSS/MG15000 other than the logins/logouts, if required. The reason is that state-walks consist of Display commands, which are passive impact, and thus are not logged.

Security audit log format

Security audit logs are formatted in a way appropriate for use by a higher level management system. This format is called Custlog V2 and has the following syntax:

```
syslog:_V2_~I=<nodeId>~H=<hostname>~A=<application>~S
=<sequence #>~~<log name> <log number> <alarmValue>
<eventType> Security Audit Log <restOfLog>
```

where:

<nodeId> is a short name identifying the system where the log originated. Standard format is <type><no>. examples are CM, MS0, SDM, GWC15, PTM1. This value is obtained through the command line argument -nodeId <nodeId> supplied to the salcserver.

<hostname> is the hostname of the machine from which the log originated. The MDM workstation name.

<application> is the name of the application that generated the log. On the MDM, this is the name of the salcserver process name.

<sequence number> is an integer from 0-9999. It increments for every log generated by the application. This number is generated by salcserver.

<log name> is a log report name consisting of 2 to 4 non blank characters. Either MDM or PPEM for OAMC or Multiservice Switch security log respectively.

<log number> is a log report number ranging from 0 to 999. The number used for all security audit logs is 601.

<alarm value> is the alarm severity level of the log report. This is a value of NONE for MDM and Multiservice Switch security logs.

<eventType> is a log report event type. This field is defined by the applications that generate the log report. It is a value of INFO for MDM and Multiservice Switch security logs.

<restOfLog> is the application specific log body text. This is part of the Nortel standard syslog record.

SCC2 output log record example

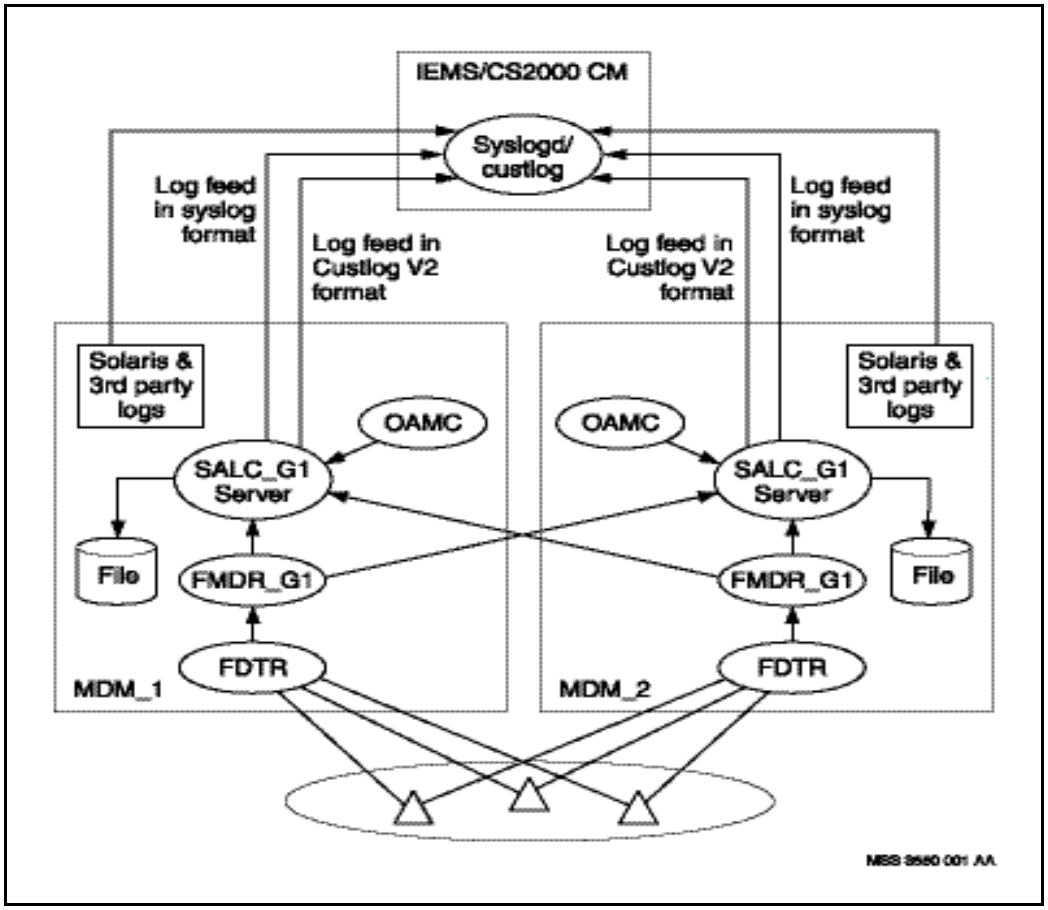
A sample SCC2 output log record is shown below:

```
38 MDM 601 0016 INFO Security Audit Log
Log from node MDM
Server_Daemon: class_security.ver01
LOG_DATE: 20040902T113856Z
SRC.USR: localhost
SRC: wcars0qp
MESSAGE: Started at 04-09-02 11:38 by localhost: End-
To-End Server;
restart#1\n
STAT: start
LOG.TYPE: security
DST: -
DOC: End-To-End Server
SRC.OFFEND: -
DST.USR: -
SRC.MAIL: -
REL: -
VOL: -
VOL.SENT: -
VOL.RCVD: -
CNT: -
CNT.SEND: -
CNT.RCVD: -
HOST: -
HOST.TYPE: -
PROG.FILE: -
PROG.LINE: -
TTY: -
PROT: -
CMD: -
EVNT.TYPE: -
SRC.OID: -
MID: MDM.SVMDMN.0
```

Security audit log flow to a higher level management system

The higher level management system (Integrated EMS for VoIP solutions and CS2000 Core Manager for VoA solutions) acts as the central log host for MDM workstation and MSS/MG15000 switch security audit logs for the central office. Security audit logs must be reviewed regularly to detect security breaches such as unauthorized login attempts or configuration changes. The NP Template Configuration Audit tool uses the security audit logs to display differences between the current MSS/MG15000 switch configuration and the configuration applied using an NP Template. “Security audit log flow to the higher level management system” (page 93) shows how security audit logs are collected from MSS/MG15000 switches and MDM workstations and sent to the higher level management system.

Figure 5
Security audit log flow to the higher level management system



"Summary MDM and MSS/MG15000 security logs being sent to a higher level management system" (page 94) lists the MDM workstation and MSS/MG15000 node security audit logs.

"Summary of desktop security logs not sent to a higher level management system" (page 95) lists security related logs that are generated on the desktop platform. These logs are not sent to the higher level management system.

Table 10
Summary MDM and MSS/MG15000 security logs being sent to a higher level management system

Log type	MDM log storage location	facility	sent to Integrated EMS	sent to CS2000 Core Manager
Solaris security logs				
PAM_Radius logs	/var/log/authlog	local1	yes	no
PAM_NSSwitch	/var/log/authlog	local1	yes	no
PAM mkdir logs	/var/log/authlog	local0	yes	no
Login logs (UNIX, X11)	/var/log/authlog	auth.*	yes	no
General UNIX logs	/var/adm/messages	*.*	yes	no
SSH and IPSec logs	/var/adm/messages	*.*	yes	no
MDM and MSS/MG15000 security audit logs				
MSS/MG15000 security audit logs (custlog V2 format)	/opt/MagellanNMS/data/security/security_custlog<_hlms name>.nlog	local1	yes	yes
MDM security audit logs (custlog V2 format)	/opt/MagellanNMS/data/security/security_custlog<_hlms name>.nlog	local1	yes	yes
MSS/MG15000 security audit logs (syslog format)		local3	optional	no
MDM security audit logs (syslog format)		local3	optional	no

(Sheet 1 of 2)

Table 10 (Continued)
Summary MDM and MSS/MG15000 security logs being sent to a higher level management system

Log type	MDM log storage location	facility	sent to Integrated EMS	sent to CS2000 Core Manager
Apache logs	/opt/nortel/logs/ 3rd_party/apache		no	no
Note 1: MSS/MG15000 security audit logs contain command information, login information, IPSec information, etc. ***Note 2:*** The Apache server on the MDM server supports the desktop Operator Client application. ***Note 3:*** <hlmsname> is the node name of the higher level management system				
(Sheet 2 of 2)				

For more information on the configuration required to send security audit logs to CS2000 Core Manager, see NN10114-511 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP*.

For more information on the configuration required to send security audit logs to Integrated EMS, see NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*.

Table 11
Summary of desktop security logs not sent to a higher level management system

Log type	log storage location
SAML logs	/opt/nortel/logs/applications/security/nsssaml/nss_saml.log
Operator Client application logs	/opt/nortel//logs/applications/desktop/plugin-mgmt.log

Chapter 8
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:

- "Carrier Voice over IP network node configuration with DCE" (page 98)
- "Displaying DCE account profiles" (page 100)
- "Changing your DCE operator account password" (page 101)
- "Creating new user accounts using DCE" (page 101)

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

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

DCE can be configured so that authentication is invoked only when the operator logs into Multiservice Data Manager. Separate user authentication is still required for logging in to Nortel 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 Multiservice Data Manager.

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 Multiservice Data Manager servers are unavailable), the administrator must ensure that this level of access is restricted to authorized operators.

Carrier Voice over IP network node configuration with DCE

In the Carrier Voice over IP 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 99) illustrates an example configuration.

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

- "Integrated log in" (page 98)
- "DCE availability" (page 98)

Integrated log in

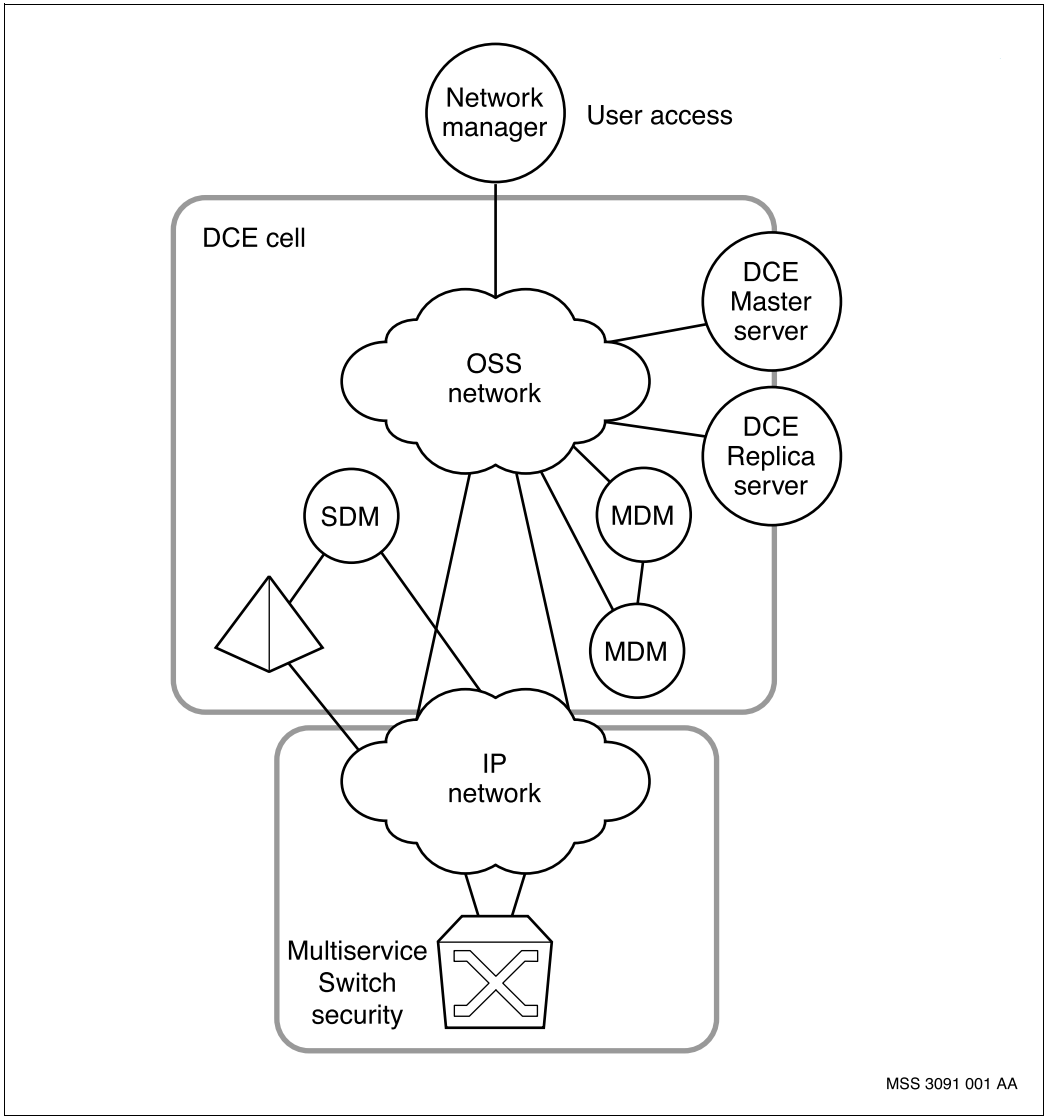
DCE is configured for integrated log in, which means the operator need log in to UNIX only; the DCE log in is automatic if the operator is authorized to enter the DCE cell. The administrator configures DCE authentication so that the operator's UNIX userid and password match a DCE userid and password. 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 log in to the server. Existing sessions are unaffected by this failure.

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

Figure 6
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 userid you entered at step 3 in the section “Creating new user accounts using DCE” (page 101)

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 log in 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 log in.

Procedure steps

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

   `/sdm/bin/create_dce_user`

2. Enter the administrator userid and password when prompted.
3. Enter the following information at the prompts:
   a. userid for the operator
   b. full name of the operator
   c. user group for this userid
   d. password for this userid (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. userid

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 100).

c. user group

d. shell for this userid

e. password

f. home directory

7 Select OK to complete the add operation.

Chapter 9
Multiservice Data Manager local user access administration

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

Userids, 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 “Userids configured on the Sun Fire™ V480 servers for VoA solutions” (page 104) lists all of the userids and passwords that were configured for a VoA solution during the Multiservice Data Manager software installation. The table “Userids configured on the Sun Fire™ V480 servers for VoIP solutions” (page 104) lists all of the userids and passwords that were configured for a VoIP solution.The names of the userids are recommended, but you can use your own names. As well, you will need to determine the passwords for all of your userids.

Table 12
Userids configured on the Sun Fire™ V480 servers for VoA solutions

Userid	Purpose	Group	Multiservice Data Manager user
root	Multiservice Data Manager root user		Yes
mdpadmin	administrative userid for the MDP application	mdpgroup	Yes
mdpprobe	probe userid for the MDP application	mdpgroup	Yes
pp15ksw	userid for the Multiservice Switch 15000 node Software Distribution Site		Yes
<>	surveillance and maintenance		Yes
Note 1: All other userids are maintained on the MDM central AAA server.			
Note 2: The userid mdm and its associated password (mdmpassword) are also used during this software installation. The mdm userid must be defined on the Communications Server LAN and Multiservice Switch 15000 nodes during each of their software installations. This userid and password are a suggested convention to follow, you can determine your own userid and password if you wish.			

Table 13
Userids configured on the Sun Fire™ V480 servers for VoIP solutions

Userid	Purpose	Group	Multiservice Data Manager user
root	Multiservice Data Manager root user		Yes
mdpadmin	administrative userid for the MDP application	mdpgroup	Yes
mdpprobe	probe userid for the MDP application	mdpgroup	Yes
Note: All other userids are maintained on the Integrated EMS central AAA server.			

For more information, see the following sections:

- “Adding additional local users” (page 105)
- “Adding additional local groups” (page 106)

- "Configuring the root user as a Multiservice Data Manager user" (page 107)

Adding additional local users

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

Procedure steps

1. Log in to the Multiservice Data Manager 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:

   For VoA networks, enter:

   passwd <userid>

   For VoIP networks with Integrated EMS providing central user authentication and authorization, enter:

   passwd -r files <userid>

   Note: If the command option *-r files* is not used on VoIP networks with Integrated EMS providing central authentication and authorization, the command will try to create the password for an Integrated EMS userid instead of the locally defined userid.
4. Enter a password for the new user at the prompt.
5. Make the new user a Multiservice Data Manager 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 userid must be unique.

Adding additional local 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 Multiservice Data Manager 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.

Changing the password for a local userid

Perform the following procedure to change the password for a local userid.

Procedure steps

1. Log in to the Multiservice Data Manager server as the *root* user.
2. Change the password for the new user:

   For VoA networks, enter:

   passwd <userid>

   For VoIP networks with Integrated EMS providing central user authentication and authorization, enter:

   passwd -r files <userid>

   Note: If the command option *-r files* is not used on VoIP networks with Integrated EMS providing central authentication and authorization, the command will try to change the password on an Integrated EMS userid instead of the locally defined userid.
3. Follow the command prompts to enter the new password and old password for validation.

Variable definitions

Variable	Definition
<userid>	is the user's ID. This userid must be unique.

Configuring the root user as a Multiservice Data Manager user

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

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

1. Log in to the Multiservice Data Manager 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 Multiservice Data Manager 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 Log out and then log back in to automatically restart the Multiservice Data Manager 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 Multiservice Data Manager application.

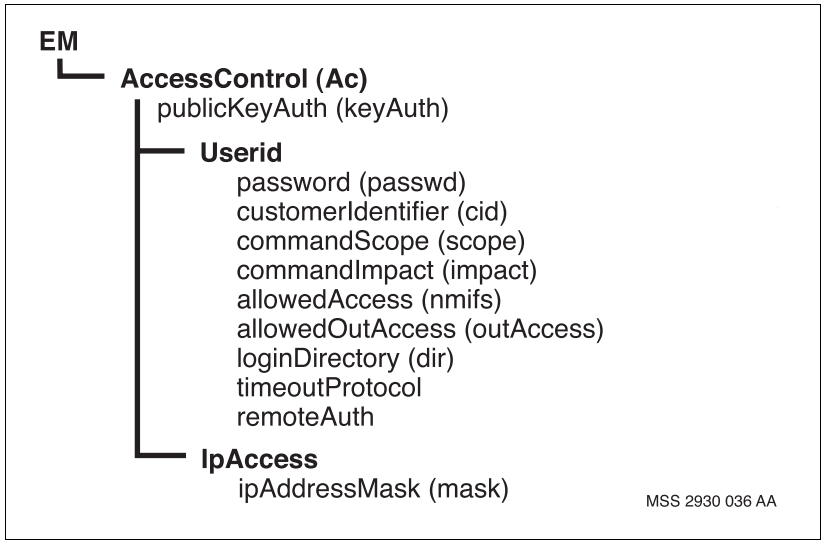
Note: After completing this procedure, you can launch the Multiservice Data Manager application on your desktop by entering the nmstool & command in a terminal window.

Chapter 10
Multiservice Switch local user access administration

Nortel Multiservice Switch access control restricts access to network nodes through userids, passwords, and authorized remote IP addresses. Operators must enter a valid userid 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 110) summarizes the associated components and attributes.

Figure 7
Access control components and attributes



Access control configuration can be done through the following tools:

- Nodal Provisioning tool (see 241-6001-610 *Nortel Multiservice Data Manager Nodal Provisioning User Guide*)
- Command Console tool (see 241-6001-804 *Nortel Multiservice Data Manager Workstation Utilities*)

The table "Summary of user access tasks" (page 110) summarizes the OAM tasks required for node security and access.

Table 14
Summary of user access tasks

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

Table 14
Summary of user access tasks (Continued)

OAM tasks	Relevant section
Setting or changing a user password	"Setting a password"
Changing a user profile	"Changing userID attributes"
Deleting a user profile, including its ID and password	"Deleting a userID"
Note: All references in the Relevant section column are to the User access configuration section of NN10600-601 *Nortel Multiservice Switch 7400/15000/20000 Security Management*.	

For complete information on access controls, see all sections of NN10600-601 *Nortel Multiservice Switch 7400/15000/20000 Security Management*.

For basic command line interface information, see "Command line interface basics" (page 111). For specific procedures for performing user access administration on nodes, see the following:

- "Adding a user using the CLI" (page 114)
- "Copying an existing userid for a new user using the CLI" (page 116)
- "Adding an IPAccess component using the CLI" (page 118)
- "Setting a password using a secure method" (page 119)
- "Changing a user profile and password using the CLI" (page 121)
- "Deleting a user profile using the CLI" (page 122)

Command line interface basics

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

- "Logging into CLI" (page 112)
- "CLI operational mode" (page 112)
- "CLI provisioning mode" (page 113)

Logging into CLI

Follow these steps to log in to CLI. For userids 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 userid at the userid prompt.
4. Enter the password at the password prompt.

   You are now logged in to 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 in to a Nortel 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 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 Multiservice Data Manager 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 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 121).

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 Carrier Voice over IP Networks, Nortel recommends always using a scope of "network". For more information on this attribute, see NN10600-601 *Nortel Multiservice Switch 7400/15000/20000 Security Management*.
<impact>	identifies the importance of the commands that the user can perform. Table 2, "Impact levels for Multiservice Switch 15000 nodes," (page 36) 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 userid for a new user using the CLI

You can copy an existing userid and all of its attributes, except password attributes. This is useful if you have a large number of userids 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 121).

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

Use the following procedure to copy an existing userid. Perform the following steps in provisioning mode. For information on working in provisioning mode, see NN10600-030 *Nortel 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 userid:

   ```
   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 121).

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

Variable definitions

Variable	Definition
<olduserID>	Is the existing userid
<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 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 userid associated with the changed password exists on both the secure and the non-secure node.

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

Procedure steps

1. Log in to 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 Multiservice Data Manager application such as Backup & Restore, do not use the same userid 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 in to the non-secure node using Multiservice Data Manager 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 Multiservice Switch 7400/15000/20000 Overview*.

13 End provisioning mode.

```
end Prov
```

Variable definitions

Variable	Definition
<userID>	Is name of the userid for which you are setting the password, or the name of the userid 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 userid 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 119) and “Risks” (page 121).

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 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 userid 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 userid with a command impact of *systemAdministration*.

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

Procedure steps

1. Remove the *userID* component:

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

Variable definitions

Variable	Definition
<userID>	Is the userid to be deleted.

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

Chapter 11
Using the Network Model tool to perform network surveillance

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

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 *Nortel Multiservice Data Manager Network Model Administration*.
2. Create a new organization called *CVoIP* within the network model. See the section on creating an organization in 241-6001-015 *Nortel Multiservice Data Manager Network Model Administration*.

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

3 Create a new region called *CVoIP* within the CVoIP organization. See the section on manually creating components and subcomponents in 241-6001-015 *Nortel Multiservice Data Manager Network Model Administration*.

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

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 Carrier Voice over IP Network office. See the section on manually creating components and subcomponents in 241-6001-015 *Nortel Multiservice Data Manager Network Model Administration*.

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

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

The two sites and the nodes representing the Multiservice Data Manager servers and the CVoIP 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 *Nortel Multiservice Data Manager Network Model Administration*.

Set the . . . to . . .

Collection Name	<customer defined>
Equipment Type	Multiservice Switch
MSS (Passport) Group	ACCESS
Userid	<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 Carrier Voice over IP Network component. See the section on manually creating components and subcomponents in 241-6001-015 *Nortel Multiservice Data Manager Network Model Administration*.

Set the . . .	to . . .
Node Name	GEN/<name of CVoIP 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 Ethernet Routing Switch 8600)	ERS8600/<name>
CSLAN (if not Ethernet Routing Switch 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 *Nortel Multiservice Data Manager Network Model Administration*.

10 Drag and drop all the remaining device icons (Multiservice Switch 15000, Ethernet Routing Switch 8600, Media Gateway 15000, MDM) to the appropriate site: the icon representing the servers onto the Multiservice Data Manager*MDM* site, and the icons representing the Multiservice Switch and Media Gateway nodes onto the correct Carrier Voice over IP 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 *Nortel Multiservice Data Manager Network Model Administration*.

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 *Nortel Multiservice Data Manager Network Model Administration*.

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 Multiservice Data Manager (MDM) does not add automatically. You can find all the sections referenced in the following procedure in the 241-6001-015 *Nortel Multiservice Data Manager Network Model Administration*.

Procedure steps

1 Enter edit mode In the Network Viewer. See the section on entering edit mode to enable editing in 241-6001-015 *Nortel Multiservice Data Manager Network Model Administration*.

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 *Nortel Multiservice Data Manager Network Model Administration*.

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 Multiservice Data Manager servers. See the section on using menu commands to create and edit links in 241-6001-015 *Nortel Multiservice Data Manager Network Model Administration*.

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 Multiservice Data Manager 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 *Nortel Multiservice Data Manager Network Model Administration*.

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 Multiservice Data Manager server to another

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

Procedure steps

1. Log in to the second server:

   telnet <MDM_name>

2. Enter the root userid 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 userid 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 Multiservice Data Manager server
<modelname>	Is the name of the model. In the example, the model name is CVoIP.
<privmdml>	Is the host name of the interface on the top port (qfe0) of the 4-port Ethernet card on the first Multiservice Data Manager server

Chapter 12
File Management on the Multiservice Data Manager server

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

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

For more information on managing various types of files stored on Multiservice Data Manager 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. Log 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 *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. Log in to the server.
2. Open a Multiservice Data Manager 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 *Nortel Multiservice Data Manager Customization and Administration*. For more information on the RTACCOL server, refer to 241-6001-310 *Nortel Multiservice Data Manager Server Reference*.

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 Log in 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 Log in 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. Log in 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.

Managing MDM log files

Perform the following procedure to create a cron job that will remove old MDM log files that have been stored on the system for more than the retention periods specified in the configuration file:
/opt/ MagellanNMS/cfg/MDMClean.cfg
This cron job is set to perform daily file removal.

The following directories should be added to the MDMClean.cfg:

- /opt/MagellanNMS/data/log/oamc
- /opt/MagellanNMS/data/log/svmdmn
- /opt/MagellanNMS/data/log/salcserver
- /opt/MagellanNMS/data/log/csvr
- /opt/MagellanNMS/data/log/ipm
- /opt/MagellanNMS/data/log/nat
- /opt/MagellanNMS/data/log/osh
- /opt/MagellanNMS/data/log/pcms
- /opt/MagellanNMS/data/log/pcserver

Procedure steps

1. Log in 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 files:

   ```
   crontab -e
   ```

   The cron file is opened with a text editor.
4. Add the following information to the cron file:

   ```
   55 0 * * * /opt/MagellanNMS/bin/mdmlogclean
   ```

   Note: This command uses the information in the file /opt/MagellanNMS/lib/cfg/MDMClean.cfg and can be overwritten by what is in /opt/MagellanNMS/cfg/MDMClean.cfg.
5. Save and close the cron file.

Managing auto-patch files

Use the mdmlogclean process to manage the disks that accumulate auto-patching log files. The process removes old auto-patch files that have been stored on the system for more than seven days.

The mdmlogclean process is used to clean up the temporary successful files, the failed files, and the optional verbose log files from the auto-patching process. MDMClean.cfg is the configuration file that controls the cleanup. This file consists of the records that define which directory the mdmlogclean process examines and the records that specify the length of time the files can accumulate in the directory.

You must populate the MDMClean.cfg file in the opt/MagellanNMS/cfg directory with the following:

```
Directory: /opt/MagellanNMS/data/log/ppautopatch

RetentionDays: 7
```

You can then run the mdmlogclean process, see “Managing MDM log files” (page 137).

Refer to Auto-patching, Disk management in NN10400-300 *Nortel Multiservice Data Manager Administration Tools* for more information.

Managing MDM syslog files

To ensure that the syslog files do not fill up the MDM disk, perform the following procedure to limit the amount of syslog data retained.

Procedure steps

1. Log in to the MDM server as the root user.
2. Open the /etc/logadm.conf file for editing:

   ```
   vi /etc/logadm.conf
   ```

3. Make the changes shown below as underlined text:

   /var/log/syslog -C 8 -P "Fri Sep 17 -7:10:00 2004’ **-S 10m** -a ’kill -HUP ‘cat /var/run/syslog.pid“ **-p 1d**

   /var/adm/message -C 4 -P "Fri Sep 17 -7:10:00 2004’ **-S 10m** -a ’kill -HUP ‘cat /var/run/syslog.pid“ **-p 1d**

   /var/log/authlog -C 4 -P "Fri Sep 17 -7:10:00 2004’ -S 10m -a ’kill -HUP ‘cat /var/run/syslog.pid“ -p 1d

   /var/adm/local -C 4 -P "Fri Sep 17 -7:10:00 2004’ -S 10m -a ’kill -HUP ‘cat /var/run/syslog.pid“ -p 1d

   /var/adm/local1 -C 4 -P "Fri Sep 17 -7:10:00 2004’ -S 10m -a ’kill -HUP ‘cat /var/run/syslog.pid“ -p 1d

   /var/adm/local3 -C 4 -P "Fri Sep 17 -7:10:00 2004’ -S 10m -a ’kill -HUP ‘cat /var/run/syslog.pid“ -p 1d

   /var/adm/local7 -C 4 -P "Fri Sep 17 -7:10:00 2004’ -S 10m -a ’kill -HUP ‘cat /var/run/syslog.pid“ -p 1d

   /var/cron/log -c -s 512k -t /var/cron/olog

```
/var/lp/logs/lpsched -C 2 -N -t '$file.$N'
```

4 Save and close the /etc/logadmin.conf file.

Chapter 13
Multiservice Data Manager software backup, restore, and synchronization

Configuring a Carrier Voice over IP Network with redundant paired Nortel 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 Multiservice Data Manager 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 Multiservice Data Manager workstation

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

Multiservice Data Manager dynamic data

Dynamic data consists of:

- active Nortel Multiservice Switch and Multiservice Data Manager alarms
- Multiservice Switch and Multiservice Data Manager 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.

Multiservice Data Manager collected data

Collected data is collected from Nortel Multiservice Switch nodes that are managed by Multiservice Data Manager workstations. Multiservice Data Manager 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)
- security audit logs (SALs) and syslogs

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 Carrier Voice over IP Networks, Multiservice Switch service data is static. Multiservice Switch backup data on a Multiservice Data Manager 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 Multiservice Data Manager 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 159).

Multiservice Switch spooled data is synchronized with the nodes. If a Multiservice Data Manager 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.

Security audit log and syslog 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.

Multiservice Data Manager configuration data

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

- Multiservice Data Manager 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.
- user access control data such as roles, policies, and the associations between users and roles for MDM Admin Servers

In a Carrier Voice over IP Network solution, Multiservice Data Manager configuration data is static and can be protected with a good backup procedure.

Generally the network model data only changes when new Nortel 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 Multiservice Data Manager workstations.

UNIX configuration data and core software

UNIX configuration data consists of the specific UNIX configuration data set up at workstation initialization. It includes userids and passwords, user data, network host addresses, cron jobs and security data. 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 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**)
- automated patching of MSS15000/MG15000 nodes from the MDM (**root crontab**)
- MDMClean.cfg file management (**root crontab**)
- syslog 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**.

In VoIP solutions, security data on the MDM Server includes:

- configuration data for the PAM_RADIUS and PAM_NSSwitch interfaces for communicating with the central AAA service provided by the Integrated EMS

- configuration information for sending syslogs to the Integrated EMS
- configuration information for IPSec protocols
- configuration information for SSH protocols

In a VoA network that uses central AAA on an MDM Admin Server, security data includes:

- configuration data for the RADIUS interface that enables the MSS15000/MG15000 nodes to authenticate with the MDM Admin Server

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.

Multiservice Data Manager core software

Nortel Multiservice Data Manager (MDM) core software is provided for a client-set workstation configuration, a server-set/standalone workstation configuration, an MDM Server configuration (VoIP network only) or an MDM Admin Server configuration (VoA network only). Multiservice Data Manager 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.

Multiservice Data Manager core software consists of:

- MDM Toolset software
- Operator Client support software:
  - JWS software
  - Operator Client GUI tools
  - Operator Client application software
  - Apache web server
- user access management software
  - user administration tools such as User Manager, Policy Manager, Security Settings and Session Manager

- authentication software
  - — Sun ONE IS software
  - — Sun ONE DS software
  - — RADIUS interface software

"Data mapping for Multiservice Data Manager workstation configurations" (page 146) shows the data relevant to each type of workstation configuration.Multiservice Data Manager

Table 15
Data mapping for Multiservice Data Manager workstation configurations

Data types	standalone	server-set	Client-set	MDM Admin Server (VoA only)	MDM Server (VoIP only)
Multiservice Data Manager dynamic data					
• Multiservice Data Manager and Multiservice Switch alarms	yes	yes	no	yes	yes
• network model states	yes	yes	no	yes	yes
Multiservice Data Manager collected data					
• 5 and 30 minute performance measurements	yes	yes	no	no	yes
• Alarms to support the Query Historical Alarms application	yes	yes	no	yes	yes
• Multiservice Switch backup and restore data	yes	yes	no	no	yes
• Processed Multiservice Switch spooled data	yes	yes	no	no	yes

(Sheet 1 of 2)

Table 15 (Continued)
Data mapping for Multiservice Data Manager workstation configurations

Data types	standalone	server-set	Client-set	MDM Admin Server (VoA only)	MDM Server (VoIP only)
• security audit logs and syslogs	yes	yes	no	no	yes
Multiservice Data Manager configuration data					
• Multiservice Data Manager services	yes	yes	no	yes	yes
• network model	yes	yes	no	yes	yes
• user access control data	no	no	no	yes	no
UNIX configuration data and core software					
• userids and passwords	yes	yes	yes	yes	yes
• network host addresses	yes	yes	yes	yes	yes
• user data	yes	yes	yes	yes	yes
• cron files	yes	yes	yes	yes	yes
• security data	no	no	no	no	yes
• Solaris operating system and configuration files	yes	yes	yes	yes	yes
Multiservice Data Manager core software					
• MDM Toolset software	yes	yes	yes	yes	yes
• Operator Client support software	no	no	no	yes	yes
• user access management software	no	no	no	yes	no
• authentication software	no	no	no	yes	no

(Sheet 2 of 2)

Understanding impacts of Multiservice Data Manager workstation outages

When two Nortel 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 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 Multiservice Data Manager administrator is unsure if changes have been made to the operational Multiservice Data Manager workstation and not applied to the out of service workstation.

"Impacts of workstation outages on Multiservice Data Manager data" (page 148) lists the impacts of workstation outages on Multiservice Data Manager data.

Table 16
Impacts of workstation outages on Multiservice Data Manager data

Data type	Impact to data
Multiservice Data Manager dynamic data	Active alarms and network model states are lost. The data will automatically resynchronize with the operational workstation data after the workstation is rebooted. [1]Multiservice Data Manager
Multiservice Data Manager 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 3)	

Table 16 (Continued)
Impacts of workstation outages on Multiservice Data Manager data

Data type	Impact to data
• Multiservice Data Manager 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 Multiservice Data Manager backup.
• 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 Multiservice Data Manager workstation has returned to service. Information will be retrieved from the node at the next collection interval.
• security audit logs and syslogs	Log files will have a gap for the SAL and syslog records generated during the out of service period. The data cannot be recovered.
Multiservice Data Manager 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 Multiservice Data Manager 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 Multiservice Data Manager workstation, changes made since the last backup must be applied manually. • In VoIP solutions, IPSec security keys restored from backup may no longer be synchronized with the MSS15000/MG15000 nodes or the other MDM workstation. These keys must be resynchronized manually. • Solaris operating system software is lost and must be restored from backup or from supplier sources.

(Sheet 2 of 3)

Table 16 (Continued)
Impacts of workstation outages on Multiservice Data Manager data

Data type	Impact to data
Multiservice Data Manager core software	For a simple outage, there is no impact to Multiservice Data Manager software. For a complex outage, the software is lost and must be restored from backup or from Multiservice Data Manager source files.
Note 1: Synchronization between Multiservice Data Manager 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 Multiservice Data Manager workstation is recovered.	
(Sheet 3 of 3)	

Backing up and restoring Multiservice Data Manager 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.

Multiservice Data Manager 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.

Table 17
MDM directories to backup

Directory	Description
/opt/MagellanNMS/cfg	MDM base software configuration
/opt/MagellanNMS/data	MDM base software data
/opt/nortel/config	Supports the Admin Server
/opt/nortel/data	Supports the Admin Server
/opt/nortel/logs	Supports the Admin Server
/opt/nortel/EPIC/cfg	Supports the Enhanced Passport Interface Controller
/opt/MagellanMDP/cfg	MDP base software configuration Backup is required only if MDP is installed
/opt/MagellanMDP/data	MDP base software data Backup is required only if MDP is installed

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/~

  Note: To prevent having to re-create your customizations, backup the configuration files in /opt/nortel/config/applications/ desktop prior to a software upgrade.

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
- /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 Multiservice Data Manager workstation software

Nortel 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 Multiservice Data Manager workstation, make sure that the workstation is restored from the same type of workstation. That is:

- a server-set is restored only from a server-set backup
- a standalone is restored only from a standalone backup
- an MDM Server is restored only from an MDM Server backup
- an MDM Admin Server is restored only from an MDM Admin Server backup
- a client-set is restored only from the client-set backup.

Backing up and restoring the Sun ONE servers of the MDM Admin Servers in VoA solutions

The following table lists the necessary tasks and references to back up and restore procedures required to back up and restore the Sun ONE servers in a VoA solution. Refer to NN10600-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration* for all of the procedures listed in the table.

Table 18
Sun ONE server backup and restore procedures in a VoA solution

Task	Procedure	Notes
Backing up the Sun ONE Directory Server	Backing up Sun ONE Directory Server	Backup up all the user, role, policy, identity server configuration, Sun ONE Directory Server configuration and security setting stored in the LDAP directory. In a replicated server deployment, you must backup both servers.
Restoring Sun ONE Directory Server	Restoring one Sun ONE Directory Server in a replicated pair	Restoring the Sun ONE Directory Server overwrites existing files on both Directory Servers. Any modifications you have made are lost.
	Restoring both Sun ONE Directory Servers in a replicated pair	Restoring the Sun ONE Directory Server overwrites existing files on both Directory Servers. Any modifications you have made are lost.
Backing up user data	Backing up desktop user interface data	Backup files that can be modified by a user and whose changes would be lost in the event of a system failure. To prevent having to recreate your customizations, prior to a software upgrade, backup the configuration files in /opt/nortel/config/ applications/ desktop.
Restoring user interface data	Restoring desktop user interface data	Copy the files you backed up to their original locations.

Synchronizing Multiservice Data Manager workstations

A Nortel 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 and no data has been changed manually on the workstation, 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 Multiservice Data Manager workstation software" (page 153).

Synchronizing configuration files

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

Note: This procedure should only be performed for server-set, standalone, MDM Admin Server, or MDM Server workstations.

Note: Refer to "Impacts of workstation outages on Multiservice Data Manager data" (page 148) to review the data that will be synchronized by this procedure.

Procedure steps

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

1. Log in 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/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 Multiservice Data Manager server to another" (page 130) 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).

Synchronizing IPSec security associations in VoIP networks

An IPsec connection will not work if the security associations assigned to that connection do not use the same security keys. Security keys can become unsynchronized when:

- a switch or workstation is out of service, and the IPSec security keys are refreshed on the other switches or workstations
- switch or workstation software is restored from backup, and an IPSec security key refresh has occurred since the backup was made.
- a switch experiences a reboot or restart, and the current active security keys have not been saved in the committed provisioning file.

When the security keys become unsynchronized, the security association applied at each end of the IPSec connection must be deleted and re-created using common security keys.

If the MDM Server or MSS/MG15000 switch has experienced a simple outage such as a system reboot, and none of the IPSec security keys on the other workstation or switches have been updated, the IPSec security keys will still be aligned and the IPSec links will automatically reconnect when the workstation or switch is restarted. No manual intervention is required.

If the MDM Server or MSS/MG15000 node experiences a complex outage where it has been out of service for a lengthy period of time, and/or the software was restored from backup, then it is likely that the IPSec security keys are no longer aligned. If the IPSec connections are no longer operational, refer to NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements* for procedures on restoring an MDM Server or an MSS/MG15000 switch in a secured network.

Chapter 14
Multiservice Switch software backup and restore

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

- "Backup site creation" (page 159)
- "Software backup" (page 162)
- "Restoring software" (page 165)

Backup site creation

- "Configuring the backup site" (page 159)
- "Configuring automatic backups to the backup site" (page 161)

Configuring the backup site

Perform this procedure to configure Nortel Multiservice Data Manager (MDM) server as a Nortel Multiservice Switch 15000 backup site. Refer to 241-6001-807 *Nortel Multiservice Data Manager Network Backup and Restore* for more information.

Note: Only configure the node backup site on the first Multiservice Data Manager server.

Procedure steps

1 Log in 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 Multiservice Data Manager user:

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

6 Log in to the server as the *ppbackup* user.

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

```
vi $HOME/PPBackupFull.list
```

This file lists the Multiservice Switch 15000 nodes in the HGDS group on which the server performs a full back up. Add the following information to the *PPBackupFull.list* file:

```
-full PASSPORT -group <HGDS group name> -auth <userid
for HGDS group> <full path to encrypted passwd file for
HGDS group>
```

8 Save and close the *PPBackupFull.list* files.

9 Open the *PPBackupInc.list* file with a text editor:

```
vi $HOME/PPBackupInc.list
```

This file lists the Multiservice Switch 15000 nodes in the HGDS group on which the server performs an incremental back up. Add the following information to the *PPBackupInc.list* file:

```
- incr PASSPORT -group <HGDS group name> -auth <userid
for HGDS group> <full path to encrypted passwd file for
HGDS group>
```

10 Save and close the *PPBackupInc.list* files.

Variable definitions

Variable	Definition
-full	the -full attribute stipulates a full backup
-incr	the -incr attribute stipulates an incremental backup
<HGDS group name>	the -group attribute refers to the HGDS group; one line is required for each HGDS group
<userid><full path to encrypted passwd file for HGDS group>	the -auth attribute refers to the userid for HGDS group and full path to the encrypted password file for the HGDS group, the password can be encrypted and is the full path and filename of the encrypted file

Configuring automatic backups to the backup site

When the Nortel 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 Log in to the Multiservice Data Manager 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 *PPBackupFull.list* file and the *PPBackupInc.list*:

```
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/nsbck -f $HOME/
PPBackupFull.list -log >& $HOME/pbackup.log.`date
+%Y%m%d`
32 1 * * 1-6 /opt/MagellanNMS/bin/nsbck -f $HOME/
PPBackupIncr.list -log >& $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 day Monday through Saturday at 01:32.

5 Save and close the cron file.

Variable definitions

Software backup

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 Multiservice Switch 15000 node to a reliable data storage site. The backup site can be a Nortel 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 Log in to the server if you are not already logged in.

2 Open a Multiservice Data Manager 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 > MSS > Administration > 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 Nortel Multiservice Data Manager (MDM) server has been configured to regularly backup the provisioning files from Nortel 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.

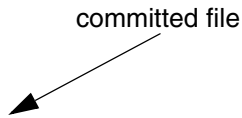
Procedure steps

1 Display the committed view and the current view:

```
display prov committedFileName, currentViewFileName
```

Figure 8
Sample output for displaying provisioning views

```
21> display prov
Prov
   adminState = unlocked
   operationalState = enabled
   usageState       = idle
   provisioningActivity = none
   activityProgress     = n/a
   standbyCpActivity    = none
   standbyCpActivityProgress= n/a
   committedFileName= hsm_221_8_20_01.full.001
   currentViewFileName= hsm_221_8_20_01.full.001
   lastUsedFileName= hsm_221_8_20_01.full.001
   provisioningSession=
   provisioningUser= none
   checkRequired= no
   confirmRequired= no
   editViewName= hsm_221_8_20_01.full.001
   editViewAddedComponents= 0
   editViewDeletedComponents= 0
   editViewChangedComponents= 0
```



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 *Nortel Multiservice Data Manager 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.

Synchronizing IPSec security associations in VoIP networks after restoring software

Refer to “Synchronizing IPSec security associations in VoIP networks” (page 156) for information on synchronizing IPSec security associations after restoring MSS/MG15000 switch software.

Appendix A
Summary of MDM tools and Operator Client application tools

MDM Toolset and Operator Client application tools

Nortel Multiservice Data Manager (MDM) tools are password protected to protect Multiservice Data Manager configuration. Accessing a Multiservice Data Manager tool requires a valid userid and password. The passwords are secured in the Server Administration tool by password encryption. Centralized AAA is available when operators access the network using the Operator Client application, however, centralized AAA is not available when you access the network through the MDM Toolset.

All system administration tasks must be performed using the MDM Toolset environment. As administrator, you configure policies, roles, and users using the MDM Toolset to enable central AAA and allow operators to have access to certain tools through an Operator Client interface. You can configure users to have access through both the Operator Client interface and the MDM Toolset interface, but if you want to control what a user can see and do, configure the user to be centrally authenticated with access through the Operator Client application only. This means that once you have defined the policies, roles and user privileges on the MDM for centrally authenticated users with Operator Client access, you should remove the local UNIX access to the MDM Toolset for those users.

The table “Multiservice Data Manager tools and utilities” (page 169) summarizes Multiservice Data Manager tools and utilities that you use to manage Multiservice Switch and Media Gateway 15000 nodes within the PT-AAL1, UA-AAL1 and UA-IP solutions.

Refer to 241-6001-122 *Nortel Multiservice Data Manager Using MDM Tool Set and Operator Client Interfaces* for more information about MDM Toolset and Operator Client interfaces and login.

Tools and Utilities for the Operator Client application

Operator Client provides an alternate user interface for operator tools to access MSS/MG15000 nodes through the MDM. This user interface is launched from a web browser that can be on an operator's UNIX desktop or PC.

Enhanced user administration system action authorization provides a finer-grained level of authorization. You will use the MDM Toolset Policy Manager to create policies that restrict user access and dictate the level of access available to users or groups of users in the Operator Client environment. Within these policies, you, as the administrator, can assign a policy to a role that limits an operator's access to the tools and the network. Multiple users can be associated with multiple policies and roles.

Operator client provides access to many but not all of the operational tools available within the MDM Toolset. Unlike the MDM Toolset, where each tool launches as a separate instance on the UNIX desktop, tools in Operator Client are hosted within the Operator Client desktop. The administrative tools that are not available in Operator Client are supported on the MDM Toolset.

Operator Client does not provide access to administrative tools such as the Server Administration tool, the Host Group Directory Server tool, or the MDP administrative tools. These tools are accessed through the MDM Toolset.

The table "Multiservice Data Manager tools and utilities" (page 169) summarizes Multiservice Data Manager tools and utilities that you use to manage Multiservice Switch and Media Gateway 15000 nodes within the PT-AAL1, UA-AAL1 and UA-IP solutions.

Refer to 241-6001-122 *Nortel Multiservice Data Manager Using MDM Tool Set and Operator Client Interfaces* for more information about MDM Toolset and Operator Client interfaces and login.

Table 19
Multiservice Data Manager tools and utilities

Tool or utility	Area of application					MDM Toolset	Operator Client
	F	C	A	P	S		
Alarm Display: Active	Y					yes	yes
Alarm Help	Y					yes	yes
Change Password			Y		Y	yes	yes
Command Console		Y	Y			yes	yes
Component Information Viewer	Y					yes	yes
Component Status Display	Y					yes	no
Data Synchronization Administration			Y			yes	no
Data Viewer				Y		yes	yes
EPIC	Y					yes	no
GMDR Administration			Y			yes	no
Host Group Administration			Y			yes	no
IP Discovery			Y			yes	no
Log Browser			Y		Y	yes	yes
Memory Utilization			Y			yes	no
MSS Service Data Backup and Restore			Y			yes	no
MSS Shelf View	Y					yes	yes
Network Browser	Y					no	yes
Network model shared memory utilization			Y			yes	no
Network Status Bar	Y					yes	yes
Network Viewer	Y					yes	no
Nodal Provisioning		Y				yes	yes
Online documentation	Y	Y	Y	Y	Y	yes	yes

(Sheet 1 of 2)

Table 19 (Continued)
Multiservice Data Manager tools and utilities

Tool or utility	Area of application					MDM Toolset	Operator Client
	F	C	A	P	S		
Operational Commands		Y	Y			yes	yes
Query Historical Alarms	Y					yes	no
Password encryption					Y	yes	no
Remote Access			Y			yes	no
Remote Telnet Access			Y			yes	yes
SASM		Y	Y			yes	no
Server Administration			Y			yes	no
Service Selection			Y			yes	yes
SISM		Y	Y			yes	no
Software Download and Configuration		Y	Y			yes	no
System Log Display			Y			yes	no
UNIX Access			Y			yes	no

(Sheet 2 of 2)

Appendix B
Mapping of Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000 access privileges to Integrated EMS groups in VoIP networks

In VoIP solutions, Integrated EMS maintains a single set of userids for access to all the MDM workstations and MSS/MG15000 switches in the associated central office. This centralization promotes ease of managing the userids across multiple switches and workstations, and reduces the time to make necessary changes.

Integrated EMS user group mappings

Integrated EMS provides thirty user groups consisting of six device areas with five associated security levels. These user groups are mapped onto the MDM and MSS/MG15000 access privileges.

The six Integrated EMS device areas are:

- ln: line services management. This category is not used for MDM or MSS/MG15000 management functions.
- tk: trunk services management. This category is not used for MDM or MSS/MG15000 management functions.
- mgc: media gateway controller management. This category is used for MSS/MG15000 management functions
- gw: gateway management. This category is not used for MSS/MG15000 management functions.
- ems: EMS management. This category is used for MDM functions.

- sec: security management. This category is not used for MDM or MSS/MG15000 management functions.

The five Integrated EMS security areas and how they are used for MSS/MG15000 and MDM management functions are:

- ro (read only) level provides the ability to display surveillance information, but not to alter it.
- rw (read/write) level provides the ability to display surveillance information and to do configuration of MSS/MG15000.
- mtc (maintenance) level provides the ability to configure MSS/MG15000 nodes. Operator Client application access is not supported.
- sprov (subscriber provisioning) level is mapped to the system administration impact level for MSS/MG15000 nodes and provides access to MSS/MG15000 administration tools from the Operator Client application.
- adm (administration) level is mapped to the debug impact level for MSS/MG15000 nodes and provides access to all MDM resources except MDP. A special local MDM userid is required to access MDP functionality.

Integrated EMS group mapping for MDM Toolset functionality

"Integrated EMS user group mapping for MDM Toolset functions" (page 172) shows the mapping between the Integrated EMS groups and the MDM Toolset functions.

Table 20
Integrated EMS user group mapping for MDM Toolset functions

MDM Toolset functions	Integrated EMS group					MDM local userid
	emsro	emsrw	emsmtc	emssprov	emsadmin	root
Alarm Display: Active	allow	allow	deny	allow	allow	allow
Alarm Help	allow	allow	allow	allow	allow	allow
Command Console	allow	allow	deny	allow	allow	allow
(Sheet 1 of 4)						

Table 20 (Continued)
Integrated EMS user group mapping for MDM Toolset functions

MDM Toolset functions	Integrated EMS group					MDM local userid
	emsro	**emsrw**	**emsmtc**	**emssprov**	**emsadmin**	**root**
Component Information Viewer	allow	allow	deny	allow	allow	allow
Component Status Display	allow	allow	deny	allow	allow	allow
Data Synchronization Administration	allow	allow	allow	allow	allow	allow
Data Viewer	deny	deny	deny	allow	allow	allow
Disruptive Command Safeguard	deny	deny	deny	deny	allow	allow
Enhanced Multiservice Switch interface controller (EPIC)	deny	allow	deny	allow	allow	allow
General management data router (GMDR) administration	deny	allow	deny	allow	allow	allow
Host group directory server (HGDS) administration	deny	allow	deny	allow	allow	allow
Log Browser	allow	allow	deny	allow	allow	allow
MDM license	deny	allow	deny	allow	deny	allow
MDM release update	deny	allow	deny	allow	allow	allow
MDP configuration	deny	deny	deny	deny	deny	deny
MDP log viewer	deny	deny	deny	deny	deny	deny
MDP data viewer	deny	deny	deny	allow	allow	deny
Memory utilization	allow	allow	allow	allow	allow	allow
Network Activation Tool	deny	allow	deny	allow	allow	allow

(Sheet 2 of 4)

Table 20 (Continued)
Integrated EMS user group mapping for MDM Toolset functions

MDM Toolset functions	Integrated EMS group					MDM local userid
	emsro	emsrw	emsmtc	emssprov	emsadmin	root
MSS Service Data Backup and Restore	deny	deny	allow	deny	allow	allow
Network Model shared memory utilization	allow	allow	allow	allow	allow	allow
Network Status Bar	allow	allow	deny	allow	allow	allow
Network Viewer	allow	allow	deny	allow	allow	allow
Nodal Provisioning	deny	allow	deny	allow	allow	allow
Nodal Provisioning Template	deny	allow	deny	allow	allow	allow
On-line documentation	allow	allow	allow	allow	allow	allow
Operational commands	allow	allow	deny	allow	allow	allow
Password Change	deny	deny	deny	deny	allow	allow
Password encryption	deny	deny	deny	deny	deny	deny
Query Historical Alarms	allow	allow	deny	allow	allow	allow
Quick Start	deny	deny	deny	deny	deny	allow
Server administration	deny	allow	deny	allow	allow	allow
Service selection	allow	allow	deny	allow	allow	allow
Shelf view	allow	allow	deny	allow	allow	allow
Software download	deny	deny	allow	deny	allow	allow
Succession ATM Software Migration	deny	allow	deny	allow	allow	allow
Succession IP Software Migration	deny	allow	deny	allow	allow	allow
System log display	allow	allow	deny	allow	allow	allow

(Sheet 3 of 4)

Table 20 (Continued)
Integrated EMS user group mapping for MDM Toolset functions

MDM Toolset functions	Integrated EMS group					MDM local userid
	emsro	emsrw	emsmtc	emssprov	emsadmin	root
UNIX access	deny	deny	deny	deny	allow	allow
Note: MDP configuration and log viewer commands must be accessed using the MDP administrator userid maintained locally on the MDM workstation.						
(Sheet 4 of 4)						

Integrated EMS group mappings for MDM Operator Client

"Integrated EMS user group mapping for MDM Operator Client tools" (page 175) shows the mapping between the Integrated EMS groups and the tools available through the Operator Client application.

Table 21
Integrated EMS user group mapping for MDM Operator Client tools

MDM Operator Client Resources	Integrated EMS group				
	emsro	emsrw	emsmtc	emssprov	emsadmin
Fault					
Alarm Display	allow	allow	deny	allow	allow
Alarm Help	allow	allow	allow	allow	allow
Net Browser	allow	allow	deny	allow	allow
Network Status Bar	allow	allow	deny	allow	allow
Component Information Viewer	allow	allow	deny	allow	allow
Shelf View	allow	allow	deny	allow	allow
Configuration					
Nodal Provisioning	deny	deny	deny	allow	allow
Template editor	deny	deny	deny	deny	allow
Performance					
Data Viewer	deny	deny	deny	allow	allow
(Sheet 1 of 2)					

Table 21 (Continued)
Integrated EMS user group mapping for MDM Operator Client tools

MDM Operator Client Resources	Integrated EMS group				
	emsro	**emsrw**	**emsmtc**	**emssprov**	**emsadmin**
System Administration					
Service Selection	allow	allow	deny	allow	allow
Log Browser	allow	allow	deny	allow	allow
Security					
Change Password	deny	deny	deny	deny	deny
Utilities					
Operator Commands	deny	allow	deny	allow	allow
Command Console	deny	allow	deny	allow	allow
Telnet	deny	allow	deny	allow	allow
NTPs	allow	allow	allow	allow	allow

(Sheet 2 of 2)

Integrated EMS group mappings for MSS/MG15000 functionality

"Integrated EMS user group mapping for MSS/MG15000 access privileges" (page 177) shows the mapping between the Integrated EMS groups and the MSS/MG15000 access privileges.

Table 22
Integrated EMS user group mapping for MSS/MG15000 access privileges

MSS/ MG15000 UserId attribute	**Integrated EMS group**				
	mgro	**mgrw**	**mgmtc**	**mgsprov**	**mgadmin**
Command Scope	network	network	network	network	network
Command Impact	passive	service	configuration	sysadm	debug
Customer Identifier	0	0	0	0	0
Allowed Access	FMIP	FMIP	FMIP FTP	FMIP FTP Telnet	FMIP FTP Telnet Local
Allowed Out Access	no	no	no	no	yes
Login DIrectory	/	/	/	/	/
Time Out Protocol	enabled	enabled	enabled	enabled	enabled

Appendix C
IPSec administration procedures for VoIP networks

The following procedures can be used to display IPSec security association information:

- "Viewing MSS/MG15000 IPSec information" located in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*.
- "Viewing MDM IPSec information" located in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*
- "Displaying IPSec security association information for call connections on the MG15000 shell interface" (page 179)

Displaying IPSec security association information for call connections on the MG15000 shell interface

The following are examples of the commands that can be used to display the IPSec policy data that has been provisioned on an Nsta component with the output of an existing SA on the same Nsta.

Prerequisites

- A userid and password with a system impact of system administration.

Using a secure connection from the desktop:

1. Log in to the MG15000 as system administrator.
2. DIsplay all the security associations defined on the switch, showing the direction of data flow and the associated source IP address and destination IP address:

   d -p Nsta/8 Vgs Ctrl/mg Spd/pvgb Policy/*

   A sample command output is shown below:

```
> d -p Nsta/8 Vgs Ctrl/mg Spd/pvgb Policy/*
Nsta/8 Vgs Ctrl/mediaGateway Spd/PVGB Policy/*

Use -noTabular to see hidden attributes: saProposal, ikePolicy and

description.
+======+-------------+-------------+-----+-----+-----+------+------
|Policy| sAddr       | dAddr       |proto|sPort|dPort|direct|action
+======+-------------+-------------+-----+-----+-----+------+------
|     1|47.142.82.220|172.31.80.182| udp |2944 | 2944|inbound|apply
|    2|172.31.80.182|47.142.82.220| udp |2944 | 2944|outbound|apply
ok           2005-04-06 09:53:12.32
```

   A pair of inbound/outbound entries with matching source and destination addresses and matching source and destination ports constitutes the pair of security associations (highlighted in bold text in the sample). Use the policy identifiers in the step 3 to determine the SPD.

3. Display the Policy 1 SA uptime, TTL, encryption algorithm, authentication algorithm, and replay protection settings for the security associations:

   d Nsta/8 Vgs Ctrl/mediaGateway spd/pvgb Policy/1 Sa/*

A sample command output is shown below:

```
Nsta/8 Vgs Ctrl/mediaGateway Spd/PVGB Policy/1 Sa/*
Use -noTabular to see hidden attributes: otherErrors, replayErrors,
   authErrors and packetCount.
+=====+=======+==========+=======+====+=========+========+==========
|SA   |upTime |remaining |saTime |pfs |encryptAl|authAl  | replay
|     |seconds|TimeToLive|ToLive |    |gorithm  |gorithm | protect
|     |       |seconds   |seconds|    |         |        | ion
+=====+=======+==========+=======+====+=========+========+==========
|61729| 207   |    93    |  300  |off |  null   | sha1   | on
ok           2005-04-05 10:36:37.14
```

Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks

Security and Administration

PT-AAL1/UA-AAL1/UA-IP

(I)SN08 and up

Publication: NN10180-611
Document status: Standard
Document version: (I)SN08 and up S1
Document date: June 2005
Printed in Canada

NORTEL