Carrier VoIP

MSS15K, MG15K, and MDM in Carrier VoIP Networks Security and Administration (PT-AAL1/UA-AAL1/UA-IP)

NN10180-611

Document status: Standard
Document version: 09.01
Document date: 20 October 2006

Contents

New in this release

There are no feature impacts in this document for this release.

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 11)
- "Administration of Multiservice Data Manager servers and Multiservice Switches using Multiservice Dat" (page 14)

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)

In VoA networks, the MDM platform can be secured by optionally applying the following features:

- restricting the ability to use the ping and traceroute functions

For more information, see "Platform security management" (page 57).

Communications security

Communications between MDM workstations, MSS/MG15000 nodes and other network elements 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 48).
- 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 48).
- 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 49).
- 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 IEMS workstations use SSH to encrypt all data including passwords. For more information, see "Secure Shell (SSH) protocol for VoIP solutions" (page 48).
- Authentication sessions are protected by using RADIUS, IPsec (VoIP only), obfuscation, HTTPS and SAML protocols.
- For solutions where sessions between MDM workstations and other MDM workstations or management systems are not protected with IPSec, SSH or other security protocol, SunScreen firewall software can optionally be used. For more information, see "Use of firewalls" (page 50).

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 15).
- Restricted access to MDM Toolset tools. Authorization to access MDM Toolset tools is controlled by the UNIX user group to which the userid is assigned. This feature is required as part of the VoIP security activation and is optional for VoA. For more information, see Restricting access to MDM Toolset tools.
- 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" (page 21).
- IEMS centralized authentication and authorization for VoIP solutions. The IEMS workstation provides user authentication and authorization for all MDM Toolset and Operator Client userids for an MDM workstation, and for the MSS/MG15000 nodes managed by it. For more information, see "Centralized user access management using IEMS" (page 39).

Security audit logs

An essential part of managing a 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 IEMS (for VoIP solutions) or to the CS2000 Core Manager (for VoA solutions) for central access and storage. Additional security audit logs are generated by the Solaris operating system and other third-party software packages.

If Server Platform Foundation Software is installed on the MDM, platform monitoring logs are also generated.

For more information on security audit logs, see "Security audit logs" (page 61).

Administration of Multiservice Data Manager (MDM) servers and Multiservice Switches using MDM

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 Appendix "Summary of MDM Toolset and Operator Client application tools" (page 203) or *241-6001-303 Nortel Multiservice Data Manager Administration*.

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" (page 21).

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 IEMS. For more information on using IEMS for central user authentication and authorization, see "Centralized user access management using IEMS" (page 39).

For more information on local user access management, see:

- "Multiservice Data Manager local user authentication and authorization" (page 15)
- "Multiservice Data Manager local user authentication and authorization for Multiservice Switch nodes" (page 17)

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.

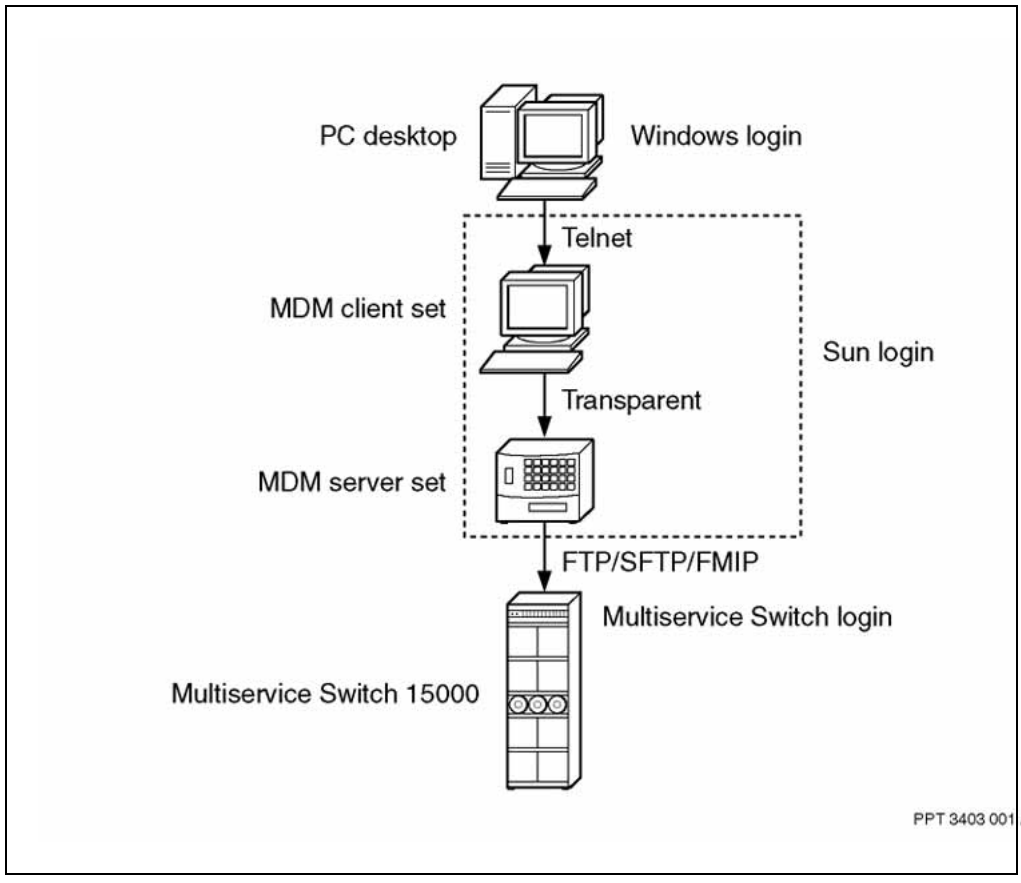
Operators who directly log in to Multiservice Data Manager require standard Multiservice Data Manager authentication (valid UNIX userid and password). This level of authentication provides access to the UNIX platform only, and permits the user to launch Multiservice Data Manager servers and to run scripts.

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 17). For more information about the security tools, see Appendix "Summary of MDM Toolset and Operator Client application tools" (page 203).

The figure "Multiservice Switch node and Multiservice Data Manager security management" (page 16) shows the levels of security.

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 17) defines the OAM security procedures required for MDM.

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.	

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) can be configured.

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

- "User profile impact levels" (page 18)
- "Security and access tasks" (page 18)
- "Secure FTP authentication" (page 48)

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).

"Impact levels for Multiservice Switch 15000 nodes" (page 18) identifies the impact levels available on Nortel Multiservice Switch 15000 nodes within the network.

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

"Security and access tasks for Multiservice Switch 15000 nodes" (page 18) identifies the security and access tasks required for Nortel Multiservice Switch 15000 nodes within the network.

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

Use case title and description	Frequency or time of use	Required input	Notes
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

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 *NN10440-450 Nortel Carrier Voice over IP Upgrade and Patches*
- 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/PT-IP/PT-AAL2*
- 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/PT-IP/PT-AAL2*
- 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 22)
- 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)

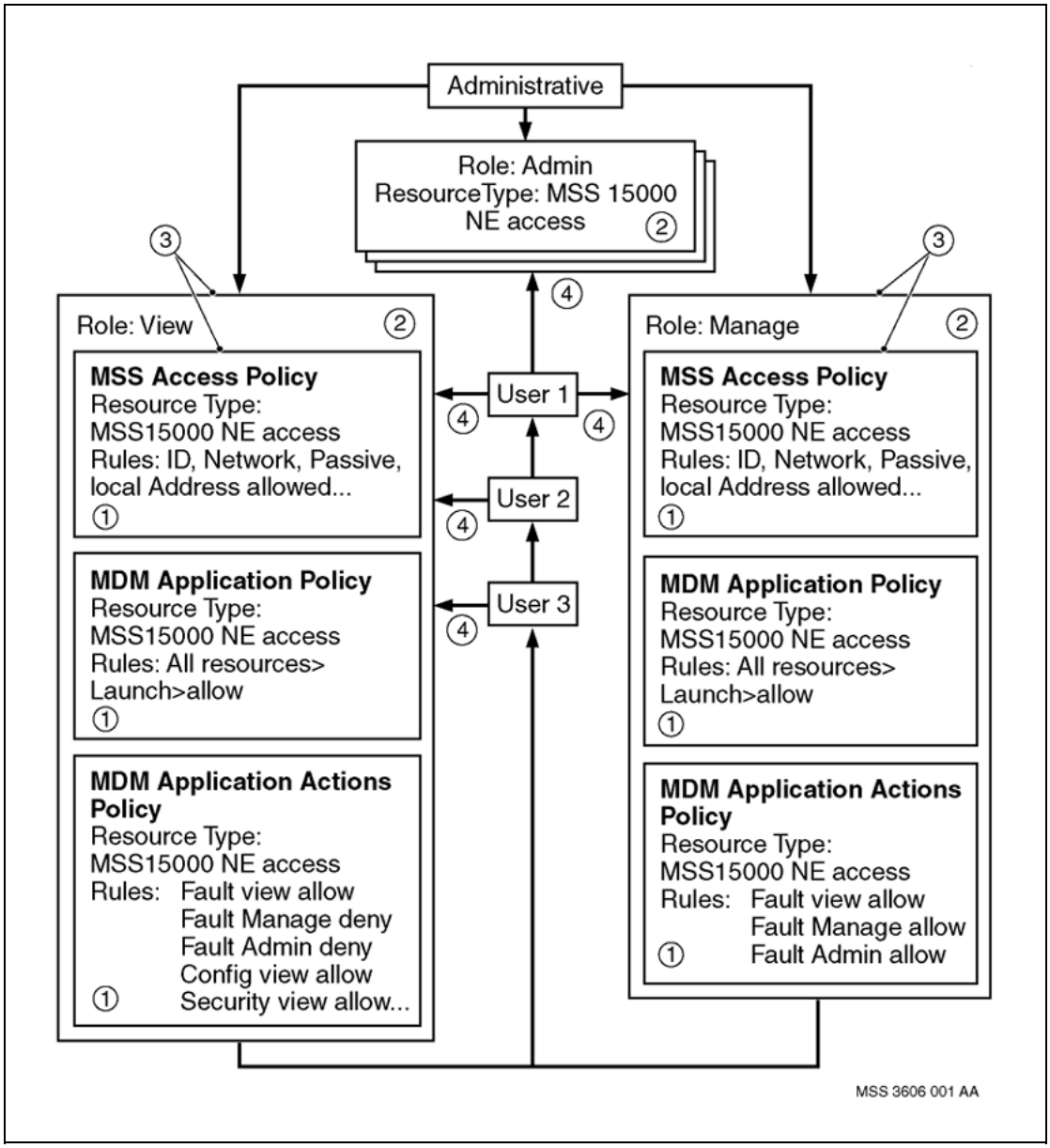
To administer access to the network, you must configure policies, which are applied to roles, to which you associate users. The combination of a policy and a role defines the access permitted to a user. See "Administering policies, roles, and users in a VoA solution with central AAA" (page 24).

The following list is the legend for "Administering policies, roles, and users in a VoA solution with central AAA" (page 24). 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 24) for an example of the values in a configured policy for users that are associated to a view only role.

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



An example of View Access Configuration Attributes - MDM Application Actions

Attribute	Value
Policy Name MDM	Application Actions View

Attribute	Value
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 *NN10400-605 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/PT-IP/PT-AAL2*.

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 *NN10400-605 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/PT-IP/PT-AAL2*.

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 49)
- 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

Step	Action
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 *NN10400-606 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 *NN10400-606 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).

4 This procedure is complete.

—End—

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 29).

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	Creating a Policy	*NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*

Action	See procedure	Reference
example, MSS15000 access definition, MDM tool access, and MDM tool actions).		
Configure the required roles. ***Note:*** Roles are used to group users that perform common tasks. Refer to *NN10400-605 Nortel Multiservice Data Manager Network Security Fundamentals* for more information about roles.	Creating a role	*NN10400-606 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	*NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*
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	*NN10400-606 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/PT-IP/PT-AAL2*

Action	See procedure	Reference
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.	*NN10400-606 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
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	*NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*

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 Toolset and Operator Client Interfaces* for initial log in procedures.
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 Toolset 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 Toolset and Operator Client Interfaces*.

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 *NN10400-606 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 *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration* that are required for account maintenance.

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.

Activity	Task	Refer to Procedure	Notes
	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.
	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-UrlAccess-Agent account password	"Changing the password for the amService-UrlAccessAgent account"	

Activity	Task	Refer to Procedure	Notes
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.
	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.

Activity	Task	Refer to Procedure	Notes
	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.
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 adm inistration 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.
	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	"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,

Activity	Task	Refer to Procedure	Notes
	authenticated from the MSS/ MG15000		to having access defined by the RADIUS server centrally authenticated.

Centralized user access management using IEMS

In VoIP solutions, IEMS 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.

IEMS user access management

IEMS 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. IEMS procedures provide for:

- configuring user settings
- configuring scope and group settings

For details on using IEMS to manage user access, refer to *NN10336-611 IEMS 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 IEMS is not available. MDP tools can only be accessed using local userids. "Local userids and groups to be retained on the MDM server" (page 40) lists the userids and groups that remain as local userids and groups after the migration of userids to the IEMS. 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 IEMS.

Local userids and groups to be retained on the MDM server

Local userids		Local groups		
root	daemon	root	adm	sysadmin
bin	sys	staff	noaccess	nortel
adm	nobody	other	uucp	sys
noaccess	Nortel	daemon	nogroup	nuucp
sshd	<mdpadmin>	bin	tty	nobody
		<mdpgroup>		
patcher		patcher		

Note 1: <mdpadmin> and <mdpgroup> may be different values, depending on how the MDP administrator userid and group were defined at installation time. Use the values set at installation.

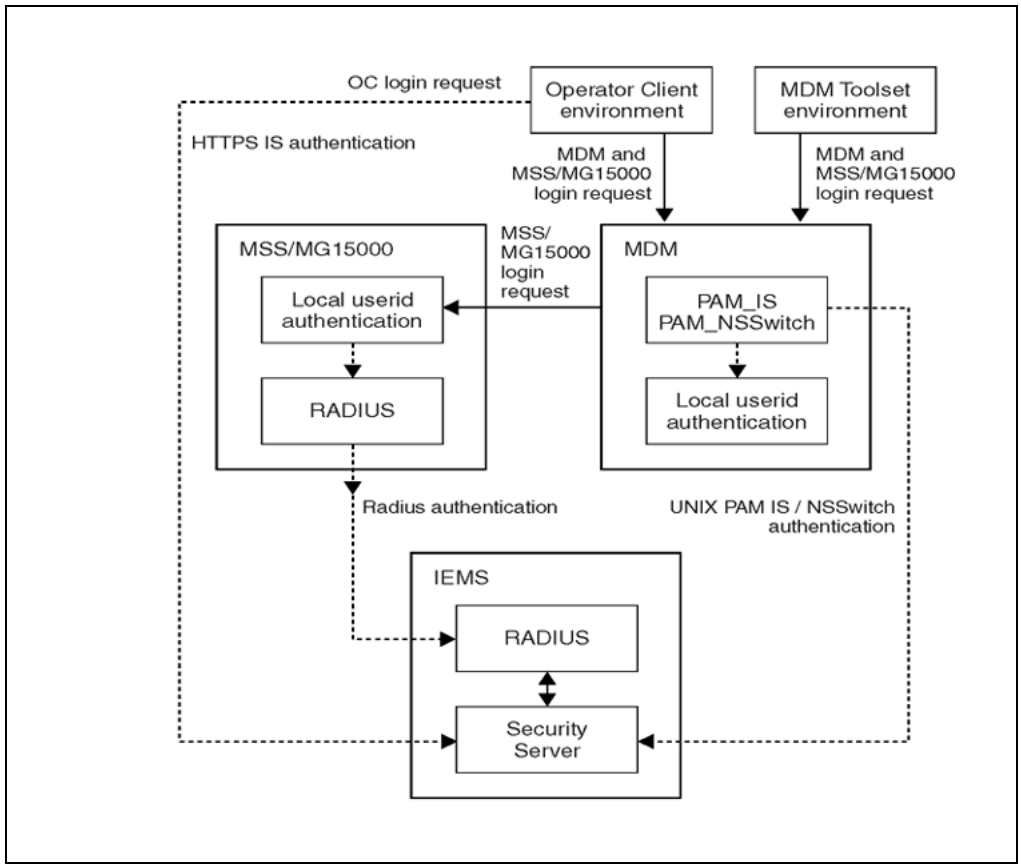
Note 2: The "patcher" userid and group are only retained as local on the MDM N240 server that hosts the NPM.

Some MSS/MG15000 userids must also be maintained as local userids. In case that the connection to IEMS 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 IEMS central AAA service

"User authentication and authorization data flow with IEMS" (page 41) shows the data flow for user authentication and authorization in VoIP solutions using IEMS central AAA service.

User authentication and authorization data flow with IEMS



MDM Toolset environment

The MDM sends an MDM Toolset login message via the PAM IS interface to the IEMS security server for authentication. When the IEMS 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 IEMS 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 IEMS 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 IEMS 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 IEMS system. When the IEMS 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).

IEMS user group mappings

The IEMS user groups and the mapping of the MDM and MSS/MG15000 access privileges onto these groups are shown in Appendix "Mapping of Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000 access privi" (page 211).

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

Administration procedures for IEMS central AAA service

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

- "Updating the MDM Server when the IEMS amadmin password changes" (page 42)
- "Updating the MSS/MG15000 switch when the IEMS RADIUS shared secret changes" (page 43)
- "Updating the MSS/MG15000 switch when the IEMS IP address changes" (page 44)
- "Updating JWS software when the MDM Server host name changes" (page 45)
- "Updating the MDM Server when the IEMS host name changes" (page 46)

Updating the MDM Server when the IEMS amadmin password changes

If the password for the IEMS 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 IEMS *amadmin* userid is distributed to the MDMServer site using a secure method.

Procedure steps

Step	Action
1	Log in to the MDM Server as root.

2 Execute the following commands:

```
cd /opt/nortel/applications/security/current_nssaml/sw
mgmt/bin

./configure_nssaml.sh -subcomponent password
```

3 At the prompt, enter the new IEMS *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>
```

4 This procedure is complete.

—End—

Variable definitions

Variable	Definition
<IEMS_amadmin_pwd>	is the new password for the IEMS *amadmin* userid

Updating the MSS/MG15000 switch when the IEMS RADIUS shared secret changes

If the IEMS 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

Step	Action
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
```

11 This procedure is complete.

—End—

Variable definitions

Variable	Definition
<new_shared_secret>	is the new IEMS Radius shared secret

Updating the MSS/MG15000 switch when the IEMS IP address changes

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

Procedure steps

Step	Action
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 IEMS 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
```

11 This procedure is complete.

—End—

Variable definitions

Variable	Definition
<new_IEMS_IPaddr>	is the new IEMS 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

Step	Action
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.

3 This procedure is complete.

—End—

Updating the MDM Server when the IEMS host name changes

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

Procedure steps

Step	Action
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 IEMS host name as prompted.
4	This procedure is complete.

—End—

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 47) shows the various management connections between MDM workstations, MSS/MG15000 nodes, and the IEMS workstation, and the protection method used for each connection. See "IP Security (IPSec) protocol for VoIP solutions" (page 49) for more information about MG15000 signalling connections.

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	IEMS	authentication data	PAM IS and PAM NSSwitch
MDM server	IEMS	fault and performance data	encryption using SSH
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
IEMS security server	MSS/MG15000	authentication data	RADIUS
IEMS security server	Operator Client desktop	authentication data	HTTPS, JAAS

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 *NN10440-450 Nortel Carrier Voice over IP Upgrade and Patches*.

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 *NN10440-450 Nortel Carrier Voice over IP Upgrade and Patches*. 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*

> ***Note:*** SSH-related files for MDM with SPFS are located in the following directory: /opt/openssh/etc.

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 *NN10400-607 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.

When digitally signed certificates are being used, security policies are statically configured but security associations are not. As a result the security associations will be lost on a system reboot, restart or CP switchover but will be renegotiated.

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 interfac" (page 217).

For more information on IPSec for MDM workstations, see *NN10400-607 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 51)
- "Refreshing IPSec security keys for the link between an MDM Server and MSS/MG15000 node" (page 53)

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 135)

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.

Internet Key Exchange (IKE) is the standard way for two IPSec clients to establish security associations or data encryption keys automatically.

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/PT-IP/PT-AAL2* for port information that must be used to configure the firewall.

Use of firewalls

SunScreen firewall software is an effective method of delivering congestion controls to counter denial of service (DOS) attacks in networks that do not use communication security features such as IPSec and SSH. For more

information, see section "SunScreen firewall deployment and configuration" in *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/PT-IP/PT-AAL2*.

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/PT-IP/PT-AAL2* for port information that must be used to configure the firewall.

IPSec 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 51)
- "Refreshing IPSec security keys for the link between an MDM Server and MSS/MG15000 node" (page 53)

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

Step	Action
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.

7 This procedure is complete.

—End—

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

Step	Action
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.

5 This procedure is complete.

—End—

Variable definitions

<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
<MSSMG_userid>	is the system administration userid for the MSS/MG15000 switch
<MSSMG_pwd>	is the system administration password for the MSS/MG15000 switch

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.

In a secured 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 such as denial of service (DOS) attacks and viruses.

In VoA networks, the MDM platform can be optionally hardened.

Multiservice Data Manager platform hardening

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

The Multiservice Data Manager platform has been hardened in the following ways in a VoIP network that has been secured:

- The Solaris 9 operating system is hardened using the MDM supplied OS hardening script. For more information on this script, see *241-6001-303 Nortel Multiservice Data Manager Administration*.
- 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 IEMS system must use SSH commands to connect to the MDM. SSH-related files for MDM with SPFS are located in the following directory: /opt/openssh/etc.
- 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/PT-IP/PT-AAL2*.

- 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 Administration*.

In a VoA network, the use of the ping and traceroute functions may optionally be restricted to help prevent denial of service (DOS) attacks such as broadcast pings, routed broadcast ping DOS attack, and viruses. See the procedure "Restricting ping and traceroute functions in VoA networks" (page 58).

Restricting ping and traceroute functions in VoA networks

Step	Action
1	Login to the MDM as root.
2	Execute the following command to allow only the root userid to execute the traceroute command:

```
chmod 500 /usr/sbin/traceroute
```

3 Execute the following commands to allow only the root userid, members of the MDP group, and the mpadmin userid to execute the ping command:

```
chmod 500 /usr/sbin/ping
setfacl -m -r group:<mdpgroup>:r-x /usr/sbin/ping
chmod u+s /usr/sbin/ping
setfacl -m user:mpadmin:r-x /usr/sbin/ping
```

4 This procedure is complete.

—End—

Variable Definitions

Variable	Definition
<mdpgroup>	is the name of the MDP group

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:

  ```
  list 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:

  ```
  list 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:

  ```
  add Ac IpAccess/<IP_address>
  ```

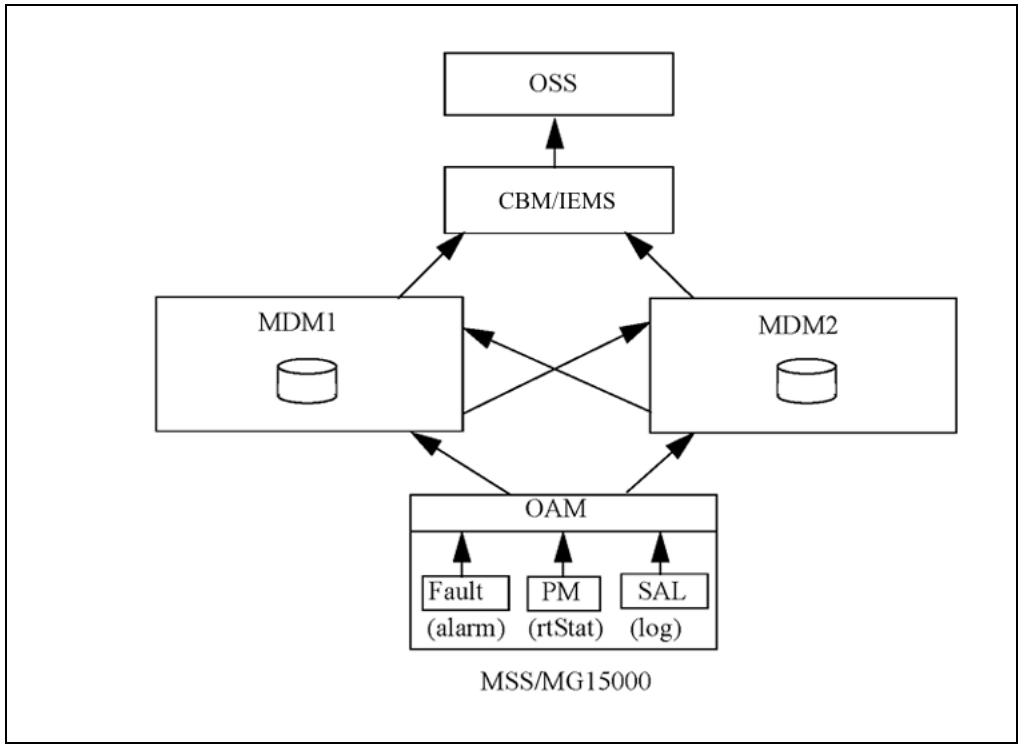
For more information, refer to *NN10600-601 Nortel Multiservice Switch 7400/15000/20000 Security Management*.

Security audit logs

Security audit logs are generated by Multiservice Data Manager servers and MSS/MG15000 switches to track events that impact the security of the system. MDM server security audit logs are generated by the MDM application and by the operating system and third party software that is running on the hardware platform.

The security audit log flow for a single MSS/MG15000 node is shown in "Security audit log (SAL) flow interworking architecture (1 node)" (page 61). When a centralized Multiservice Data Manager (MDM) pair is used to manage multiple nodes, the architecture for security audit log interworking is maintained.

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 server and MSS/MG15000 can be categorized as follows:

MDM software and MSS/MG15000 security audit logs

- 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
  - Applying Nodal Provisioning service templates to commission MSS/MG15000 nodes, or re-applying the templates to modify the configuration
- 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.
  - Auditing node level configuration when the Configuration Audit Scheduler runs an audit task it generates a security audit log per

audited node. This log captures audit information such as audit task start time, audit status, audit report location.

— 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.

— MSS/MG15000 generates security audit logs when the auto-patching scripts initiate the FTP login to MSS/MG15000.

— 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.

Platform security audit logs

Other types of security audit logs are generated by the Solaris operating system and third party software, including:

- authentication logs generated by:
  - the Base Security Module (BSM) in the Solaris operating system for MDM local logins and UNIX logins.
  - the SunOne Identification Server for Operator Client logins (VoA only)
  - PAM_IS for logins authenticated by IEMS central AAA (VoIP only)
- IPSec and SSH logs (VoIP only)
- general UNIX logs

For VoIP networks, logging of Solaris operating system and third party software events using the Solaris Base Security Module (BSM) is activated when the network is secured. For information on securing a VoIP 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*.

For VoA networks, the Solaris BSM can optionally be activated by executing the MDM OS Hardening script. To activate the Solaris BSM for VoA networks, refer to the procedure "Hardening the Solaris operating system" in *241-6001-303 Nortel Multiservice Data Manager Administration*.

For more information on third-party software generated logs, see the section "Third-party security audit logs" in *NN10400-605 Nortel Multiservice Data Manager Network Security Fundamentals*.

For systems with SPFS installed, SPFS records log events generated by the operating system, third party software applications, and SPFS service applications. "Summary of SPFS log events and log file locations" (page 64) shows the types of events logged, and where the log files are stored on the server.

Summary of SPFS log events and log file locations

Log type	Storage location
alarm logs and customer visible information	/var/log/customerlog
user actions taken	/var/log/auditlog
authentication events	/var/log/authlog
security events	/var/log/securitylog
software or hardware errors	/var/log/debuglog

Log type	Storage location
platform events	/var/log/sspfslog
log system sanity events	/var/log/marklog
file system events	/var/log/filesys/fs.log /var/log/filesys/lv.log
webservices events	/var/log/tomcat/catalina.out
Network Patch Manager events	/var/log/npm_designlog

Security audit log format

Security audit logs that are sent to a higher level management system are formatted using a format called Custlog V2 which 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:

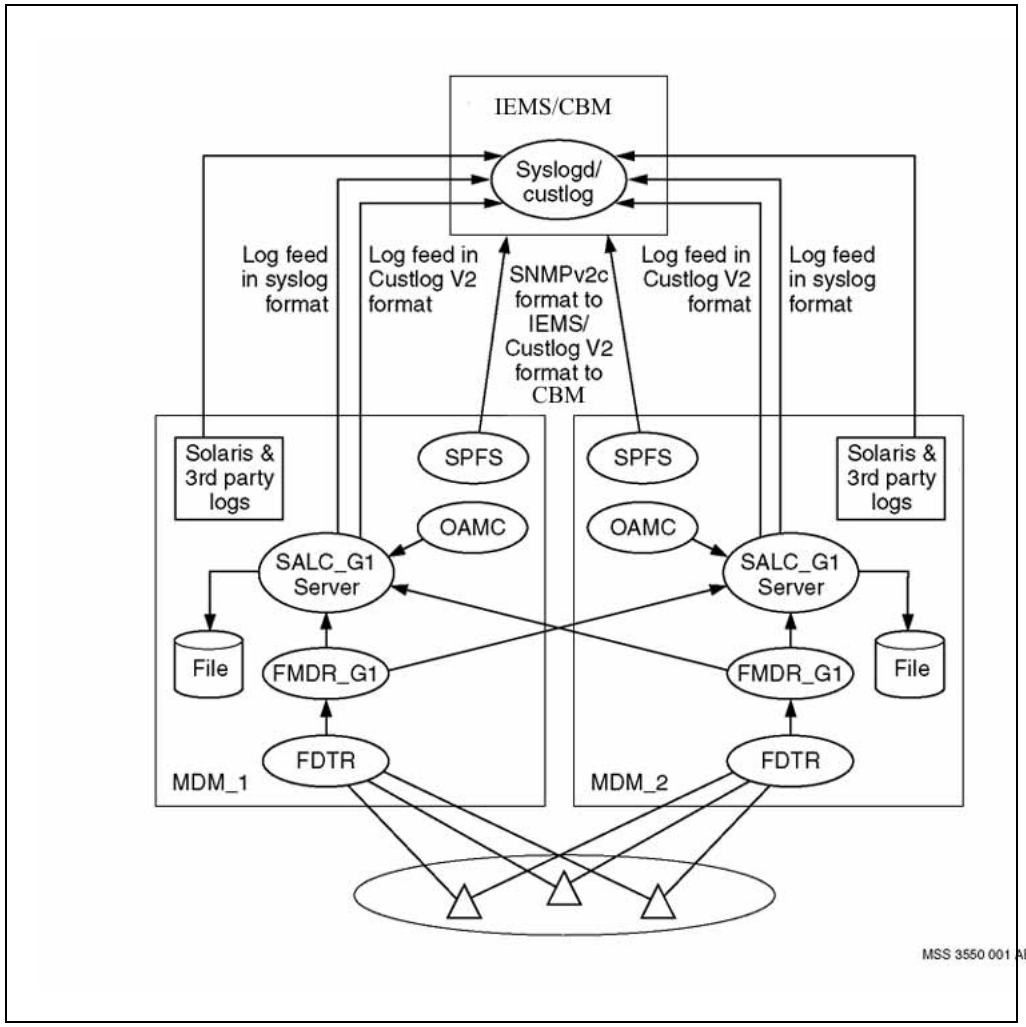
```
38 MDM 601 0016 INFO Security Audit Log
```

```
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 (IEMS 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 67) shows how security audit logs are collected from MSS/MG15000 switches and MDM workstations and sent to the higher level management system.

Security audit log flow to the higher level management system



"Summary of MDM and MSS/MG15000 security logs being sent to a higher level management system" (page 68) 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 69) lists security related logs that are generated on the desktop platform. These logs are not sent to the higher level management system.

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

Log type	Storage location	sent to IEMS	sent to CS2000 Core Manager	on facility
Operating system security logs				
PAM_IS logs	/var/log/authlog	yes	no	local1
PAM_NSSwitch	/var/log/authlog	yes	no	local1
PAM mkdir logs	/var/log/authlog	yes	no	local0
Login logs (UNIX, X11)	/var/log/authlog	yes	no	auth.*
General UNIX logs	/var/adm/messages	yes	no	*.*
SSH and IPSec logs	/var/adm/messages	yes	no	*.*
Apache logs	/opt/nortel/logs/3rd_party/apache	no	no	
MDM and MSS/MG15000 security audit logs				
MSS/MG15000 security audit logs (custlog V2 format)	/opt/MagellanNMS/data/security/security_custlog<_hlmsname>.nlog	yes	optional	local1
MDM security audit logs (custlog V2 format)	/opt/MagellanNMS/data/security/security_custlog<_hlmsname>.nlog	yes	optional	local1
MSS/MG15000 security audit logs (syslog format)	/opt/MagellanNMS/data/security/security_<-name>.nlog	optional	no	local3
MDM security audit logs (syslog format)	/opt/MagellanNMS/data/security/security_<-name>.nlog	optional	no	local3
Server Platform Foundation Software (SPFS) logs				

Log type	Storage location	sent to IEMS	sent to CS2000 Core Manager	on facility
platform alarm logs	/var/log/customerlog	yes via SNMPv2c	yes via custlog V2 on facility local1	

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

Note 4: <-name> is the matching -name value specified in the MDM salcserver startup command used.

Note 5: In MDM log storage location column and after the current date, the security audit logs raw MDM file will be compressed and time-stamped to /opt/MagellanNMS/data/security/security_custlog <hlms>_<yyyymmdd>.nlog.gz and it is year-month-date time format stamped. Similarly filename scheme for security audit raw log file in syslog format.

Note 6: Apply NP template security audit log records (SAL) and Node configuration audit SAL records are subset of MDM SAL.

For more information on the configuration required to send security audit logs to the 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/PT-IP/PT-AAL2*.

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

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

Restricted MDM Toolset access

The MDM Toolset uses a special set of menus to control access to tools according to user group authorization. The MDM Toolset application identifies the user group of the user who launches the Toolset application, and allows access to only those tools that the user group is authorized to use.

User groups for restricted MDM Toolset access

The following user groups are authorized to access the MDM Toolset tools:

- emsro (read only) level provides the ability to display surveillance information, but not to alter it.
- emsrw (read/write) level provides the ability to display surveillance information and configure MSS/MG15000 switches.
- emsmtc (maintenance) level provides the ability to configure MSS/MG15000 nodes.
- emssprov (subscriber provisioning) level is mapped to the system administration impact level for MSS/MG15000 nodes.
- emsadm (administration) level is mapped to the debug impact level for MSS/MG15000 nodes and provides access to all MDM resources except MDP.

See the table "User group mapping for restricted access to MDM Toolset tools in VoA networks" (page 206) for the tools that each user group is authorized to use.

> ***Note:*** When a MDM Toolset userid is added, it must be assigned to one of the five user groups. MDM Toolset userids that are deleted must be deleted from the user group.

This feature is required as part of the VoIP security activation sequence. For more information, see *NN10180-612 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*.

This feature is optional for VoA solutions.

Restricting access to MDM Toolset tools

To install the MDM Toolset restricted access menus, you must be logged in to the MDM workstation as root and have the Carrier VoIP SN09 Security Software CD inserted in the drive in the MDM workstation.

Procedure steps

Step	Action
1	Login to the MDM local console as root.

2	Backup the tsets directory before installing the new files:
	`cd /opt/MagellanNMS/cfg/tsets`
	`tar cvf /opt/MagellanNMS/cfg/tsets.orignal.tar /opt/MagellanNMS/cfg/tsets/.`

3	Install the customized MDM Toolset menu files from the Carrier VoIP SN09 Security Software CD:
	`cp <CVoIP cdrom>/tsets.C.tar /opt/MagellanNMS/cfg/tsets/tsets.C.tar`
	`cd /opt/MagellanNMS/cfg/tsets/`
	`tar xvf tsets.C.tar`

4	Use the Solaris Management Console to check that user groups emsadm, emsrw, emssprov, emsmtc, and emsro exist. Execute the following command to activate the Solaris Management Console: `smc &` For information on using the Solaris Management Console to list user groups, refer to the Solaris on-line help documentation.
5	If the user groups do not exist, create the following group names and numbers using the Sun administration tool or Solaris Management Console (SMC): 1021 emsadm 1022 emsrw 1023 emssprov 1024 emsmtc 1025 emsro
6	For MDM on SPFS with VoIP central users, execute: `/opt/MagellanNMS/bin/nmuser <userid>`

ATTENTION
DO NOT EXECUTE the command:
/opt/MagellanNMS/bin/nmsuser <MDM user> for the Root.

7 Launch the MDM Toolset application to activate the restricted access menus:

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

8 This procedure is complete.

—End—

Variable definitions

Variable	Definition
<CVoIP cdrom>	is the directory path of the Carrier VoIP SN09 Security Software CD.

Procedure roll-back

To restore the MDM Toolset to unrestricted user access, perform the following steps.

Step	Action

1 Restore the original tsets directory from the backup copy made prior to installation of the restricted access files:

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

```
tar xvf /opt/MagellanNMS/cfg/tsets.original.tar
```

2 Launch the MDM Toolset application to activate the unrestricted access menus:

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

3 This procedure is complete.

—End—

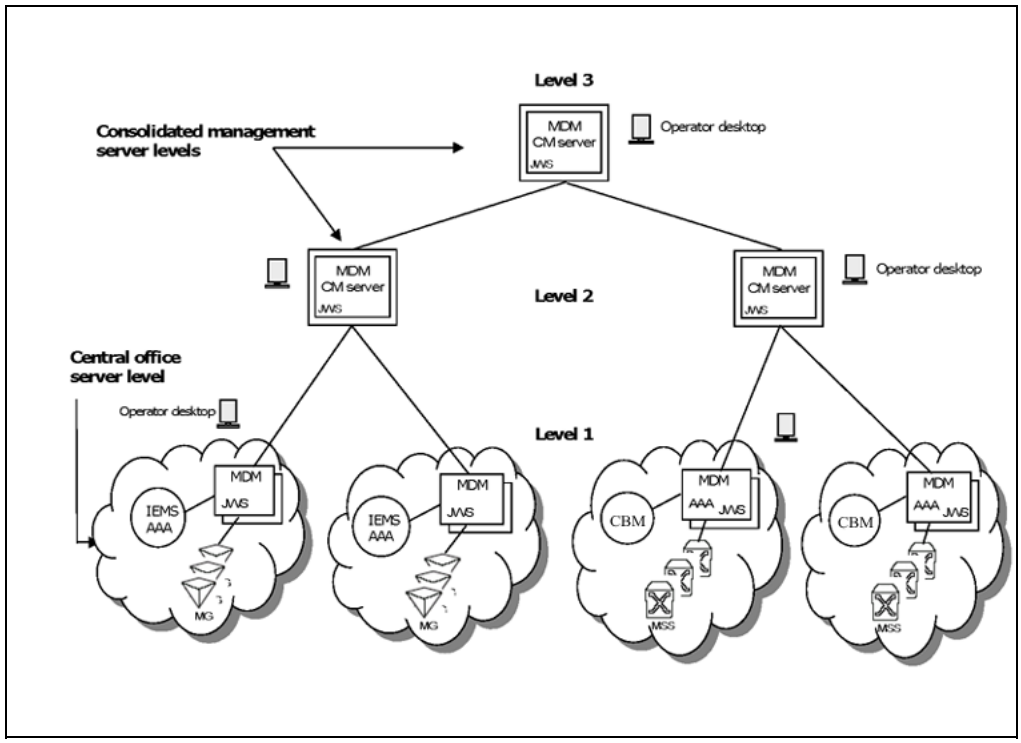
Consolidated network management

In the consolidated network management approach for deploying Nortel Multiservice Data Manager servers, a hierarchical topology of consolidated management (CM) servers is used to partition the network according to geographical, traffic flow or other network management needs.

The hierarchical topology can have as many levels as are required to partition the network into the required regional views. The lowest level of the topology consists of the MDM servers connected to the MSS/MG15000 switches. These lowers level MDM servers are located in the central office (dedicated deployment) or in the NOC (centralized deployment). The intermediate levels of the topology consist of CM servers that consolidate management information into regional views of the network. The CM server at the highest level of the topology provides the management view of the entire network.

The figure "Sample Multiservice Data Manager consolidated management server configuration" (page 76) shows a sample consolidated management topology. Level 1 MDM servers are central office servers that directly manage the MSS/MG15000 switches. Levels 2 and 3 represents MDM consolidated management servers. The number of levels in the hierarchical topology depends on the needs of the network. Consolidated management servers may be deployed singly, or in redundant pairs for greater reliability.

Sample Multiservice Data Manager consolidated management server configuration



CM servers are used for:

- monitoring the network partition (or the entire network if located at the highest level)
- performing required configuration management of MSS/MG15000 switches in the network partition

Operators using a regional CM server do not have visibility of other network partitions, nor can they make configuration changes to MSS/MG15000 switches in other network partitions. Operators using the highest level CM server can view network information and make configuration changes across the entire network.

Network monitoring from a CM server

Network monitoring of a network partition is performed from the appropriate level CM server. Each CM server has visibility of the network model covering any lower level CM servers, and the MDM servers and MSS/MG15000 switches at the lowest level of the topology. The CM server aggregates fault data from the MSS/MG15000 switches through the intermediate levels of CM servers. For more information, see "Managing the network model on a CM server" (page 79).

Configuration management from a CM server

To perform configuration management of an MSS/MG15000 switch in the network partition controlled by the CM server, the operator first logs in to his designated CM server. Using service selection, the operator accesses the MDM server managing the switch, and performs the necessary configuration operations. The System Wide Service Selection feature is used to define the MDM server in the office most commonly accessed by the operator. The User Specific Service Selection feature is used if the operator needs to access a different MDM server in another office. For more information, see "Managing Service Selection from a CM server" (page 78).

CAUTION

The Service Data Backup and Restore tool cannot be run from a consolidated management (CM) server.

The tool can only be run on the Multiservice Data Manager server used to manage the Multiservice Switch 15000 or Media Gateway 15000 switch.

User authentication and authorization on a CM server

Access to a CM server using the MDM Toolset environment requires local user authentication. The userids, passwords, and groups must be defined locally on the CM server.

Access to a CM server using the Operator Client application requires that the userids, passwords, and groups be defined on a central AAA server providing authentication and authorization for the network partition. The address of the CM server is used to launch the Operator Client application.

To perform configuration operations on an MSS/MG15000 switch, the operators userid, password and group must be defined on the central AAA server providing authentication for the switch.

For more information, see "Managing userids and passwords for CM server access" (page 78).

Security audit logs on a CM server

Security audit logs from lower levels are not aggregated by CM servers. Security audit logs collected by the MDM server managing the MSS/MG15000 switches continue to be directed to the higher-level management system. Security audit logs generated by the CM server are stored locally on the server. For more information, see "Managing logs on CM servers" (page 80).

Managing userids and passwords for CM server access

For MDM Toolset access, userids, passwords and groups must be defined locally on each CM server to which access is authorized. If a user account is changed or deleted, then the modification or deletion must be performed on each CM server on which the userid is defined.

> ***Note:*** Centralized authentication and authorization is not supported for MDM Toolset access to CM servers.

Operator Client userids, passwords and groups must be defined on a server providing central AAA services (MDM Admin Server for VoA, IEMS for VoIP) in the office. If the operator must access MDMs and MSS/MG15000 switches in different offices, then the userid, password and group must be defined on each central AAA server.

To make configuration changes to an MSS/MG15000 switch, the operator's userid, password and group must be defined on the central AAA server providing authentication services for the switch.

Changes to userids, passwords and groups that are maintained across multiple central AAA servers and CM servers must be coordinated carefully.

When deleting an IEMS central AAA userid, the user directories for the userid must be deleted from every workstation that was used to perform logins.

Managing Service Selection from a CM server

In order to perform configuration activities on MSS/MG15000 switches in an office, the operator must use the Service Selection feature to access the MDM server in the correct office.

The administrator uses the MDM Toolset to define the System Wide Service Selection feature for both MDM Toolset and Operator Client users. The server defined for System Wide Service Selection should be the MDM server in the office that is most commonly used by the operators.

The operator can use the User Specific Service Selection feature to select an alternate office. The operator must be aware of the network topology in order to correctly determine the MDM server to use for service selection.

> ***Note:*** User Specific service selection does not persist across tool sessions.

For more information on service selection, see *NN10400-300 Nortel Multiservice Data Manager Administration Tools*.

Note: Since IEMS launches only the MDMs located in the same central office, MDMs launched by IEMS cannot perform Service Selection to MDMs in other central offices or to CM servers located at higher levels in the hierarchical topology.

Managing the network model on a CM server

MDM servers and MSS/MG15000 switches in the network partition are propagated into the network model for the CM servers during installation and initial configuration of a CM server.

The network model is maintained from the CM server at the highest level in the network.

Adding an MDM server to a central office

Use the following task table to update the consolidated management network model when an MSS/MG15000 switch is added to a central office. These tasks are carried out on the highest level CM server.

Tasks for adding a new MSS/MG15000 node to the consolidated management network model

Step	Task	Reference section in *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*
1	Load the network model for the affected central office.	Loading the network model
2	Update the Configuration Data Files (CDF for the MSS/MG15000 switches in the affected central office (CO). Specify the new MSS/MG15000 in this CO.	Collecting network model data
3	Import the data collected in step 2 into the network model for the CO.	Managing collections and applying collected data to the network model
4	Save the model using portable format. Enter the name of the office in CLLI format as the model name.	Saving and distributing network model files
5	Repeat steps 1 through 4 for each CO affected by the MSS/MG15000 addition. Distribute the models to the appropriate MDM servers in the CO and the CM servers in the lower levels of the partition as appropriate.	
6	This procedure is complete.	

Removing an MDM server from a central office

Use the following task table to update the consolidated management network model when an MSS/MG15000 switch is removed from a central office. These tasks are carried out on the highest level CM server.

Tasks for adding a new MSS/MG15000 node to the consolidated management network model

Step	Task	Reference section in *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*
1	Load the network model for the affected central office.	Loading the network model
2	Specify the MSS/MG15000 switch that was removed from the central office (CO).	Deleting elements from the network model
3	Import the data collected in step 2 into the network model for the CO.	Managing collections and applying collected data to the network model
4	Save the model using portable format. Enter the name of the office in CLLI format as the model name.	Saving and distributing network model files
5	Repeat steps 1 through 4 for each CO affected by the MSS/MG15000 addition. Distribute the models to the appropriate MDM servers in the CO and the CM servers in the lower levels of the partition as appropriate.	

Managing logs on CM servers

For each MDM CM server, the OAMC server is connected to the GMDR server. The MDM servers in a central office do not have a GMDR - OAMC connection to MDM servers in other central offices, nor with upper level CM servers in the network partition. The flow of alarms and security audit logs is unidirectional from lower level MDM servers to higher level CM servers, allowing operators at higher level servers to see the alarms and logs from lower level servers but preventing operators at lower level servers from seeing the aggregated information available at higher level servers.

The OAMC server is connected to the SALC server on all MDM CM servers. This ensures that all security relevant actions by any operator in the network are logged. The SALC server also writes logs to file on CM servers at all levels in the topology.

Security audit log information collected on CM servers is not forwarded to the higher level management systems (CS2000 Core Manager for VoA solutions or IEMS for VoIP solutions). For more information on the configuration of the SALC server in a CM server configuration, see the

"No Northbound" column of the table in the section "Security Audit Log Collector (SALC) server configuration" in *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/PT-IP/PT-AAL2*.

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.

"Userids configured on the Sun Fire® V480 servers for VoA solutions" (page 83) lists all of the userids and passwords that were configured for a VoA solution during the Multiservice Data Manager software installation. "Userids configured on the Sun Fire® V480 servers for VoA solutions" (page 83) 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.

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

Userid	Purpose	Group	Multiservice Data Manager user
<>	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 as necessary.

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 IEMS central AAA server.

For more information, see the following sections:

- "Adding additional local users" (page 84)
- "Adding additional local groups" (page 85)

Adding additional local users

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

Procedure steps

Step	Action
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 IEMS 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 IEMS providing central authentication and authorization, the command will try to create the password for an IEMS 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>
```

6 This procedure is complete.

—End—

Variable definitions

Variable	Definition
<groupname>	is the group to which the new user belongs
<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.

Step	Action
1	Log in to the Multiservice Data Manager server as the *root* user.
2	Add a new group: `groupadd <groupname>`
3	This procedure is complete.

—End—

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

Step	Action
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 IEMS 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 IEMS providing central authentication and authorization, the command will try to change the password on an IEMS userid instead of the locally defined userid.

3	Follow the command prompts to enter the new password and old password for validation.
4	This procedure is complete.

—End—

Variable definitions

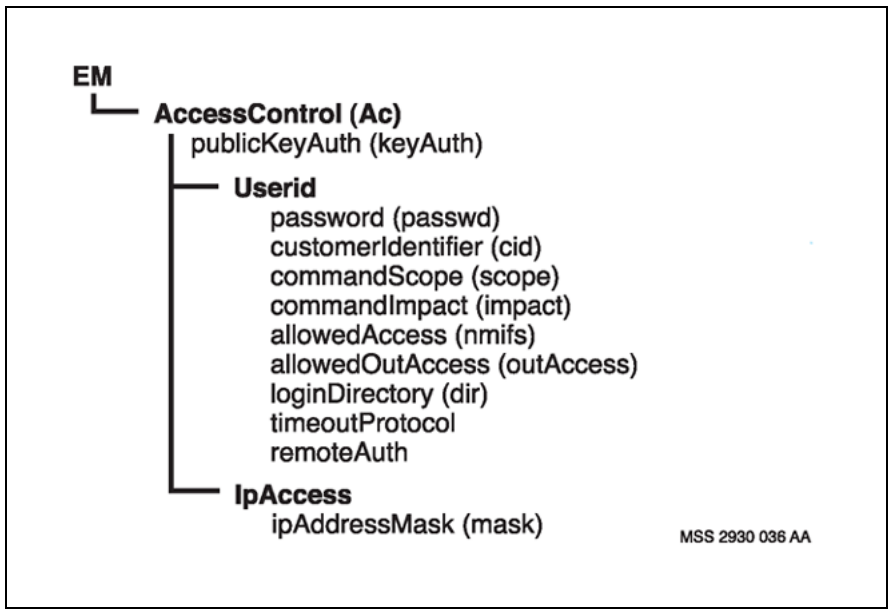
Variable	Definition
<userid>	is the user's ID. This userid must be unique.

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 89) summarizes the associated components and attributes.

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 Utilities*)

"Summary of user access tasks" (page 90) summarizes the OAM tasks required for node security and access.

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"
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 90). For specific procedures for performing user access administration on nodes, see the following:

- "Adding a user using the CLI" (page 92)
- "Copying an existing userid for a new user using the CLI" (page 95)
- "Adding an IPAccess component using the CLI" (page 96)
- "Setting a password using a secure method" (page 97)
- "Changing a user profile and password using the CLI" (page 100)
- "Deleting a user profile using the CLI" (page 101)

Command line interface basics

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

- "Logging into CLI" (page 91)
- "CLI operational mode" (page 91)
- "CLI provisioning mode" (page 92)

Logging into CLI

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

Procedure steps

Step	Action
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.
5	This procedure is complete.

—End—

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

Step	Action
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 100).

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.

11 This procedure is complete.

—End—

Variable definitions

Variable	Definition
<userid>	on first reference, 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
<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

Variable	Definition
	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. "Impact levels for Multiservice Switch 15000 nodes" (page 18) 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.

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 100).

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

Step	Action
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 100).
3	To change the attributes of the new *userID* component, use the set command.
4	This procedure is complete.

—End—

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

Step	Action
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.
5	This procedure is complete.

—End—

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

Step	Action
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
```

14 This procedure is complete.

—End—

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.
<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>

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 97) and "Risks" (page 100).

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

Step	Action
1	Change the attributes of the *userID* component: `set Ac userID/<userID> <attribute> <value>`
2	Set the password: `set Ac userID/<userID> password <password>`
3	This procedure is complete.

—End—

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

Step	Action
1	Remove the *userID* component: `delete accessControl userID/<userID>`
2	This procedure is complete.

—End—

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 activated, 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.

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" (page 103)
- "Configuring the Ethernet links in the network model" (page 106)
- "Copying the network model from one Multiservice Data Manager server to another" (page 107)

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

Step	Action
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*.
3	Create a new region called CVoIP within the CVoIP organization. See the section on manually creating components and subcomponents

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

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 ManagerMDM 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 and PT-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.

13 This procedure is complete.

—End—

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

Step	Action

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

Set the	To ...
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.

6 This procedure is complete.

—End—

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

Step	Action
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
```

15 This procedure is complete.

—End—

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

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/PT-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

Step	Action
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.
5	This procedure is complete.

—End—

For more information, refer to "Configuring data file retention" in *241-6001-309 Nortel Multiservice Data Manager Management Data Provider*.

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

Step	Action
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**.

12 This procedure is complete.

—End—

For more information on using the Server Administration tool, refer to *241-6001-303 Nortel Multiservice Data Manager 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

Step	Action
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
\Qfind .  -name "*.csv" -mtime +1 -print\Q)
```

5 Save and close the cron file.

6 This procedure is complete.

—End—

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

Step	Action
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 \Qfind .  -name "*.FIVE.CSV" -mtime +5 -print\Q)`
5	Save and close the cron file.

6 This procedure is complete.

—End—

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

Step	Action
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 \Qfind . -name "*.THIRTY.CSV" -mtime +10 -print')`
5	Save and close the cron file.
6	This procedure is complete.

—End—

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

Step	Action
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.
6	This procedure is complete.

—End—

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 115).

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

Step	Action
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.

5 This procedure is complete.

—End—

Managing Server Platform Foundation Software log files

SPFS log files are automatically rotated, so that file size or number of log files remains manageable. After rotation, the log files are compressed by the gzip compression program.

File rotation can also be manually triggered through the SPFS "cli" interface.

SPFS file rotation is managed through entries in the file /opt/rotatelog/conf/rotatelog.conf. "Summary of default SPFS log file rotation parameters" (page 118) shows the SPFS log files managed by file rotation and the default rotation parameters.

Note: To manage the file /var/log/authlog, see "Managing MDM syslog files" (page 117).

Summary of default SPFS log file rotation parameters

Path name	Trigger	Archive limit
/var/log/nmp_designlog	10 MB	9
/var/log/tomcat/catalina.out	250 KB	12
/var/log/filesys/fs.log	250 KB	12
/var/log/filesys/lv.log	250 KB	12
/var/log/sspfslog	250 KB	12
/var/log/securitylog	250 KB	12
/var/log/debuglog	250 KB	12
/var/log/customerlog	250 KB	12
/var/log/auditlog	250 KB	12
/var/log/marklog	250 KB	12

SPFS log file rotation administration procedures

Use the following procedure to view the file management entries in the SPFS log rotation configuration file, or to manually initiate the SPFS log file rotation utility.

Step	Action
1	Log in to the MDM server as root, using Telnet (for unsecured networks) or SSH (for secured networks). ***Note:*** SSH-related files for MDM with SPFS are located in the following directory: /opt/openssh/etc

2	Access the command line interface by typing the following command after the command line prompt and pressing the Enter key:
	
	`/opt/nortel/sspfs/Scripts/cli`
	
	Sample response:
	
	`Command Line Interface`
	`1 - View`
	`2 - Configuration`
	`3 - Other`
	
	`X - exit`
	
	`select -`

3	Enter the number next to the "Other" option in the menu.
	
	Sample response:
	
	`Other`
	
	`1 - Log Rotation`
	`2 - capt_files (Capture Various SSPFS Files/Logs For Debugging Purposes)`
	`3 - sun_explorer (Execute the Sun Explorer Data Gathering Tool)`
	`4 - mount_image (Mount A Generic Iso Image To the SSPFS Unit)`
	`5 - umount_image (Un-Mount A Generic Iso Image From the SSPFS Unit)`
	`6 - disp_sspfspatch (Display the patching status of the SSPFS unit)`
	`x - exit`
	`select -`

4	Enter the number next to the "Log Rotation" option in the menu.

Sample response:

```
Log Rotation
1 - exec_rlog (Execute The Rotatelog Function)
2 - view_rlog (View The Rotatelog Configuration
File)
x - exit
select -
```

5 Enter the number next to the "exec_rlog" option to execute the log rotation utility.

Enter the number next to the "view_rlog" option to display the contents of the log rotation configuration file /opt/rotatelog/conf/rotatelog.conf.

6 This procedure is complete.

—End—

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" (page 121)
- "Understanding impacts of Multiservice Data Manager workstation outages" (page 127)
- "Backing up and restoring Multiservice Data Manager workstation software" (page 129)
- "Synchronizing Multiservice Data Manager workstations" (page 133)

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 137).

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

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 IS and PAM NSSwitch interfaces for communicating with the central AAA service provided by the IEMS
- configuration information for sending syslogs to the IEMS
- 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

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), an MDM Admin Server configuration (VoA network only) or a consolidated management server configuration. 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

Operating system software

The UNIX core software consists of the Solaris operating system and third party software packages, and the associated 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.

Server Platform Foundation Software

Server Platform Foundation Software (SPFS) is installed on Sun Netra 240 platforms. SPFS installation installs the software for the Solaris operating system and third party software, and provides SPFS software and data for service applications such as the resource monitor (RESMON) and the Network Patch Manager (NPM). SPFS service application data is static and can be protected with a good backup procedure. The software can be restored from backup of from the supplied source files.

"Data mapping for Multiservice Data Manager workstation configurations" (page 125) shows the data relevant to each type of workstation configuration.Multiservice Data Manager

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

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					
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
Operating system software					
Solaris operating system and third party software packages	yes	yes	yes	yes	yes
Server Platform Foundation Software (installed on Sun Netra 240 platforms only)					
Solaris operating system and third party software packages	yes	yes	yes	yes	yes

Data types	standalone	server-set	client-set	MDM Admin Server (VoA only)	MDM Server (VoIP only)
SPFS service applications	yes	yes	yes	yes	yes
Note: Deployment of some SPFS service applications such as the Network Patch Manager is dependent on the MDM workstation configuration. 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/PT-IP/PT-AAL2* for more information.					

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 127) lists the impacts of workstation outages on Multiservice Data Manager data.

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.
• 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	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.
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.

Operating system software	For a simple outage, there is no impact to the Solaris operating system or third party software. For a complex outage, Solaris operating system software and third party software packages are lost and must be restored from backup or from Solaris source files.
SPFS service applications and data	For a simple outage, there is no impact to the Solaris operating system, third party software or SPFS service applications. For a complex outage, • Solaris operating system software, third party software packages, and SPFS service application software packages are lost and must be restored form backup or from SPFS source files. • SPFS service application 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.

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.

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.

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

Operating system 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.
- a consolidated management server is restored only from a consolidated management server backup

Backing up and restoring Server Platform Foundation Software service application data

Use the following procedures to back up and restore Server Platform Foundation Software (SPFS) service application data.

Backing up SPFS service application data

To back up SPFS service application data on Sun Netra 240 servers, including the data for configured service applications such as NPM, use the following procedure:

Step	Action
1	Create a file containing the SPFS service application data: `/opt/sspfs/bks/bkdata -f /backup/<SPFS_bk_filename>` This creates a file /backup/<SPFS_bk_filename> which contains the SPFS data.
2	Use the "tar" command to copy the contents of the /backup directory to a <SPFS backup>.tar file that can be stored on a secure remote system or put on removable media for storage in a secure, offline storage location.
3	This procedure is complete.

—End—

Perform this procedure prior to any system migration. As this data is stable, backing it up weekly or monthly is sufficient.

Restoring SPFS service application data

To restore SPFS service application data on Sun Netra 240 servers, including the data for configured service applications such as NPM, use the following procedure:

Step	Action
1	Retrieve the <SPFS backup>.tar file from the secure storage location, and use the "tar" command to restore the contents of the /backup directory.
2	Restore the SPFS service application data: `/opt/sspfs/bks/rsdata -f /backup/<SPFS_bk_filename>`
3	This procedure is complete.

—End—

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 *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration* for all of the procedures listed in the table.

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.

Task	Procedure	Notes
	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 131).

Synchronizing configuration files

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

Note 1: This procedure should only be performed for server-set, standalone, MDM Admin Server, or MDM Server workstations.

Note 2: Refer to "Impacts of workstation outages on Multiservice Data Manager data" (page 127) 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.

Step	Action
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 107) 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).
5	This procedure is complete.

—End—

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.

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 137)
- "Software backup" (page 140)
- "Restoring software" (page 143)

CAUTION
The Service Data Backup and Restore tool cannot be run from a consolidated management (CM) server.

The tool can only be run on the Multiservice Data Manager server used to manage the Multiservice Switch 15000 or Media Gateway 15000 switch.

Backup site creation

- "Configuring the backup site" (page 137)
- "Configuring automatic backups to the backup site" (page 139)

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

Step	Action
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.

11 This procedure is complete.

—End—

Variable definitions

Variable	Definition
-full	the -full attribute stipulates a full backup

Variable	Definition
-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

Step	Action
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.

6 This procedure is complete.

—End—

Variable definitions

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

Software backup

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

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

Step	Action
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.

11 This procedure is complete.

—End—

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

Step	Action

1 Display the committed view and the current view:

```
display prov committedFileName, currentViewFileName
```

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
```

committed file

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.

6 This procedure is complete.

—End—

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 135) for information on synchronizing IPSec security associations after restoring MSS/MG15000 switch software.

SPFS Administration

The Server Platform Foundation Software (SPFS) package consists of the base operating system and third-party application tools. Service applications provided in the main package are the Resource monitor (RESMON), Service application monitor (servman), and EMS proxy services. SPFS is installed only on the Sun Netra 240 platform.

The service application monitor (servman) is used to register, deregister and query the state of applications on the server where the SPFS resides. The MDM application does not register with the service application monitor (servman). Use MDM commands to start, stop and query the status of the MDM servers.

Sub-packages such as the Network Patch Manager, which contains the patch management application, are included as separate packages.

SPFS display utilities

The SPFS command line interface (cli) provides the following utilities:

SPFS administration utilities

Utility	Purpose
sspfs_soft	Display the software installation level of SPFS.
chk_sspfs	Display the SPFS processes.
sw_conf	Display the software configuration of the platform (pkginfo).
cpu_util	Display the overall CPU utilization.
cpu_util_proc	Display CPU utilization by process.
port_util	Display I/O port utilization.
disk_util	Display file system utilization.

To run an SPFS administration utility:

Step	Action

1 Log in to the MDM server as root, using Telnet (for unsecured networks) or SSH (for secured networks).

Note: SSH-related files for MDM with SPFS are located in the following directory: /opt/openssh/etc.

2 Access the command line interface by typing the following command after the command line prompt and pressing the Enter key:

`/opt/nortel/sspfs/Scripts/cli`

Sample response:

```
Command Line Interface
 1 - View
2 - Configuration
3 - Other

x - exit

select -
```

3 Enter the number next to the "View" option in the menu.

Sample response:

```
View
1 - sspfs_soft
2 - chk_sspfs
3 - sw_conf
4 - cpu_util
5 - cpu_util_proc
6 - port_util
7 - disk_util

x - exit

select -
```

4 Enter the number next to the utility you wish to use.

5 This procedure is complete.

—End—

SPFS security and administration procedures

This section contains a set of solution-level Server Platform Foundation Software procedures that are relevant to Security and Administration. Use the information in the following procedures in the context of Note 1 to Note 4:

Note 1: An N240 server with SPFS and MDM runs in a simplex configuration; it is not part of a high-availability cluster configuration. When dual MDM servers are deployed, they are functioning as two distinct one-server systems.

Note 2: In secured systems, SSH is used to log in to the server instead of telnet. SSH-related files for MDM with SPFS are located in the following directory: /opt/openssh/etc.

Note 3: As these procedures are used in different contexts in the Carrier Voice over IP suite of documentation, they may contain references to procedures that are not used by Nortel Multiservice Data Manager.

Note 4: Server Platform Foundation Software (SPFS) may alternately be referred to as Succession Server Platform Foundation Software (SSPFS).

- "Increasing the size of a file system on an SPFS-based server" (page 192)

Rebooting an SPFS-based server

Application

Use this procedure to reboot a Server Platform Foundation Software (SPFS)-based server, which may be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core and Billing Manager (CBM)
- Multiservice Data Manager (MDM)

MDM when installed on SPFS-based servers is not configured as a two-server cluster but as two distinct one-server configurations.

ATTENTION

The SPFS-based server may be hosting more than one of the preceding components, therefore, ensure it is acceptable to reboot the server.

Prerequisites

You must have root user privileges.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Telnet to the Sun server by typing `> telnet <IP address>` and pressing the Enter key. where **`IP address`** is the IP address of the SPFS-based server you want to reboot
2	When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Reboot the server by typing

```
# shutdown -i 6 -y
```

and pressing the Enter key.

6 You have completed this procedure.

—End—

Shutting down an SPFS-based server

Application

Use this procedure to shut down a Server Platform Foundation Software (SPFS)-based server, which may be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)
- Multiservice Data Manager (MDM)

MDM when installed on SPFS-based servers is not configured as a two-server cluster but as two distinct one-server configurations.

ATTENTION

The SPFS-based server may be hosting more than one of the preceding components, therefore, ensure it is acceptable to shut down the server.

Prerequisites

You must have root user privileges.

Perform this procedure from a console only.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions. Therefore, Step 3 and Step 9 are not required.
- You must obtain non-restricted shell access.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration, NN10358-611*
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration, NN10358-611*
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration, NN10358-611*

Action

Use one of the following procedures according to your office configuration:

- "One-server configuration" (page 152)
- "Two-server (cluster) configuration" (page 153)

One-server configuration

Step Action

At your workstation

1 Log in to the server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address is the IP address of the SPFS-based server you want to power down

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Shut down the server by typing

```
# init 0
```

and pressing the Enter key.

The server shuts down gracefully, and the telnet connection is closed.

6 If required, turn off the power to the server at the circuit breaker panel of the frame.

You have completed this procedure.

To bring the server back up, turn on the power to the server at the circuit breaker panel of the frame. The server recovers on its own once power is restored.

—End—

Two-server (cluster) configuration

Step	Action

At your workstation

1 Log in to the Inactive server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address is the physical IP address of the Inactive SPFS-based server in the cluster you want to power down (unit 0 or unit 1)

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

Ensure you are on the Inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

5 Shut down the Inactive server by typing

```
# init 0
```

and pressing the Enter key.

The server shuts down gracefully, and the telnet connection is closed.

6 If required, turn off the power to the Inactive server at the circuit breaker panel of the frame. You have completed a partial power down (one server).

If you want to perform a full power down (both servers), proceed to step 7, otherwise, you have completed this procedure.

ATTENTION
Only perform the remaining steps if you want to perform a full power down, which involves powering down both servers in the cluster.

7 Telnet to the Active server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address is the physical IP address of the Active SPFS-based server in the cluster you want to power down

8 When prompted, enter your user ID and password.

9 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

10 When prompted, enter the root password.

11 Shut down the Active server by typing

```
# init 0
```

and pressing the Enter key.

The server shuts down gracefully, and the telnet connection is closed.

12 If required, turn off the power to the servers at the circuit breaker panel of the frame. You have completed a full power down (two servers).

You have completed this procedure.

To bring the servers back up, turn on the power to the servers at the circuit breaker panel of the frame. The servers recover on their own once power is restored.

—End—

Preparing a DVD-RW for use

Application

Use this procedure to verify the DVD-RW is ready for use when using it for the first time, or when you want to erase the contents of a used DVD-RW to use it again.

Prerequisites for Core and Billing Manager 850

All users with non-restricted shell access are authorized to perform this procedure.

You require root-user access, or must be a user in a role group authorized to perform config-admin actions, if an error occurs when ejecting a DVD.

For more information about how to log in to the CBM as an authorized user, how to request non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration for GSM/UMTS, NN20000-321*
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration for GSM/UMTS, NN20000-321*
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration for GSM/UMTS, NN20000-321*

Action

Perform the following steps to complete this procedure.

Step	Action
	At the server
1	Insert the DVD into the drive. Only rewriteable media can be erased. Verify that the DVD you are attempting to erase is a DVD-RW before inserting it into the drive.
	At your workstation
2	Log in to the server by typing `> telnet <server>` and pressing the Enter key.

where

server is the IP address or hostname of the SPFS-based server

3 When prompted, enter your user ID and password.

4 Use the following table to determine your next step.

If the DVD is	Do
new	step 5
used	step 6

5 Verify the DVD is ready for use by typing

```
$ cdrw -l
```

and pressing the Enter key

If the system response	Do
provides the CD device	step 11
indicates "No CD writers found or no media in the drive"	step 6

6 Erase the contents of the DVD by typing

```
$ cdrw -b all
```

and pressing the Enter key

ATTENTION

Erasing a DVD-RW can take over two hours. You can also use the "fast" and "session" arguments. For more details, refer to the man pages by typing **man cdrw**

7 Reinsert the DVD into the drive.

8 Verify the DVD is ready for use by typing

```
$ cdrw -l
```

and pressing the Enter key

If the system response	Do
provides the CD device	step 11
indicates "No CD writers found or no media in the drive" or "Media in the device is not erasable"	step 9

9 Eject the DVD from the drive as follows:

a. Ensure you are at the root directory level by typing

```
$ cd /
```

and pressing the Enter key.

b. Eject the DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, re-try the "eject cdrom" command.

c. Remove the DVD from the drive.

10 Obtain another DVD and repeat the process starting with step 4.

11 Proceed to use the DVD.

You have completed this procedure.

—End—

Viewing patching information for the SPFS

Application

Use this procedure to display the patching status for the Server Platform Foundation Software (SPFS) on the server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing **`> telnet <server>`** and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server
2	When prompted, enter your user ID and password.
3	Change to the root user by typing **`$ su - root`** and pressing the Enter key.
4	When prompted, enter the root password.

5	Access the command line interface by typing
	`# cli`
	and pressing the Enter key.
	Example response
	`Command Line Interface`
	`1 - View`
	`2 - Configuration`
	`3 - Other`
	`X - exit`
	`select -`

6	Enter the number next to the "Other" option in the menu.

Example response

```
Other
1 - Log Rotation
2 - capt_files (Capture Various SPFS Files/Logs For
Debugging Purposes
3 - sun_explorer (Execute the Sun Explorer Data
Gathering Tool)
4 - mount_image (Mount A Generic Iso Image To The SPFS
Unit)
5 - umount_image (Un-Mount A Generic Iso Image From the
SPFS Unit)
6 - disp_SPFSpatch (Display the patching status of the
SPFS unit)
X - exit
select -
```

7 Enter the number next to the ‘disp_SPFSpatch’ option in the menu.

Example response:

```
===Executing "disp_SPFSpatch"
SPFS Patch    Installed   Applied
==================================
SPFS07MA      Yes         Yes
SPFS07MB      Yes         Yes
==="disp_SPFSpatch" completed successfully
```

If no SPFS patches are installed, the response will display "No SPFS Patches Installed on This Unit".

8 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Setting up local user accounts on an SPFS-Based Server

Application

Use this procedure to add local user accounts on a Server Platform Foundation Software (SPFS)-based server and assign them to user groups. Also use this procedure to assign existing user accounts to user groups. For information on user groups, see "Additional information" (page 163).

If you choose to centrally manage your user accounts, refer to procedure "Adding new users" in *IEMS Security and Administration* (NN10336-611).

If you want to launch the ping and traceroute operations that are performed remotely on SPFS-based platforms from a centralized GUI on Integrated Element Management System (IEMS), refer to procedures "Running a ping test on the GWC network element or SPFS platform" and "Running a traceroute test on the GWC network element or SPFS platform" in *IEMS Basics* (NN10329-111).

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

Prerequisites

To perform this procedure, you need to have the root user ID and password to log in to the server.

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where

server is the IP address or host name of the SSFPS-based server

In a two-server configuration, log in to the active server using its physical IP address.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If you are	Do
adding a new user	step 6
assigning an existing user to secondary user groups	step 11

6 Add the user to the primary user group *succssn* by typing

```
useradd -d /export/home/<userid> -g succssn -G
<any additional groups> -m <userid>
```

and press the Enter key.

where

userid is a variable for the user name

7 Create a password for the user you just added by typing

```
# passwd -r files <userid>
```

and press the Enter key.

where

userid is the user name you added in the previous step

8 When prompted, enter a password of at least three characters.

It is not recommended to set a password with an empty value. Use a minimum of three characters.

9 When prompted, enter the password again for verification.

10 Proceed to step 13.

11 Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.

where

userid is a variable for the user name

12 Note the user groups the user currently belongs to.

13 Assign the user to one or more secondary user groups by typing

```
# usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

groupA, groupB,... are the secondary user groups (see table "Secondary user groups" (page 163)) and any other user groups you noted in step 12 to which the user already belonged Include a comma between groups, but no space.
userid is a variable for the user name

Example input for a user who can perform line and trunk maintenance operations

```
# usermod -g succssn -G lnmtc,trkmtc johndoe
```

The usermod command overwrites any previous user groups. Therefore, anytime you enter this command, specify all the user groups for the user.

You have completed this procedure.

—End—

Additional information

Users of the Nortel OAM&P client applications must belong to the primary user group succssn for login access. Users must also belong to one or more secondary user groups listed in the following table, which specify the operations a user is authorized to perform.

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm	secadm
trkrw	lnrw	mgcrw	mgrw	emsrw	secrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov	secmtc
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc	secro
trkro	lnro	mgcro	mgro	emsro	

A secondary user group consists of

- a user group domain
- a user group operation

User group domain

A user group domain defines the range of applications to which a user group applies. The user group domains are listed in the following table:

Domain	Application mapping
trk	trunks, trunk-based services, small trunking gateways (port level), carrier-based services
ln	line services, line cards, small line gateways (port level)
mgc	CS2K, CS3K, USP, GWC, SAM21, IMS, 3PC, Storm, CS 2000 SAM21 Manager, CS 2000 GWC Manager
mg	small and large gateways such as UAS, line gateways, trunk gateways
ems	SDM, MDM, MDP, KDC, device manager, NPM

User group operation

A user group operation dictates the operations a user can perform using the Nortel OAM&P client applications. The user group operations are listed in the following table:

Operation	User role mapping
adm (administration)	Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, sprov, mtc, and ro user operations.
rw (read/write)	Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do sprov, mtc, and ro user operations.
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do sprov and ro user operations.
sprov (subscriber provisioning)	Can view status and configuration and change provisioning data, but cannot change maintenance state or do base component configuration. The sprov user can also do ro user operations.
ro (read-only)	Can view status and configuration, but cannot make changes.

When assigning users to secondary user groups, use the tables that follow, which provide a mapping between commands and secondary user groups. The list of the available tables is as follow:

The mappings of commands to secondary user groups in the tables in this section do not apply to Multiservice Data Manager (MDM) when installed on a SPFS-based server.

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Disassociate a media gateway (MG) from a gateway controller (GWC)		x			
Associate an MG with a GWC		x			
Change the provisioning data for an MG		x			
Query site info					x

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Query a GWC					x
Query an MG					x
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			
Perform a swact			x		
Firmware flash			x		
Assign/unassign services		x			

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Configure audit	x				
Run audit	x				
Get audit description					x
Get audit configuration					x
Get list of registered audits					x

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Retrieve audit report					x
Take action on problem	x				

Carrier provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Add carrier		x			
Delete carrier		x			
Get endpoint					x
Get carrier					x
Get carrier by filter					x

Alarm operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
View/filter alarms					x

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro

Add, delete, change SPC	x				
Query SPCs					x
Set network VCAC	x				
Add, delete, change a network zone	x				
Query one or all network zones					x
addMPGroup	x	x			
changeMPGroup	x	x			
queryMPGroup	x	x	x	x	x
deleteMPGroup	x	x			
addVPN	x	x			
deleteVPN	x	x			
queryVPN	x	x	x	x	x

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Get tuple					x
Get tuple range					x
Add tuple		x			
Replace tuple		x			
Delete tuple		x			

Trunk maintenance operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro

Post by trunk CLLI					x
Maintenance by trunk CLLI			x		
Post by gateway					x
Maintenance by gateway			x		
Post by carrier					x
Maintenance by carrier			x		
D-channel Post by trunk CLLI					x
D-channel maintenance by trunk CLLI			x		
ICOT			x		
Set Auto Refresh					x

ADSL provisioning operations

Command	User group				
	lnadm	**lnrw**	**lnmtc**	**lnsprov**	**lnro**
Get subscriber					x
Add subscriber				x	
Add cross connection				x	
Modify subscriber				x	
Modify cross connection				x	

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Delete subscriber				x	
Delete cross connection				x	

Line provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
ECHO, QX75, QBB, QBERT, QCM, QCOUNTS, QCPUGNO, QDCH, QDN, QDNA, QGRP, QHLR, QIT, QLEN, QLRN, QLT, QMODEL, QMSB, QPHF, QPRIO, QSCONN, QSCUGNO, QSIMR, QSL, QTOPSPOS, QTP, QWUCR					x
QCUST, QDNSU, QDNWRK, QHA, QHASU, QHU, QLENWRK, QLOAD, QMADN, QNCOS, QPDN	x				
All other supported commands for line provisioning				x	

Line maintenance operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Validate line using DN CLLI					x
Validate line using TID CLLI					x
Get line post info					x
Busy line			x		
Return line to service			x		
Force release line			x		
Installation busy line			x		
Cancel deload			x		
Get CM CLLI					x
Get endpoint state					x
GetGwlp					x
run all TL1 line test commands			x		

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, delete, modify V5.2 interface		x					x			

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
View all V5.2 interfaces					x					x
View signalling channel information entry, update list (V5 Prov)					x					x
Add, modify, delete signalling channel information entry (V5Prov)		x					x			
View ringing cadence mapping, update list (V5 Ring)					x					x
Add, modify, delete ringing cadence mapping (V5 Ring)		x					x			

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
View signalling characteristic profile, update list (V5 Sig)					x					x
Add, delete, modify signalling characteristic profile (V5Sig)		x					x			
View carrier-to-interface and interface-to-carrier mappings					x					x

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro

apply, remove, activate, deactivate, auditd, restart, and smartimage from the NPM GUI or CLUI	x				
Software image from MG 9000 Manager GUI		x			

Automated upgrade operations

Command	User group									
	emsadm	emsrw	emsmtc	emsprov	emkro	mgcadm	mgcrw	mgcmtc	mgcprov	mgcro
Access and run the GWC upgrade CLUI			x					x		
Access and run the SC upgrade CLUI			x					x		

Ping and traceroute operations

Command	User group		
	emsadm	emsrw	emsmtc

Launch remote ping	x	x	x
Launch remote traceroute	x	x	x
These operations are for remote operations performed on SPFS platforms but launched from a centralized GUI on IEMS.			

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Disassociate a media gateway (MG) from a gateway controller (GWC)		x			
Associate an MG with a GWC		x			
Change the provisioning data for an MG		x			
Query site info					x
Query a GWC					x
Query an MG					x

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			
Perform a swact (refer to the notes that follow this table)			x		
Firmware flash			x		
Assign/unassign services		x			

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro

Configure audit	x				
Run audit	x				
Get audit description					x
Get audit configuration					x
Get list of registered audits					x
Retrieve audit report					x
Take action on problem	x				

Carrier provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Add carrier		x			
Delete carrier		x			
Get endpoint					x
Get carrier					x
Get carrier by filter					x

Alarm operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro

View/filter alarms					x

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, delete, change SPC	x				
Query SPCs					x
Set network VCAC	x				
Add, delete, change a network zone	x				
Query one or all network zones					x

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Get tuple					x
Get tuple range					x
Add tuple		x			

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Replace tuple		x			
Delete tuple		x			

Trunk maintenance operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Post by trunk CLLI					x
Maintenance by trunk CLLI			x		
Post by gateway					x
Maintenance by gateway			x		
Post by carrier					x
Maintenance by carrier			x		
D-channel Post by trunk CLLI					x
D-channel maintenance by trunk CLLI			x		
ICOT			x		
Set Auto Refresh					x

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emsspro v	emsro

apply, remove, activate, deactivate, auditd, restart, and smartimage from the NPM GUI or CLUI	x				
Software image from MG 15000 Manager GUI		x			

Automated upgrade operations

Command	User group									
	emsadm	**emsrw**	**emsmtc**	**emssprov**	**emkro**	**mgcadm**	**mgcrw**	**mgcmtc**	**mgcsprov**	**mgcro**
Access and run the GWC upgrade CLUI			x					x		
Access and run the SC upgrade CLUI			x					x		

Deleting local user accounts from an SPFS-based server

Application

Use this procedure to delete local user accounts from a Server Platform Foundation Software (SPFS)-based server.

If you are centrally managing your user accounts, refer to procedure "Deleting users" in the *IEMS Security and Administration* document, (NN10336-611).

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step	Action

At your workstation

1 Log in to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server

In a two-server configuration, log in to the active server using its physical IP address.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

ATTENTION

Do not delete the following critical user IDs from the server:

root, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, oracle, nortel

5 Delete the user from the server by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid is a variable for the user name

You have completed this procedure.

—End—

Changing a user password on an SPFS-based server

Application

Use this procedure to change a user password on a Server Platform Foundation Software (SPFS)-based server.

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step	Action

At your workstation

1 Log in to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server

In a two-server configuration, log in to the active server using its physical IP address.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

4 When prompted, enter the root password.

5 Change the password for a specific user by typing

```
# passwd -r files <userid>
```

and pressing the Enter key.

where

userid is a variable for the user's login identification

6 When prompted, enter a password of at least three characters.

It is not recommended to set a password with an empty value. Use a minimum of three characters.

7 When prompted, enter the password again for verification.

You have completed this procedure.

—End—

Changing an expired root password on an SPFS-based server

Application

Use this procedure to change the root password on a Server Platform Foundation Software (SPFS)-based server in the event that it has expired.

Perform this procedure when your root password failed with `su: Sorry`.

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

Prerequisites

Before you perform this procedure, ensure you entered the root password without the Caps Lock key on. Also ensure the password was not changed.

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step	Action
	At the server console
1	Log in to the Active server through the console (port A) using the root user ID and the expired root password.
2	When prompted, enter the old (expired) password.
3	When prompted, enter a password of at least three characters. It is not recommended to set a password with an empty value. Use a minimum of three characters.
4	When prompted, enter the password again for verification. You have completed this procedure.

—End—

Setting secure FTP proxy

Application

In order to have a secure (encrypted) channel of FTP communication between the OSS/FTP clients and network elements, you need to set up SSH port forwarding. Use one of the following procedures to set secure FTP proxy using SSH port forwarding:

- "Setting up SSH port forwarding on UnixSetting secure FTP proxy" (page 189)
- "Setting up SSH port forwarding on Windows" (page 190)

Once set up, SSH port forwarding establishes a port forwarding session from client to server, wherein all data forwarded are encrypted and hence secure.

Prerequisites

You need to have SSH software.

Action

Perform the following steps to complete this procedure.

Setting up SSH port forwarding on Unix

Step	Action
	At your workstation
1	Install the SSH software.
2	Establish a port-forwarding session between your workstation and the SPFS-based server by typing **`# ssh -L 9999:<remote-host>:9999 <remote-host>`** and pressing the Enter key. The first time you run the above command on your workstation in an attempt to forward data to remote-host, you will receive the following message and prompt: `The authenticity of host "remote-Host (1.2.3.4)" can't be established. RSA key fingerprint is <finger print information>. Are you sure you want to continue connecting (yes/no)?` SSH is verifying whether the host "remote-host" is a trusted host and whether you want to continue connecting to it.
3	When prompted, confirm you want to continue connecting by typing

```
# yes
```

and pressing the Enter key.

4 When prompted, enter your password.

Once your password is verified, a port-forwarding session is established. From this point on, all new sessions connecting to 'localhost:local-port' will be forwarded to 'remote-host:remote-port' in a secure channel.

Example
You set up SSH port forwarding on machine A with the following command:

```
# ssh-L 9999:SSPFS-based host:9999 SSPFS-based host
```

To securely transmit data from machine A to the SPFS-based server, you need to open a window logged into machine A, and type the following command:

```
# telnet localhost 9999
```

The telnet connection automatically gets secured between machine A and the SPFS-based server.
You have completed this procedure.

—End—

Setting up SSH port forwarding on Windows

Step	Action

At your workstation

1 Install PuTTY software.

2 Launch PuTTY to display the PuTTY Configuration window.

3 Configure SSH port forwarding as follows:

a. Click Session and complete the following fields:

- In the Host Name (or IP address) field, enter the host name or IP address of the SPFS-based server.
- In the Port field, enter 22.
- Under Protocol: select SSH.

b. Click Tunnels and complete the following fields:

- In the Source port field, enter any local port value, for example 9999.

- In the Destination field, enter <host:port>, where host is the host name of the SPFS-based server, and port is the port number on which the SPFS-based server listens for input (9999 is the standard port on which the SPFS-based server listens for a client connection)
- Select Local, and click Add.
- Click Open.

The first time you attempt to open a session, a PuTTY Security Alert window pops up to verify whether the host you want to connect to is a trusted host and whether you want to continue connecting to it.

4 Confirm you want to connect by clicking Yes in the PuTTY Security Alert window.

5 When prompted, enter your user ID and password.

This port-forwarding session is established.

You can now establish a secure connection between your workstation (client machine) and the SPFS-based server as long as the port-forwarding session you just created exists.

6 Establish a secure connection as follows:

a. Click the computer icon in the top left-hand corner of the window.

b. Select New Session... from the pull-down menu.

The PuTTY Configuration window opens.

c. Click Session and complete the following fields:

- In the Host Name (or IP address) field, enter *localhost*.
- In the Port field, enter 9999.
- Under Protocol:, select Telnet.

A secure session with the SPFS-based server is established.

You have completed this procedure.

—End—

Increasing the size of a file system on an SPFS-based server

Application

Use one of the following procedures to increase the size of a file system on a Server Platform Foundation Software (SPFS)-based server:

- "Simplex configuration (one server)" (page 193)
- "High-availability configuration (two servers)" (page 196)

It is recommended you perform this procedure during off-peak hours.

The SPFS creates file systems to best fit the needs of applications. However, it may be necessary to increase the size of a file system.

Not all file systems can be increased. The following table lists the file systems that cannot be increased, and lists examples of those that can be increased.

Not all the file systems that can be increased are listed.

SPFS file systems

Cannot be increased	Can be increased (examples)
/ (root)	/data
/var	/opt/nortel
/opt	/data/oradata
/tmp	/audio_files
	/PROV_data
	/user_audio_files
	/data/qca
	/data/mg9kem/logs

While file systems are being increased, writes to the file system are blocked, and the system activity increases. The greater the size increase of a file system, the greater the impact on performance.

Prerequisites

It is recommended that you back up your file systems and oracle data (if applicable) prior to performing this procedure. Refer to procedures Performing a backup of oracle data on an SPFS-based server and Performing a backup of file systems on an SPFS-based server if required.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

Step	Action

At your workstation

1 Log in to the server by typing

> > telnet < server>

and pressing the Enter key.

where

server is the IP address or host name of the server

2 When prompted, enter your user ID and password. You may log on as root or emsadm.

3 Determine the amount of disk utilization by the file systems as follows:

a. Access the command line interface by typing

 # cli

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
  2 - Configuration
  3 - Other
X - exit
select -
```

b. Enter the number next to the ‘View’ option in the menu.

Example response

```
View
  1 - SPFS_soft (Display Software
      Installation Level Of SPFS)
  2 - chk_SPFS (Check SPFS Processes)
  3 - sw_conf (The software configuration of
      the znc0s0jx)
  4 - cpu_util (Overall CPU utilization)
  5 - cpu_util_proc (CPU utilization by
      process)
  6 - port_util (I/O port utilization)
  7 - disk_util (Filesystem utilization)
  X - exit
select -
```

c. Enter the number next to the ‘disk_uti’" option in the menu.

Example response

```
Filesystem             size   used  avail capacity  Mounted on
/dev/md/dsk/d2         3.9G   1.6G   2.3G    42%    /
/proc                    0K     0K     0K     0%    /proc
mnttab                   0K     0K     0K     0%    /etc/mnttab
fd                       0K     0K     0K     0%    /dev/fd
/dev/md/dsk/d8         2.0G    86M   1.8G     5%    /var
swap                   2.5G   160K   2.5G     1%    /var/run
swap                   512M   3.8M   508M     1%    /tmp
/dev/md/dsk/d11        4.9G   1.5G   3.4G    32%    /opt
/dev/md/dsk/d21        2.9G   111M   2.8G     4%    /opt/nortel
/dev/md/dsk/d22        5.9G   145M   5.7G     3%    /var/mysql/data
/backup                3.9G   4.0M   3.9G     1%    /backup
/data                  2.9G   5.9M   2.9G     1%    /data
/data/oradata          9.8G   2.5G   7.3G    26%    /data/oradata
/data/oradata/arch     968M    12M   893M     2%    /data/oradata/arch
/data/qca              9.8G    10M   9.7G     1%    /data/qca
```

The ‘capacity’ column indicates the percentage of disk utilization by the file system, which is specified in the ‘Mounted on’ column.

4 Note the file system you want to increase, as well as its current size (under column ’size’).

5 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

ATTENTION

Before you proceed with this procedure, ensure the file system you want to increase is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that are taking up disk space.

6 Determine the size by which to increase the file system, by subtracting the desired size for the file system based on your specific needs, from its current size (noted in 6).

For example, to determine the size by which to increase the “data/oradata” file system, subtract its current size, 10337 MB from the desired size, for example, 15000 MB. You would increase the size of the “data/oradata” file system by 4662786 KB, or 4663 MB.

7 Determine the amount of free disk space that can be allocated to file systems as follows:

a. Determine the amount of free disk space on your system by typing

```
# /opt/nortel/sspfs/fs/meta.pl free_space
```

and pressing the Enter key.

Divide the resulting number by 2048 to determine the amount of free disk space in megabytes (MB) that can be allocated to existing file systems

If the value is	Do
less than zero (0)	contact Nortel for assistance
more than zero (0)	step b

b. Use the following table to determine your next step.

If	Do
the value you determined in step 8 (size by which to increase the file system) is greater than the value you obtained in step 9a (amount of free disk space you can allocate to file systems)	contact Nortel for assistance
the value you determined in step 8 (size by which to increase the file system) is less than the value you obtained in step 9 a (amount of free disk space you can allocate to file systems)	step 10

ATTENTION

Once you increase the size of a file system, you cannot decrease it. Therefore, it is strongly recommended that you grow a file system in small increments.

8 Increase the size of the file system by typing

```
#  filesys grow -m <mount_point> -s <size>m
```

where

`mount_point` is the name of the file system you want to increase (noted in step 6)
`size` is the size in megabytes (m) by which you want to increase the file system (determined in step 8)

Example

```
# filesys grow -m /data -s 512m
```

The preceding example increases the '/data' file system by 512 megabytes (MB).

You have completed this procedure.

—End—

ATTENTION

During this procedure, the cluster will be running without a standby node. The duration is estimated at approximately one hour.

High-availability configuration (two servers)

Step Action

At your workstation

1 For all users except those using Core and Billing Manager (CBM), start a login session using telnet. For CBM, start a login session connecting to the inactive node using ssh.

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 6

2 Log in to the Inactive node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the physical IP address of the Inactive node in the cluster

If you use the cluster IP address, you will log in to the Active node. Therefore, ensure you use the physical IP address of the Inactive node to log in.

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

Ensure you are on the Inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

6 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the physical IP address of the inactive server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

b. When prompted, enter the root password.

At the Inactive node

7 Verify the cluster indicator to ensure you are logged in to the Inactive node, by typing

```
# ubmstat
```

and pressing the Enter key.

If the system response is	Do
ClusterIndicatorSTBY	step 8
ClusterIndicatorACT	step 2

8 Verify the status of file systems on this server by typing

```
# udstat
```

and pressing the Enter key.

If the file systems are	Do
STANDBY normal UP clean	step 9
not STANDBY normal UP clean	contact your next level of support

9 Determine the amount of disk utilization by the file systems as follows:

a. Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
  2 - Configuration
  3 - Other
X - exit
select -
```

b. Enter the number next to the ‘View’ option in the menu.

Example response

```
View
  1 - SPFS_soft (Display Software
      Installation Level Of SPFS)
  2 - chk_SPFS (Check SPFS Processes)
  3 - sw_conf (The software configuration of
      the znc0s0jx)
  4 - cpu_util (Overall CPU utilization)
  5 - cpu_util_proc (CPU utilization by
      process)
  6 - port_util (I/O port utilization)
  7 - disk_util (Filesystem utilization)
  X - exit
select -
```

c. Enter the number next to the ‘disk_util’ option in the menu.

Example response

```
Filesystem            size   used  avail capacity  Mounted on
/dev/md/dsk/d2        3.9G   1.6G   2.3G    42%    /
/proc                   0K     0K     0K     0%    /proc
mnttab                  0K     0K     0K     0%    /etc/mnttab
fd                      0K     0K     0K     0%    /dev/fd
/dev/md/dsk/d8        2.0G    86M   1.8G     5%    /var
swap                  2.5G   160K   2.5G     1%    /var/run
swap                  512M   3.8M   508M     1%    /tmp
/dev/md/dsk/d11       4.9G   1.5G   3.4G    32%    /opt
/dev/md/dsk/d21       2.9G   111M   2.8G     4%    /opt/nortel
/dev/md/dsk/d22       5.9G   145M   5.7G     3%    /var/mysql/data
/backup               3.9G   4.0M   3.9G     1%    /backup
/data                 2.9G   5.9M   2.9G     1%    /data
/data/oradata         9.8G   2.5G   7.3G    26%    /data/oradata
/data/oradata/arch    963M    12M   893M     2%    /data/oradata/arch
/data/qca             9.8G    10M   9.7G     1%    /data/qca
```

The *capacity* column indicates the percentage of disk utilization by the file system, which is specified in the *Mounted on* column.

10 Note the file system you want to increase, as well as its current size (under column 'size').

11 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

ATTENTION

Before you proceed with this procedure, ensure the file system you want to increase is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that are taking up disk space.

12 Determine the size by which to increase the file system, by subtracting the desired size for the file system based on your specific needs, from its current size (noted in 10).

For example, to determine the size by which to increase the 'qca' file system, subtract its current size, 123 MB from the desired size, for example, 256 MB. You would increase the size of the 'qca' file system by 133153 KB, or 133 MB.

13 Determine the amount of free disk space that can be allocated to file systems as follows:

a. Determine the amount of free disk space on your system by typing

```
# /opt/nortel/sspfs/fs/meta.pl fs

# /opt/nortel/sspfs/fs/meta.pl free_space
/ 5000 - p | dc
```

and pressing the Enter key.

Divide the resulting number by 2048 to determine the amount of free disk space in megabytes (MB) that can be allocated to existing file systems.

If the value is	Do
less than zero (0)	contact Nortel for assistance
more than zero (0)	step b

b. Use the following table to determine your next step.

If	Do
the value you determined in step 12 (size by which to increase the file system) is greater than the value you obtained in step 13 a (amount of free disk space you can allocate to file systems)	contact Nortel for assistance
the value you determined in step 12 (size by which to increase the file system) is less than the value you obtained in step 13 a (amount of free disk space you can allocate to file systems)	step 14

ATTENTION

Once you increase the size of a file system, you cannot decrease it. Therefore, it is strongly recommended that you grow a file system in small increments.

14 Increase the size of the desired file system by typing

```
#  GrowClusteredFileSystem.ksh <mount_point>
<size>m
```

where

mount_point is the name of the file system you want to increase (noted in step 10)

size is the size in megabytes (m) by which you want to increase the file system (determined in step 12)

Example

```
# GrowClusteredFileSystem.ksh /data/qca 10m
```

The preceding example increases the '/data/qca' file system by 10 megabytes (MB).

15 Verify the status of file systems on the Inactive node by typing

```
# udstat
```

and pressing the Enter key.

If the file systems are	Do
STANBY normal UP clean	step 16
otherwise	repeat step 15 until the file systems are "STANDBY normal UP clean".

16 Reboot the Inactive node by typing

```
# init 6
```

and pressing the Enter key.

Wait for the unit to recover before proceeding.

17 Perform a swact on the active unit by typing

```
# swact
```

and pressing the Enter key.

This action causes a cluster failover and makes the active node inactive, and the inactive node active.

18 Log in to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the physical IP address of the active node in the cluster.

19 When prompted, enter your user ID and password.

20 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

21 When prompted, enter the root password.

Ensure you are on the Active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicator*ACT, which indicates you are on the Active server.

22 Verify all applications are running on the active node by typing

```
# servquery -status all
```

and pressing the Enter key.

Verify all applications are running.

23 Verify all replicated file systems are "active up normal" by typing

```
# udstat
```

and press the Enter key.

Ensure all file systems are in the "active up normal" state.

24 Clone the other node using procedure "Cloning the image of one server in a cluster to the other server", ensuring you log into the active node.

You have completed this procedure.

—End—

Appendix A Summary of MDM Toolset and Operator Client application tools

MDM Toolset and Operator Client application tools

Access to Nortel Multiservice Data Manager (MDM) tools requires appropriate user authentication and authorization for both the MDM Toolset environment and the Operator Client environment. Additionally, access to MDM servers used for configuration can be password protected. These server passwords can be further protected by using password encryption. For more information on password encryption for MDM servers, see *241-6001-310 Nortel Multiservice Data Manager Server Reference*.

Access to tools using the MDM Toolset environment

On initial installation of Multiservice Data Manager software, a user who has authorization to launch the MDM Toolset has authorization to access all of its tools. User access to the various tools can optionally be controlled by installing a set of MDM Toolset menus that restricts access to the tools according to the authorization granted to a set of user groups. A user's access to the tools is controlled by assigning them to the appropriate user group.

All system administration tasks, including administration of the Operator Client environment, must be performed using the MDM Toolset environment.

In VoIP networks, restricting access to MDM Toolset tools is activated as part of securing the network. Restricting access to MDM Toolset tools is an optional feature activation applied during the MDM upgrade procedure for VoA networks.

For information on user group authorizations for access to MDM Toolset tools in VoA networks, see "User group mapping for restricted access to MDM Toolset tools in VoA networks" (page 206).

For information on user group authorizations for access to MDM Toolset tools in VoIP networks using IEMS as the central AAA server, see "IEMS user group mapping for MDM Toolset functions" (page 212).

Access to tools and utilities for the Operator Client environment

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.

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 by 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.

In VoA networks, the central AAA service of the User Administration Server supports action authorization to provide 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.

In VoIP networks using IEMS to provide central AAA services, the Operator Client tool access is mapped onto user groups as shown in "IEMS user group mapping for MDM Operator Client tools" (page 214). User access to the Operator Client tools is managed by assigning users to the user group appropriate to their responsibilities.

To avoid any confusion about the level of tool access allowed between the MDM Toolset environment and the Operator Client environment, all userids should be unique.

"Multiservice Data Manager tools and utilities" (page 205) 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, UA-IP, and PT-IP solutions.

For VoA networks, the table "Correspondence between MDM Toolset restricted access user groups and Operator Client roles" (page 209)provides the correspondence of the restricted access user groups defined for MDM Toolset tools and the roles defined for Operator Client tools access.

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

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

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

Restricted MDM Toolset access

"User group mapping for restricted access to MDM Toolset tools in VoA networks" (page 206) shows the authorized access to MDM Toolset tools for the restricted access user groups.

User group mapping for restricted access to MDM Toolset tools in VoA networks

MDM Toolset functions	MDM local userid	MDM Toolset restricted access user groups				
	root	emssprov	emsadmin	emsrw	emsro	emsmtc
Fault Menu						
Network Viewer	allow	allow	allow	allow	allow	deny
MSS Shelf view	allow	allow	allow	allow	allow	deny
Alarm Display: Active	allow	allow	allow	allow	allow	deny
Alarm Display: Log	allow	allow	allow	allow	allow	deny
Alarm Help	allow	allow	allow	allow	allow	allow
Network Status Bar	allow	allow	allow	allow	allow	deny
Component Information Viewer	allow	allow	allow	allow	allow	deny
Query Historical Alarms	allow	allow	allow	allow	allow	deny

MDM Toolset functions	MDM local userid	MDM Toolset restricted access user groups				
	root	emssprov	emsadmin	emsrw	emsro	emsmtc
Component Status Display	allow	allow	allow	allow	allow	deny
Configuration Menu						
Nodal Provisioning	allow	allow	allow	allow	deny	deny
Nodal Provisioning Template Editor	allow	deny	deny	deny	deny	deny
Configuration Audit Scheduler	allow	allow	allow	allow	allow	allow
Configuration -> Administration Sub-Menu						
Software download	allow	deny	allow	deny	deny	allow
Network Activation Tool	allow	allow	allow	allow	deny	deny
SASM	allow	allow	allow	allow	deny	deny
SISM	allow	allow	allow	allow	deny	deny
Succession Release Name	allow	allow	allow	allow	deny	deny
Service Data Backup and Restore	allow	allow	allow	allow	allow	allow
Accounting Menu						
Data Viewer	allow	allow	allow	deny	deny	deny
MDP configuration	deny	deny	deny	deny	deny	deny
MDP log viewer	deny	deny	deny	deny	deny	deny
MDP data viewer	deny	allow	allow	deny	deny	deny
Performance Menu						
Data Viewer	allow	allow	allow	deny	deny	deny
System Menu						
System -> Administration Sub-Menu						
Quick Start	allow	deny	deny	deny	deny	deny
Server administration	allow	allow	allow	allow	deny	deny
Service selection: system	allow	allow	allow	allow	allow	allow
Service selection: user	allow	allow	allow	allow	allow	allow
Service selection: OC	allow	allow	allow	allow	allow	allow

MDM Toolset functions	MDM local userid	MDM Toolset restricted access user groups				
	root	emssprov	emsadmin	emsrw	emsro	emsmtc
General management data router (GMDR) administration	allow	allow	allow	allow	deny	deny
Host group directory server (HGDS) administration	allow	allow	allow	allow	deny	deny
System log display	allow	allow	allow	allow	allow	allow
Log Browser	allow	allow	allow	allow	allow	allow
MDM license configuration	allow	deny	deny	deny	deny	deny
System -> Security Sub-Menu						
Disruptive Command Safeguard	allow	deny	allow	deny	deny	deny
Password encryption	allow	deny	deny	deny	deny	deny
System -> Utilities Sub-Menu						
UNIX access	allow	deny	allow	deny	deny	deny
Remote SSH access	allow	deny	allow	deny	deny	deny
Remote access	allow	deny	allow	deny	deny	deny
Enhanced Multiservice Switch interface controller (EPIC)	allow	allow	allow	allow	deny	deny
Operational commands	allow	allow	allow	allow	allow	deny
Command Console	allow	allow	allow	allow	allow	deny
On-line documentation	allow	allow	allow	allow	allow	allow
Memory utilization	allow	allow	allow	allow	allow	allow
Network Model shared memory utilization	allow	allow	allow	allow	allow	allow
System -> Custom Sub-Menu						
None	allow	allow	allow	allow	allow	allow

For VoA solutions, the following correspondence exists between MDM Toolset restricted access user groups and Operator Client roles:

Correspondence between MDM Toolset restricted access user groups and Operator Client roles

Operator Client role	MDM Toolset user group
View	emsro
Manage	emsrw
Admin	emsadm

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

In VoIP solutions, IEMS 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.

IEMS user group mappings

IEMS 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 IEMS 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 IEMS 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.

IEMS group mapping for MDM Toolset functionality

"IEMS user group mapping for MDM Toolset functions" (page 212) shows the mapping between the IEMS groups and the MDM Toolset functions.

IEMS user group mapping for MDM Toolset functions

MDM Toolset functions	MDM local userid	IEMS group				
	root	emsro	emsrw	emsmtc	emssprov	emsadmin
Alarm Display: Active	allow	allow	allow	deny	allow	allow
Alarm Display: Log	allow	allow	allow	allow	allow	allow
Alarm Help	allow	allow	allow	allow	allow	allow
Command Console	allow	allow	allow	deny	allow	allow
Component Information Viewer	allow	allow	allow	deny	allow	allow
Component Status Display	allow	allow	allow	deny	allow	allow
Configuration Audit Scheduler	allow	allow	allow	allow	allow	allow
Data Synchronization Administration	allow	allow	allow	allow	allow	allow
Data Viewer	allow	deny	deny	deny	allow	allow

MDM Toolset functions	MDM local userid	IEMS group				
	root	emsro	emsrw	emsmtc	emssprov	emsadmin
Disruptive Command Safeguard	allow	deny	deny	deny	deny	allow
Enhanced Multiservice Switch interface controller (EPIC)	allow	deny	allow	deny	allow	allow
General management data router (GMDR) administration	allow	deny	allow	deny	allow	allow
Host group directory server (HGDS) administration	allow	deny	allow	deny	allow	allow
Log Browser	allow	allow	allow	allow	allow	allow
MDM license	allow	deny	allow	deny	allow	deny
Succession release update	allow	deny	allow	deny	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	deny	allow	allow
Memory utilization	allow	allow	allow	allow	allow	allow
Network Activation Tool	allow	deny	allow	deny	allow	allow
Service Data Backup and Restore	allow	deny	deny	allow	allow	allow
Network Model shared memory utilization	allow	allow	allow	allow	allow	allow
Network Status Bar	allow	allow	allow	deny	allow	allow
Network Viewer	allow	allow	allow	deny	allow	allow
Nodal Provisioning	allow	deny	allow	deny	allow	allow
Nodal Provisioning Template	allow	deny	allow	deny	allow	allow
On-line documentation	allow	allow	allow	allow	allow	allow
Operational commands	allow	allow	allow	deny	allow	allow

MDM Toolset functions	MDM local userid	IEMS group				
	root	emsro	emsrw	emsmtc	emssprov	emsadmin
Password encryption	allow	deny	deny	deny	deny	deny
Query Historical Alarms	allow	allow	allow	deny	allow	allow
Quick Start	allow	deny	deny	deny	deny	deny
Server administration	allow	deny	allow	deny	allow	allow
Service selection	allow	allow	allow	deny	allow	allow
Shelf view	allow	allow	allow	deny	allow	allow
Software download	allow	deny	deny	allow	deny	allow
Succession ATM Software Migration	allow	deny	allow	deny	allow	allow
Succession IP Software Migration	allow	deny	allow	deny	allow	allow
System log display	allow	allow	allow	deny	allow	allow
UNIX access	allow	deny	deny	deny	deny	allow
Note: MDP configuration and log viewer commands must be accessed using the MDP administrator userid maintained locally on the MDM workstation.						

IEMS group mappings for MDM Operator Client

"IEMS user group mapping for MDM Operator Client tools" (page 214) shows the mapping between the IEMS groups and the tools available through the Operator Client application.

IEMS user group mapping for MDM Operator Client tools

MDM Operator Client Resources	IEMS 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

MDM Operator Client Resources	IEMS group				
	emsro	emsrw	emsmtc	emssprov	emsadmin
Configuration					
Nodal Provisioning	deny	deny	deny	allow	allow
Template editor	deny	deny	deny	deny	allow
Performance					
Data Viewer	deny	deny	deny	allow	allow
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

IEMS group mappings for MSS/MG15000 functionality

"IEMS user group mapping for MSS/MG15000 access privileges" (page 215) shows the mapping between the IEMS groups and the MSS/MG15000 access privileges.

IEMS user group mapping for MSS/MG15000 access privileges

MSS/MG15000 UserId attribute	IEMS 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

MSS/MG15000 UserId attribute	**IEMS group**				
	mgro	**mgrw**	**mgmtc**	**mgsprov**	**mgadmin**
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 203)

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:

Step	Action
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 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
```

4 This procedure is complete.

—End—

Carrier VoIP

MSS15K, MG15K, and MDM in Carrier VoIP Networks Security and Administration (PT-AAL1/UA-AAL1/UA-IP)

Publication: NN10180-611
Document status: Standard
Document version: 09.01
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.