Carrier VoIP

MSS15K, MG15K and MDM in Carrier VoIP Networks - Securing Network Elements

NN10180-612

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

New in this release

ATTENTION

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

This document is intended for people who are securing Nortel Multiservice Switch 15000 switches, Nortel Media Gateway 15000 switches, and Nortel Multiservice Data Manager (MDM) Servers in a Carrier Voice over IP UA-IP or PT-IP network.

Securing other network elements in a Carrier Voice over IP network is beyond the scope of this document. For more information about solution-level security and security aspects of other network elements, see NN10402-600 ATM/IP Solution-level Security and Administration.

Securing the MG15000 call control connections to the gateway controller is beyond the scope of this document. For more information, see NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals.

For information on security administration tasks in a secure VoIP network, see NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP.

The following sections detail what's new in *Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration - Securing Network Elements (NN10180-612)* for release (I)SN09U.

- "Features" (page 3)
- "Other changes" (page 3)

Features

There have been no updates to the document in this release.

Other changes

There are no other changes that are not feature-related.

Preparing to secure the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager network elements

The following activities are required to prepare for successfully securing Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager network elements in a VoIP network:

Terminology

To avoid any confusion that could result in problems with securing the network elements, the following terminology is used in this guide:

- An MDM Server is the set of MDM tools and applications that provides:
  - fault, performance and security data to the higher level management systems (such as IEMS and CS2000 Core Manager)
  - FCAPS and system administration functionality using the MDM Toolset environment

  - FCAPS functionality using the Operator Client environment supported by Java Web Start (JWS) software
  - interfaces to the IEMS central AAA service

- An MDM Server workstation is the hardware platform that runs the Sun Solaris 9 operating system and MDM Server software.
- A security domain is the set of interconnected Multiservice Data Manager, Media Gateway 15000 and IEMS network elements that must be secured following the methodology specified in this guide to minimize loss of surveillance data flow or loss of connectivity to management functions.
- The IEMS central security server is the central AAA system that provides centralized user authentication, authorization and administration services for a security domain.
- An IPSec configuration record is the document, spreadsheet or other job aid that is used to record IPSec security association information for the links in the security domain. This record is filled out during the planning activities and referred to during the activation stages.

Understanding how the network elements are secured

The Multiservice Data Manager, Multiservice Switch 15000 switches, and Media Gateway 15000 switches are secured to prevent unauthorized access to network management functions and data. This is done by applying security measures in several different areas:

- securing the network element platforms by removing unnecessary software functions that could be used to gain access to the system, by restricting access by remote systems, by providing session management for all authorized access, and by providing local user access controls.
- protecting the communication links used to send management commands and OAM&P data from one network element to another. Connections between the desktop (X11 access) and the MDM Server are secured using the SSH protocol. Connections between the desktop (Operator Client access) and the MDM Server are secured using HTTPS and SAML protocols. Connections between MSS/MG15000 switches and MDM Servers, and between MDM Servers are secured using the IPSec protocol. Connections between MDM Servers and the IEMS are secured using the SSH and RADIUS protocols.
- performing user access authentication and authorization at a central IEMS system to enable better control of user access across all the network elements. This includes restricting user access to the minimum set of functions required to perform the job.

- providing security audit logs that can be regularly monitored at a central IEMS system for auditing of security functions to detect unauthorized access attempts and configuration changes

For more information on how these security measures operate, see *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

Identifying the network elements to be secured as a group

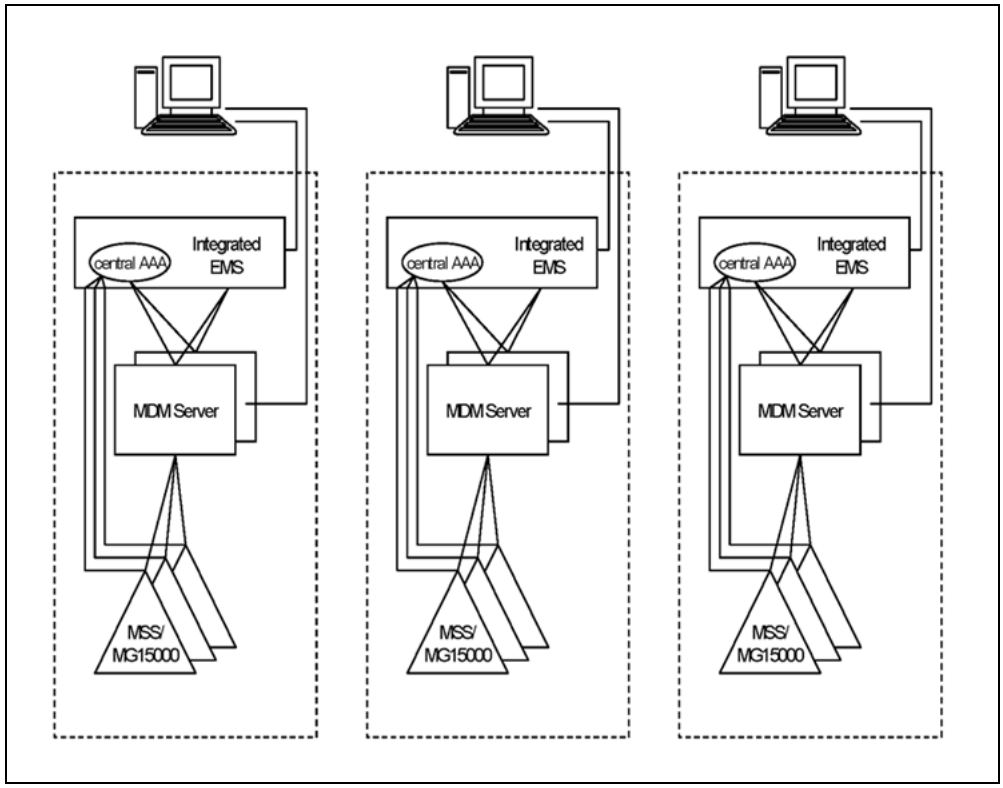
Because of the peer-to-peer nature of the protocols used to secure the OAM&P communications links and the use of the IEMS central AAA service, all MSS/MG15000, Media Gateway 15000, Multiservice Data Manager and IEMS network elements with OAM&P communication links to each other must be secured as a group.

Note: Only OAM&P connections are secured through the procedures in this guide.

The following figure shows a simplified network configuration where the MDM Servers are deployed to provide dedicated services for regional offices. In this configuration, the IEMS in the regional office provides central user authentication and authorization for the MDM Servers and MSS/MG15000 switches in the office, and collects the security audit logs, fault and performance data from the switches and Servers.

In this sample figure, each regional office forms an independent security domain.

Security domain example



Review your network architecture and identify all the security domains that need to be secured.

The order in which the security domains are secured depends on the operational needs of the network. The ordered work flow in this guide applies only to securing the network elements contained in a single security domain.

Understanding migration requirements

All of the network elements in the security domain must have migrated to an SN08 or later release prior to activating the security features. This includes the Multiservice Switch 15000, Media Gateway 15000, Multiservice Data Manager and IEMS network elements. For more information on upgrading MSS/MG15000 switches and MDM Servers, see:

- *NN10419-461 Upgrading Nortel Multiservice Switch 15000 and Media Gateway 15000/20000 in Carrier Voice over IP Networks*
- *NN10440-450 Upgrading the Carrier Voice over IP Network*

The Domain Name Server (DNS) for the network must be available.

All UNIX-based desktop systems that are used to connect to MDM Servers must have the SSH client installed and operational.

Understanding IEMS requirements

Once the IEMS system has migrated to an SN08 or later release, the following must be completed before starting to secure the security domain:

- The IEMS must be configured to provide central authentication, authorization and administration services.
- The IEMS must have all the MDM and MSS/MG15000 network elements in the security domain. The MSS/MG15000 network elements are added as RADIUS clients.
- The IEMS RADIUS security keys (shared secrets) for use in configuring the RADIUS client on MSS/MG15000 network elements must be transmitted to the MSS/MG15000 sites by a secure method. Do not use any clear text method of sending the security keys to remote sites.

Defining the order for securing the network elements and communication links in the security domain

Consider the following when determining the order for securing network elements and OAM&P communication links in the security domain:

- Installation and activation of the IPSec and SSH security protocols on MDM Servers will require a reboot of the workstation.
- The initial configuration of MSS/MG15000 switches must be done on site with a VT100 terminal plugged into the local port.
- If there is an MSS15000 acting as a gateway for a group of MG15000 switches, the MSS15000 gateway is secured in exactly the same was as the other MG15000 switches.
- In order to secure a link using IPSec, the security protocol must be activated at each end of the link. Once the protocol as been activated at one end of the link, the link will be non-operational until the protocol has been activated at the other end of the link. The procedure order specified in this guide minimizes any loss of communication that could affect northbound data flows or connection to management functions.
- Once IPSec software is activated on the MDM Server, all IP packets that are not explicitly covered by the defined IPSec policies will be accepted.

Providing the information required to secure communication links

Before using the security activation procedures for securing communication links, define, document, and verify the configuration data required by the procedures.

SSH links

No configuration is required after installation of the SSH software.

Central AAA service links

To configure the RADIUS client on MSS/MG15000 switches, provide the following information:

- MSS/MG15000 management Vr IP address (nas IP address)
- MSS/MG15000 UDP port number
- IEMS/AAA server IP address and RADIUS shared secret

To configure the IS client on MDM Servers, provide the following information:

- IEMS fully qualified domain name (FQDN), Nortel domain name

IPSec links

ATTENTION

In order to avoid problems with configuring IPSec on links, all the security association data required to configure IPSec links must be planned, recorded and validated before using the procedures.

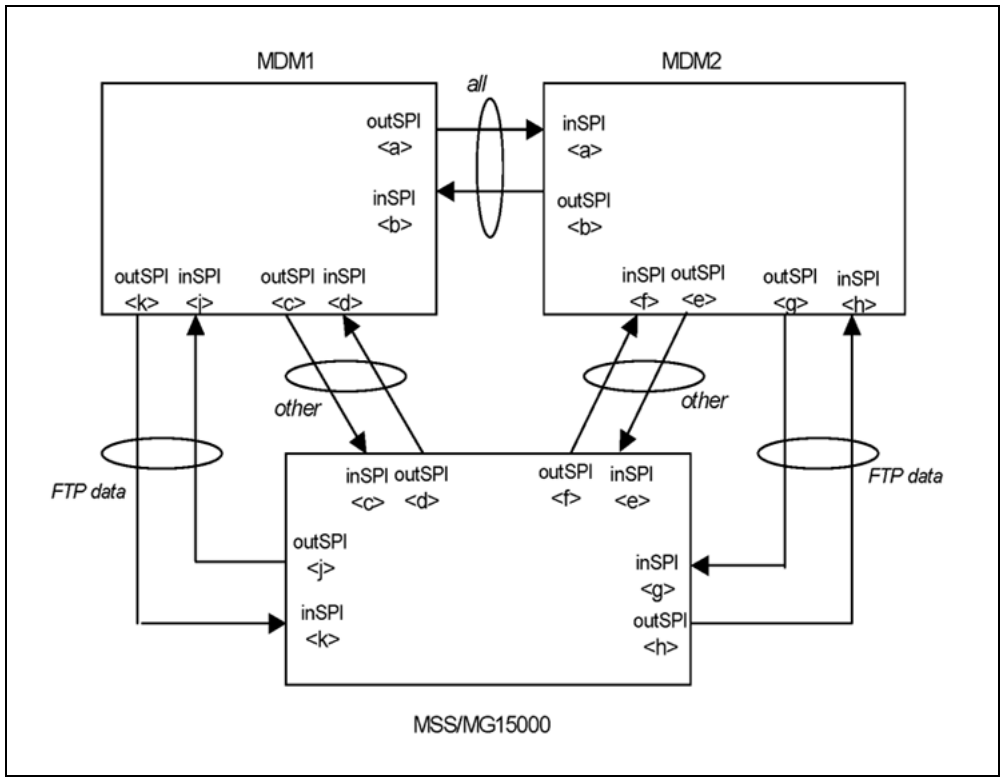
The following requirements apply to defining security associations for IPSec links:

- Security associations (SAs) must be defined for each network element end point of the link.
- Two SAs are defined on each network element for the link: one SA for outgoing data and one SA for incoming data.
- SAs are organized in a particular order for lookup. On the MSS/MG15000, SAs are sorted by a Policy number that is associated with the SA at creation time. On the MDM Server, the lookup order is controlled by an Index number which is associated with the SA at creation time.
- An SA is identified by an SP index (SPI). All SPIs on a network element must be unique.
- The SA defined for one end of the link must align with the SA defined at the other end of the link as follows:
  - when a direction of "in" is used on one network element, the direction "out" must be used on the other network element.
  - the *inSPI* value on one network element will be the same as the *outSPI* value on the other network element.
  - the source address on one network element must be the same as the destination address on the other network element.

— the protocol, encryption algorithms and security keys must be the same.

The following figure shows the alignment of the SPIs for the security associations between two MDM Servers and between the MDM Servers and an MSS/MG15000 switch.

SPI alignment between MDM Servers and MSS/MG15000 switches



Security associations between MDM Servers

The following applies to security associations defined between MDM Servers:

- all security associations use the ESP protocol, the SHA1 data authentication algorithm and the AES data encryption algorithm

The following table shows the information to specify the four SAs for a link between two MDM Servers.

Information alignment for the security association between two MDM Servers

NE	data flow	in SPI	out SPI	src IP addr	dest IP addr	protocol	encryption / authentication algorithm	key
MDM1	out		<a>	MDM1	MDM2	esp	aes / sha1	system generated
MDM2	in	<a>		MDM1	MDM2	esp	aes / sha1	system generated
MDM2	out		<b>	MDM2	MDM1	esp	aes / sha1	system generated
MDM1	in	<b>		MDM2	MDM1	esp	aes / sha1	system generated

Security associations between MSS/MG15000 switches and MDM Servers

The following applies to security associations defined between MSS/MG15000 switches and MDM Servers:

- Security associations for all data flows except FTP data use the ESP protocol, the AES data encryption algorithm and the SHA1 data authentication algorithm
- Security associations for the FTP data flow use the AH protocol and the MD5 authentication algorithm. Since the data in the FTP data channel is not sensitive, and encrypting and decrypting the volume of data could have performance impacts, only the data authentication protocol is used.

The following table shows the information to specify the eight SAs for the link between MDM1 and an MSS/MG15000 switch.

Information alignment for the security associations between MDM1 and an MSS/MG15000 switch

NE (data type)	data flow	in SPI	out SPI	src IP addr	dest IP addr	protocol	encryption / authentication	key

							algorithm	
MDM1 (other)	out		<c>	MDM1	MSS	esp	aes / sha1	system generated
MSS (other)	in	<c>		MDM1	MSS	esp	aes / sha1	system generated
MSS (other)	out		<d>	MSS	MDM1	esp	aes / sha1	system generated
MDM1 (other)	in	<d>		MSS	MDM1	esp	aes / sha1	system generated
MDM1 (FTP data)	out		<j>	MDM1	MSS	ah	- / md5	system generated
MSS (FTP data)	in	<j>		MDM1	MSS	ah	- / md5	system generated
MSS (FTP data)	out		<k>	MSS	MDM1	ah	- / md5	system generated
MDM1 (FTP data)	in	<k>		MSS	MDM1	ah	- / md5	system generated

The following table shows the information to specify the eight SAs for a link between MDM2 and an MSS/MG15000 switch.

Information alignment for the security associations between MDM2 and an MSS/MG15000 switch

NE (data type)	**data flow**	**in SPI ***	**out SPI ***	**src IP addr**	**dest IP addr**	**protocol**	**encryption / authentication algorithm**	**key**
MDM2 (other)	out		<e>	MDM2	MSS	esp	aes / sha1	system generated
MSS (other)	in	<e>		MDM2	MSS	esp	aes / sha1	system generated
MSS (other)	out		<f>	MSS	MDM2	esp	aes / sha1	system generated
MDM2 (other)	in	<f>		MSS	MDM2	esp	aes / sha1	system generated
MDM2 (FTP data)	out		<f>	MDM2	MSS	ah	- / md5	system generated

Note: * *inSPI* and *outSPI* values are generated by the pp_ipsecsetup command used on the MDM.

NE (data type)	data flow	in SPI *	out SPI *	src IP addr	dest IP addr	protocol	encryption / authentication algorithm	key
MSS (FTP data)	in	<f>		MDM2	MSS	ah	- / md5	system generated
MSS (FTP data)	out		<h>	MSS	MDM2	ah	- / md5	system generated
MDM2 (FTP data)	in	<h>		MSS	MDM2	ah	- / md5	system generated

Note: * *inSPI* and *outSPI* values are generated by the pp_ipsecsetup command used on the MDM.

Assigning SPIs for security associations between MDM Servers

MDM to MDM SPIs are assigned manually. The range of values used for these SPIs must not overlap with the range of values used for MDM to MSS/MG15000 SPIs. The recommended range for these SPIs is 500-599.

Assigning SPIs for security associations between an MDM Server and an MSS/MG15000 switch

The SPIs for the initial security associations between each MSS/MG15000 switch and MDM1 are assigned manually. The recommended range of SPI values is 400-499. The values are assigned when the SA is initialized on MDM1. For example,

- for the SA with MSS/MG1: *inSPI*=400, *outSPI*=401
- for the SA with MSS/MG2: *inSPI*=402, *outSPI*=403
- for the SA with MSS/MG3: *inSPI*=404, *outSPI*=405

When the initial SAs are set up on the MSS/MG15000 switches for the links to MDM1, the corresponding SPIs must be used:

- for the SA on MSS/MG1: *inSPI*=401, *outSPI*=400
- for the SA on MSS/MG2: *inSPI*=403, *outSPI*=402
- for the SA on MSS/MG3: *inSPI*=405, *outSPI*=404

Once the initial connection between the switch and the first MDM Server (MDM1) has been secured manually, the pp_ipsecsetup command script is used to automatically apply the security associations on the other MDM Server (MDM2) and the MSS/MG15000 switch. The script generates these *inSPI* and *outSPI* values automatically. Once these security associations have been configured, the security association information must be displayed and the automatically generated SPI values for the associations

must be recorded in the IPSec configuration record. Failure to record this information may result in duplicate SPIs being assigned on one of the network elements.

When the security associations for the FTP data flow between MDM1 and the MSS/MG15000 switches is configured, refer to the recorded list of SPIs for the security associations already set up to make sure that you are using unique SPIs.

Identifying userids to transfer from MDM Servers and MSS/MG15000 switches to IEMS for central authorization and authentication

All the userids and groups that will use the central user authentication and authorization service must be identified, along with the userid authorization level. This includes MDM Toolset userids, Solaris userids, Operator Client userids and MSS/MG15000 switch userids. These userids will have to be manually transferred from the network elements to the IEMS central authentication and authorization system.

On IEMS, a userid is assigned to a group which defines the tasks that the userid is authorized to perform. The MDM and MSS/MG15000 userids must be assigned to IEMS groups that provide the same access privileges that were assigned on the MDM Servers and MSS/MG15000 switches. The mapping of MDM and MSS/MG15000 userid access privileges onto IEMS groups is described in *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*. For information on adding userids on IEMS, refer to *NN10336-611 IEMS Security and Administration*.

Some Solaris and MDM userids and groups, and some MSS/MG15000 userids cannot be moved to the IEMS central AAA service and must remain configured locally. Refer to "Securing user access for the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data M" (page 89) for the lists of these userids and groups.

Understanding the task flow for activating security features for the security domain

The following steps provide the order in which the various network elements in the security domain must be secured. This order has been chosen to minimize the downtime of the communication links, and ensure continued northbound flow of OAM&P data and access to the network elements for management functions.

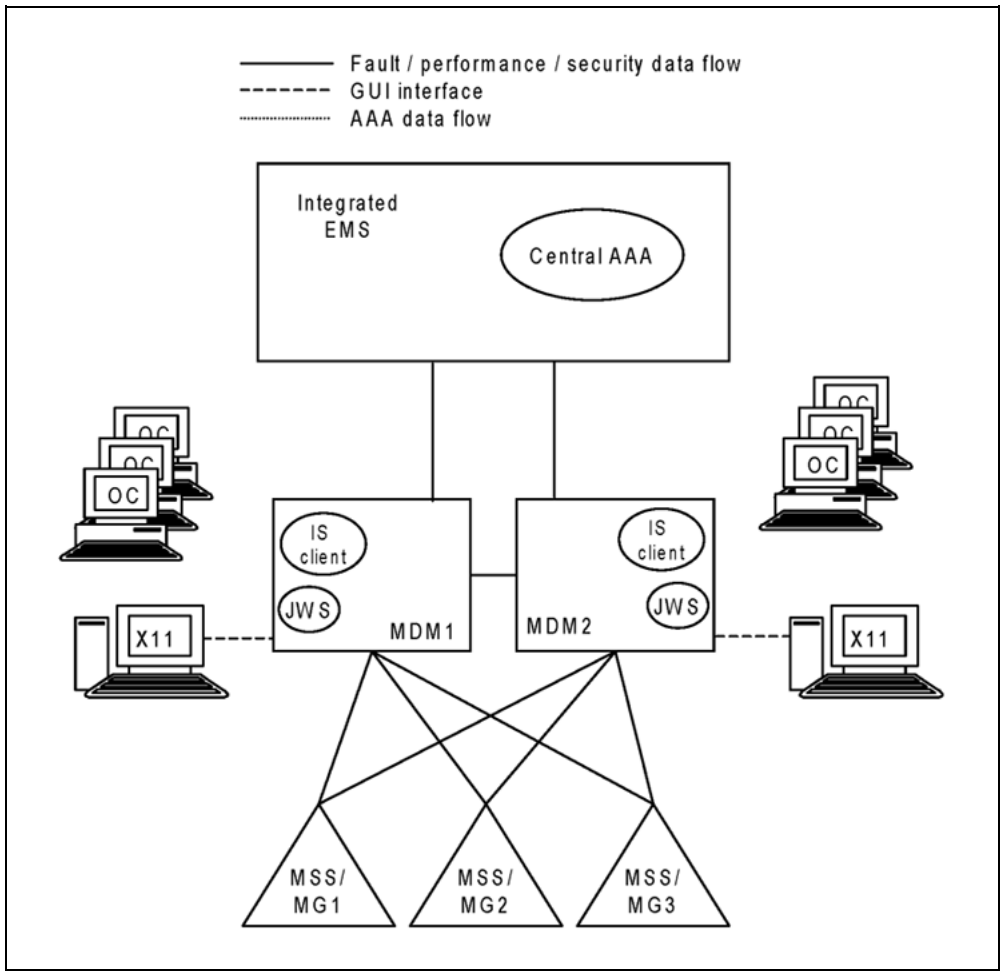
Note: All the procedures in the task flow require:

- root userid and password for the MDM Servers
- system administrator userid and password for the MSS/MG15000 switches

For purposes of this task flow, MDM1 is the first MDM Server workstation to be secured, followed by MDM2. MSS/MG1 is the first MSS/MG15000 switch to be secured, followed by MSS/MG2 and MSS/MG3. X11 refers to the desktops using X11 to access the MDM Toolset user environment. OC refers to the desktops using the Operator Client application to access the MDM Operator Client user environment.

The following figure shows the sample security domain before security activation is started.

Sample security domain before security activation

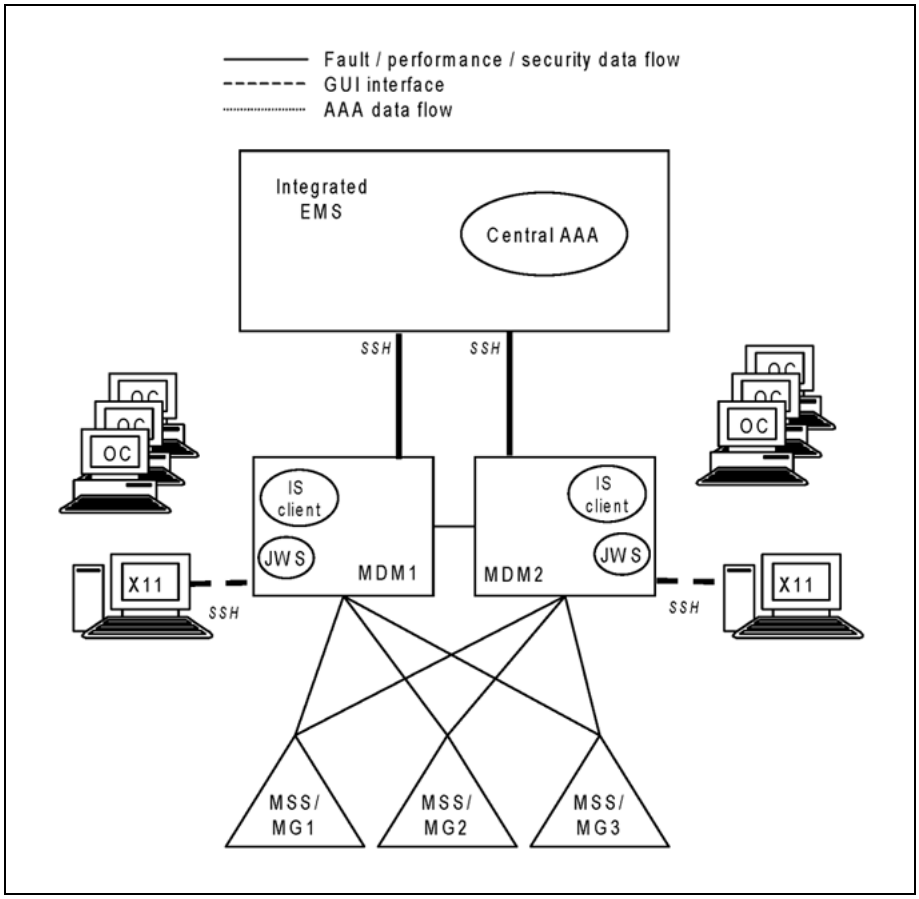


The following stages show the order in which the network elements and links must be secured. As the network elements and links are secured, they will be shown in bold in the associated figure.

1. Install and activate the SSH protocol on the MDM Servers, starting with MDM1.

   For task flow and detailed procedures, see "Using SSH to secure X11 desktop and IEMS connections with the MDM" (page 29).

Sample security domain after SSH activation



After this stage, X11 desktops installed with SSH can communicate over an SSH-secured link with the MDM Servers. All data, including passwords, will be encrypted.

At this point, IEMS can be configured to access an SN09 MDM Server.

> ***Note:*** Desktops using Operator Client access will not be operational until the MDM Server is configured to use IEMS central AAA and userids have been defined on the IEMS.

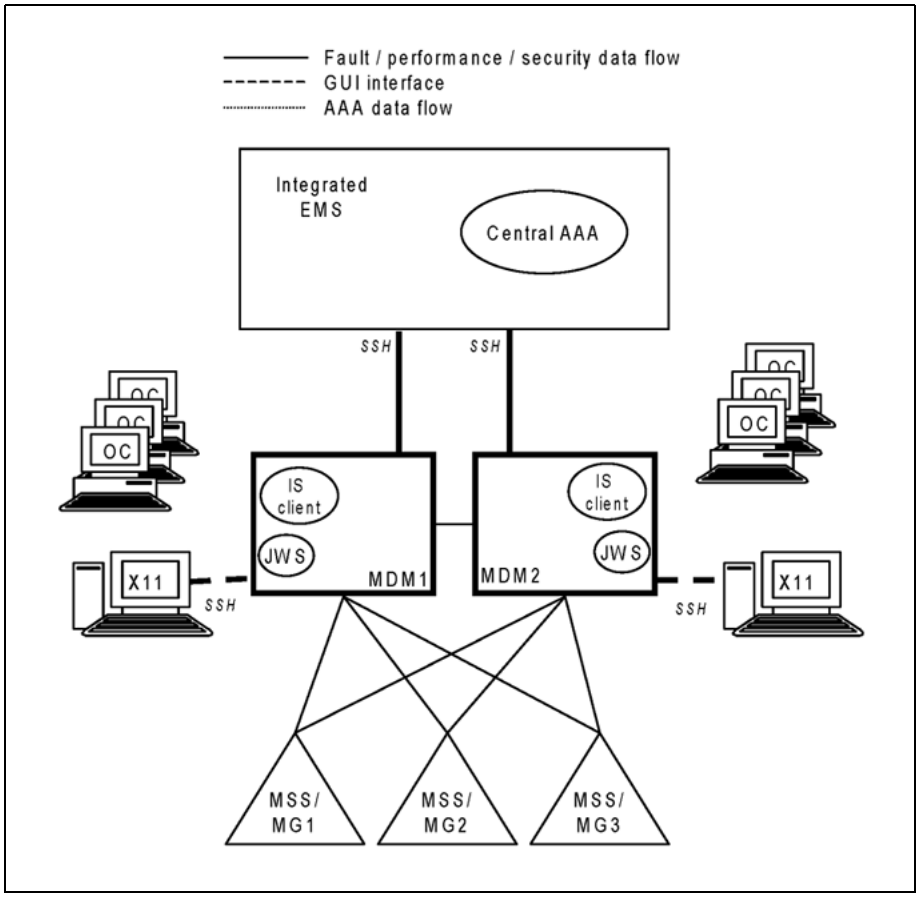
2. Starting with MDM1, harden the MDM platform to:
   - remove unused userids
   - control userid and password lengths
   - remove insecure remote access methods, such as telnet. SSH capabilities replace these functions.
   - restrict remote access
   - control access to MDM tools through passwords

Note 1: The MDM Servers are rebooted as part of this phase.

Note 2: Only the MDM script for hardening the Solaris operating system is used in this step.

For task flow and detailed procedures, see "Hardening the Multiservice Data Manager Server platform" (page 43).

Sample security domain after MDM platform hardening



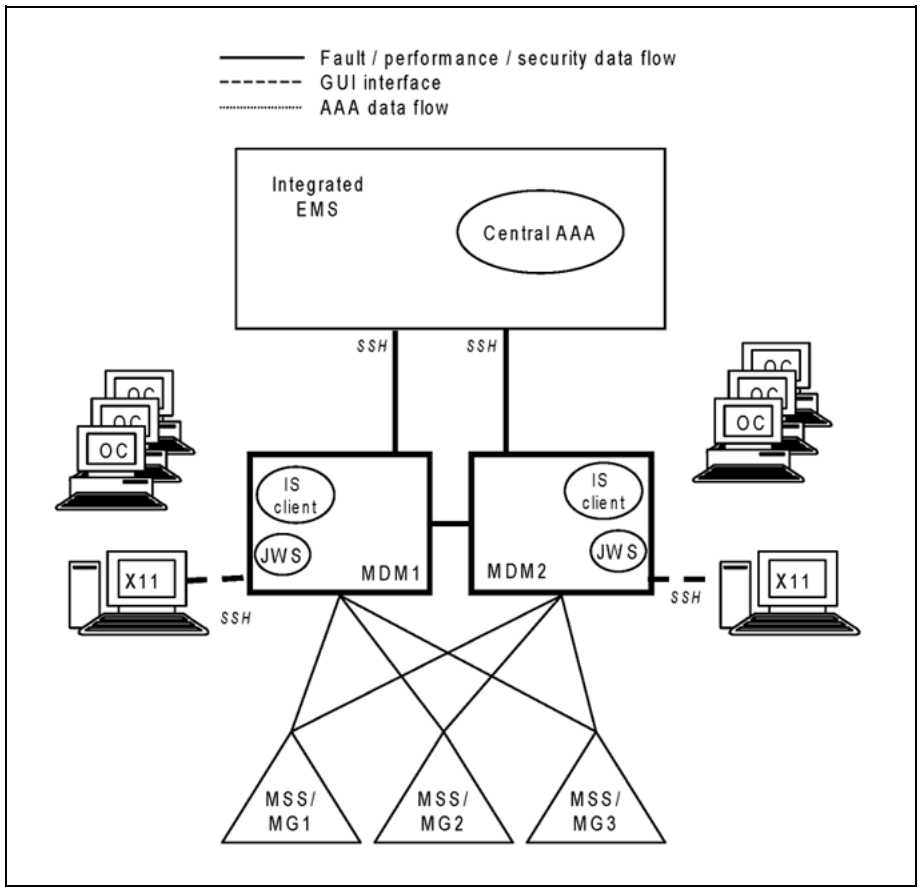
After this phase, only SSH-enabled desktops and an SSH-enabled IEMS can communicate with the MDM Servers.

3. Using the IPSec protocol, secure the links between the two MDM Servers.

   Note: The MDM Servers will be rebooted as part of this phase.

   For task flow and detailed procedures, see "Securing links between MDM Servers using IPSec" (page 35).

Sample security domain after IPSec enabled between MDM Servers

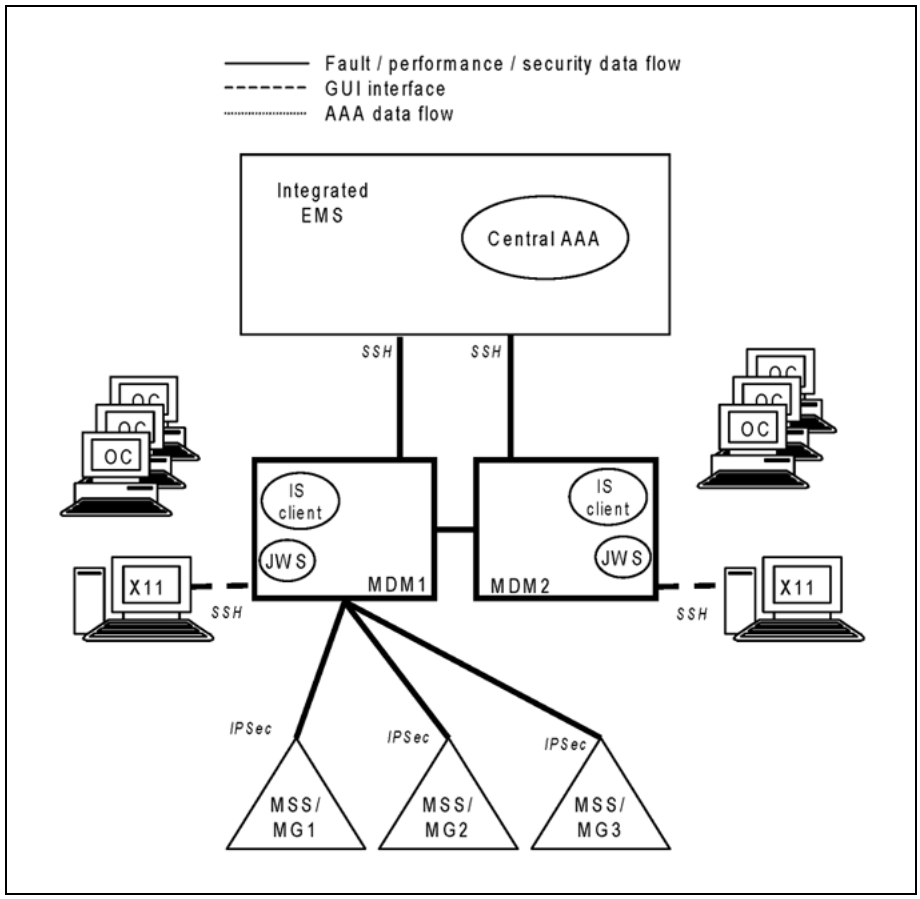


After this phase, the link between the two MDM Servers is secured with IPSec. All data is encrypted and authenticated.

4. Using the IPSec protocol, secure the links between the MDM Servers and the MSS/MG15000 switches.

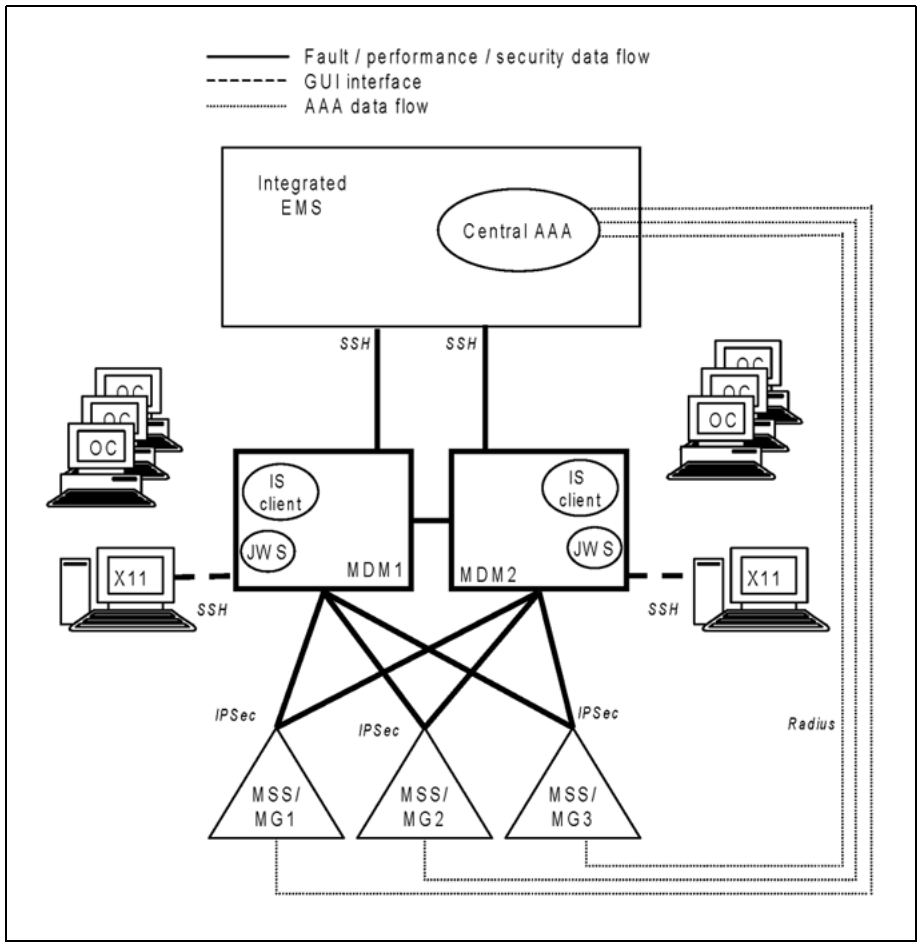
   For task flow and detailed procedures, see "Securing links between MDM Servers and MSS/MG15000 switches using IPSec" (page 55).

Sample security domain after IPSec is enabled between MDM1 and the MSS/MG15000 switches



After the links between MDM1 and the MSS/MG15000 switches have been secured, all communication with the MSS/MG15000 switches is through MDM1 using the IPSec-secured links. The links to MDM2 are not operational.

Sample security domain after IPSec is enabled between MDM2 and the MSS/MG15000 switches

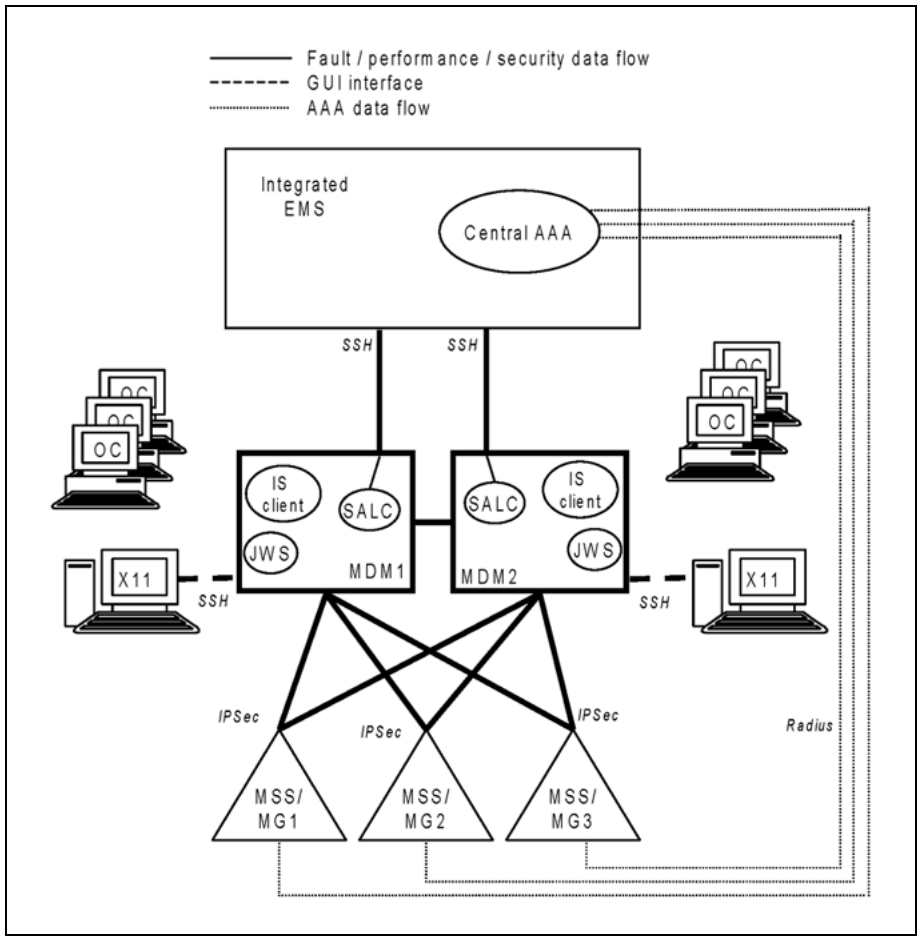


After the links between MDM2 and the MSS/MG15000 switches have been secured, data flows normally between the switches and the MDM Servers. This procedure also sets up the IPSec bypass for the RADIUS links that will carry authentication data between the switches and the IEMS central AAA service.

5. Enable sending of security audit logs to the IEMS.

   For task flow and detailed procedures, see "Sending security audit logs from an MDM Server to IEMS" (page 73).

Sample security domain after enabling security audit log transmission to IEMS

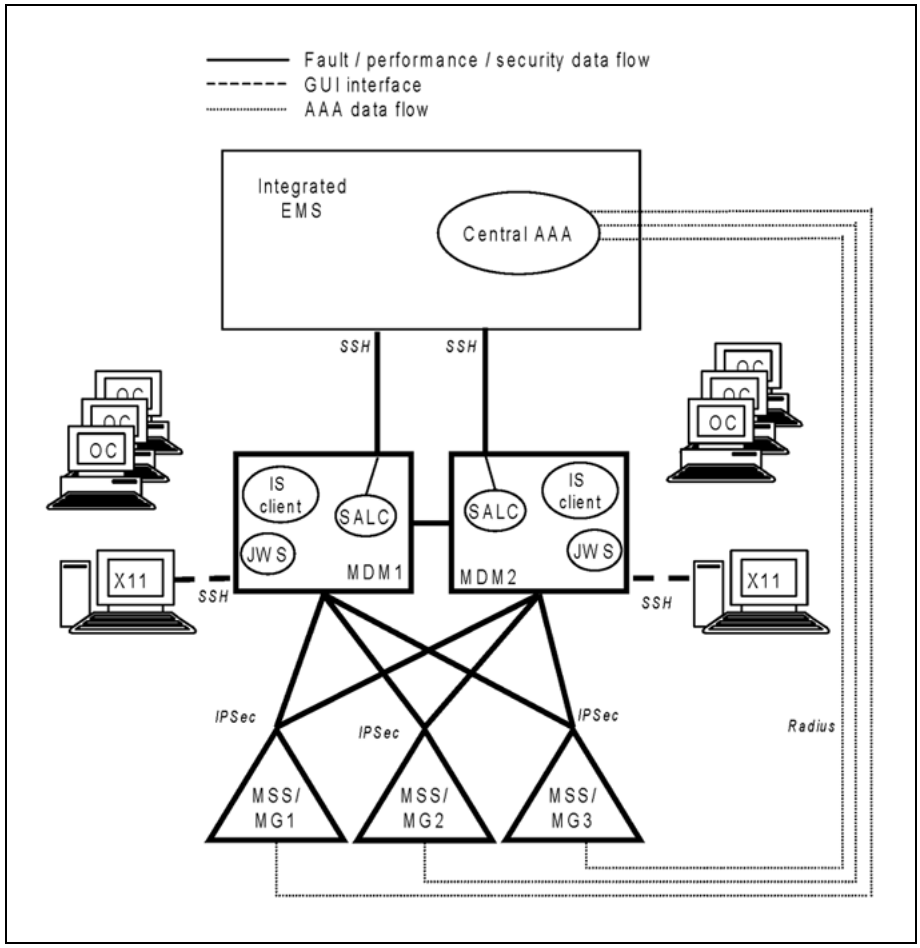


After this phase, all Solaris, MDM Server and MSS/MG15000 security audit logs are sent to the syslog daemon on the IEMS workstation in either Custlog V2 format or syslog format, or both. Sun Solaris logs are also sent to the IEMS.

6. If required, third party firewall software can be configured on the MDM Servers at this stage. Use the appropriate third party software documentation to set up the firewall, and 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 the MDM Server port mappings.
7. Harden the MSS/MG15000 platform to:
   - set up session timeout periods
   - restrict the remote systems that are allowed access

For task flow and detailed procedures, see "Hardening the Multiservice Switch 15000 or Media Gateway 15000 platform" (page 85).

Sample security domain after hardening the MSS/MG15000 platforms



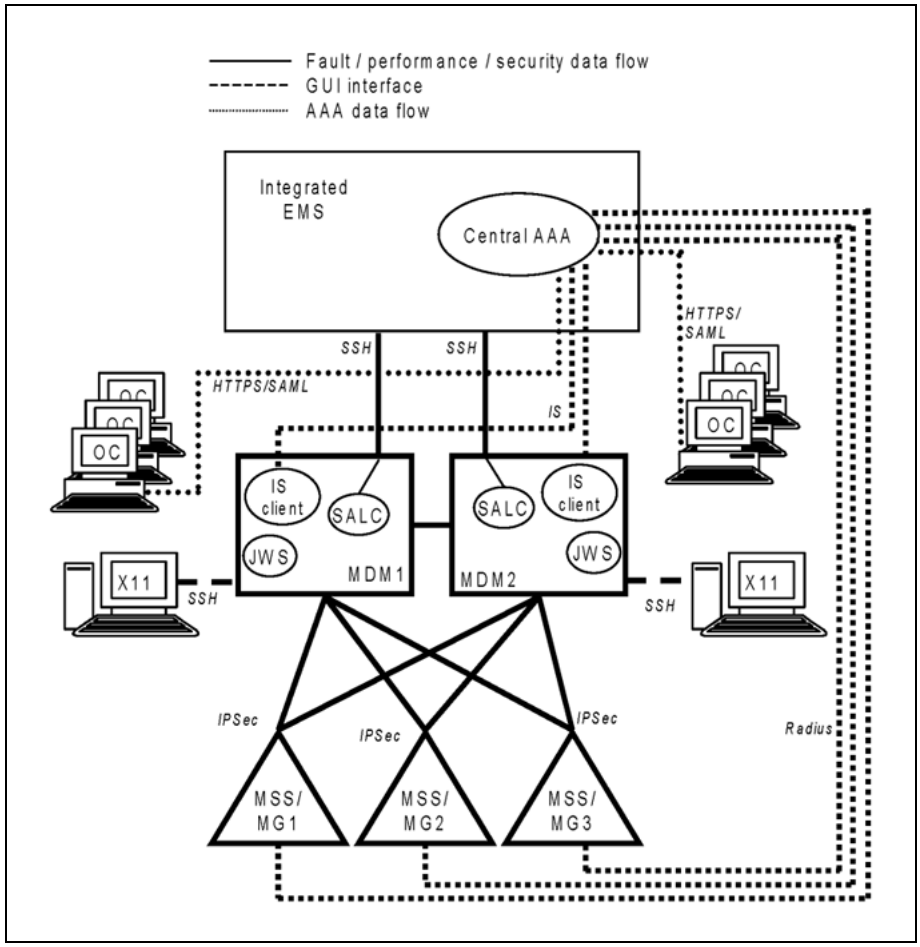
8. Migrate users to the central AAA service using the IEMS central security server. This involves:
   - configuring the IS client on MDM Servers
   - configuring the RADIUS client on MSS/MG15000 switches
   - transferring userids from MDM Servers and MSS/MG15000 switches to the IEMS

   For task flow and detailed procedures, see "Securing user access for the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data M" (page 89).

   Note 1: Not all MDM UNIX userids can be transferred to IEMS. See "Transferring userids from MDM to IEMS" (page 97) for more information.

Note 2: Some locally defined userids must be maintained on the MSS/MG15000 switches in case of loss of communication with the IEMS. See "Transferring userids from MSS/MG15000 to IEMS" (page 101) for more information.

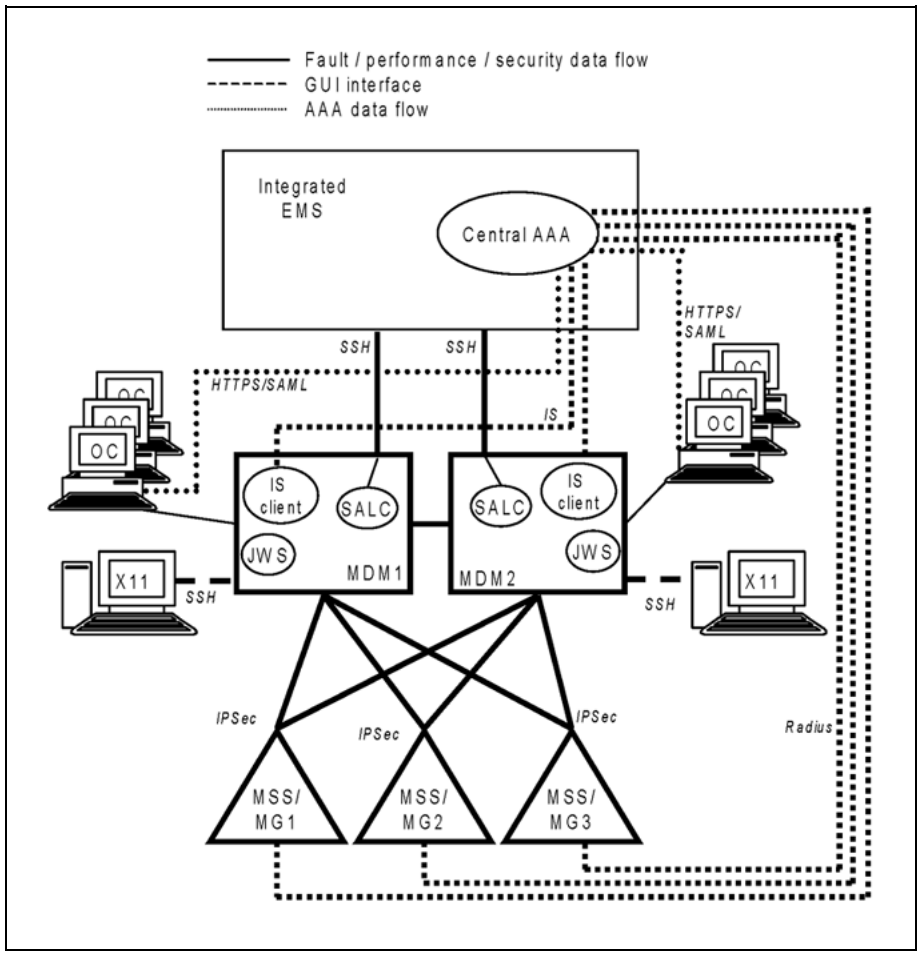
Sample security domain after enabling IEMS central authentication and authorization



After this phase, user authentication and authorization for most userids is performed by the IEMS. Unused local userids have been removed from the MDM Servers and MSS/MG15000 switches.

9. Confirm Operator Client access from the desktops.

Sample security domain after security activation is complete



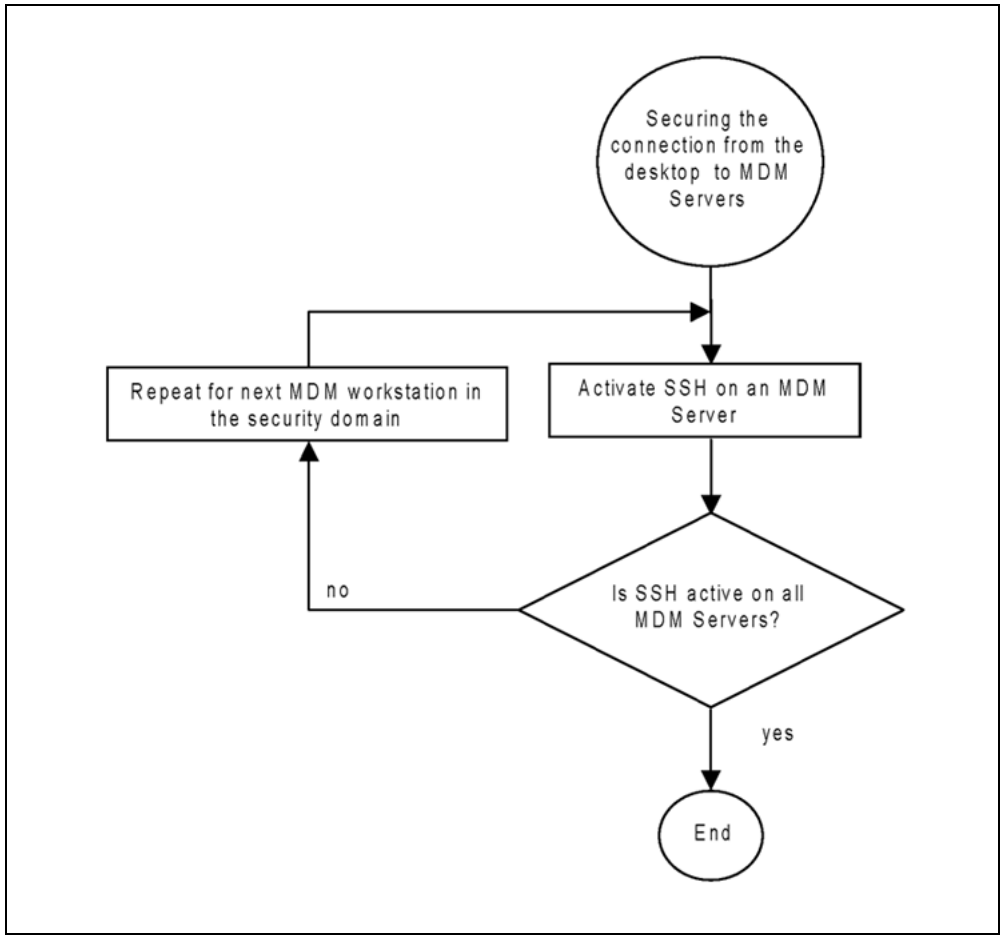
After this stage is complete, the security domain has been secured.

Using SSH to secure X11 desktop and IEMS connections with the MDM

The following task flow shows the procedures to follow to activate the Secure Shell (SSH) protocol to secure communication links between:

- desktops using X11 and MDM Servers for access to MDM Toolset applications
- MDM Servers and the IEMS for transfer of fault, performance and security data

Task flow for enabling SSH between the X11 desktop and IEMS



Activating SSH on an MDM Server

The SSH security protocol is used to secure communications between:

- the X11 desktop and an MDM Server
- the IEMS and an MDM Server

Prerequisites

Before using this procedure:

- Ensure the desktop using X11 to connect to the MDM Server has SSH installed.
- Determine if the MDM server is running on a Sun Fire V480 or a Sun Netra 240 with SPFS installed.

Installing and activating SSH software on the MDM Server

Repeat this procedure for each MDM Server in the security domain.

Step	Action

On the MDM Server

1 Log in to the MDM Server as root.

2 Verify that the SSH software has been installed as part of the upgrade procedures by executing the following command:

```
pkginfo | grep -i ssh
```

For Sun Fire V480 servers, the following output is expected:

```
# pkginfo | grep -i ssh
system SUNWsshcu SSH Common, (Usr)
system SUNWsshdr SSH Server, (Root)
system SUNWsshdu SSH Server, (Usr)
system SUNWsshr SSH Client and utilities, (Root)
system SUNWsshu SSH Client and utilities, (Usr)
```

For Sun Netra 240 servers, the following output is expected:

```
# pkginfo | grep -i ssh
application NTSSH Succession Platform OpenSSH Installation
```

If the SSH software has not been installed:

- For Sun Netra 240 platforms with SPFS, contact Nortel support for installation instructions.
- For Sun V480 platforms, add the required Solaris 9 software following the procedures in NN10440-450 Upgrading the Carrier Voice over IP Network.

3 Prepare a backup of the file sshd_config.

For N240 platforms, execute the following command:

```
cp /opt/openssh/etc/sshd_config
/opt/openssh/etc/sshd_config.presecurity
```

For V480 platforms, execute the following command:

```
cp /etc/ssh/sshd_config
/etc/ssh/sshd_config.presecurity
```

This file will be used if SSH must be disabled.

4 Edit the following lines in the sshd_config file by removing any leading "#" characters and setting the parameter values as shown:

```
PrintMotd=no
Banner /etc/issue
X11Forwarding yes
```

```
AllowTcpForwarding yes
PermitRootLogin yes
```

5 Determine if SSH is already active:

For V480 servers, execute the command:

pgrep sshd

If there is no value <*ssh_pid*> output by the command, the SSH daemon is not running. Go to step 7.

For Sun Netra 240 servers with SPFS, execute the command:

ps -eaf | grep sshd

For Sun Netra 240 servers with SPFS, the following output is expected:

```
$ ps -eaf |grep sshd
    root  1611  1045    0   Aug 23  ?       0:07 /opt/openssh/sbin/sshd -D
    root  1045     1    0   Aug 23  ?       0:00 /bin/ksh
/opt/openssh/rcscripts/start_sshd
    root  11238  1611   0  18:48:46  ?      0:01 /opt/openssh/sbin/sshd –D -R
    root  24445  1611   0  18:36:50  ?      0:01 /opt/openssh/sbin/sshd –D -R
    root  24911  1611   0   Sep 02   ?      0:39 /opt/openssh/sbin/sshd -D -R
    root  20097  1611   0  18:54:59  ?       0:01 /opt/openssh/sbin/sshd -D -R
0010002  9145  9105   0  19:51:47 pts/5     0:00 grep sshd
```

In this example, the ID of the process */opt/openssh/sbin/sshd -D* is *1611*.

6 If the SSH daemon is running, stop it:

For V480 servers, execute the command :

kill -1 <ssh-pid>

For Sun Netra 240 servers, execute the command:

kill -HUP <ssh-pid>

An example value of ssh-pid can be seen in the output example in step 5.

7 Start SSH daemon:

/etc/init.d/sshd.sh start

The SSH daemon will use the changes made to the file */etc/ssh/sshd_config* when it starts.

From an X11 desktop enabled with SSH

8 Use the ssh command to login to the MDM Server. Verify that the SSH connection is working by completing the login sequence.

9 Verify that all the X11 desktops can connect to the MDM Server.

10 If problems are encountered with the desktop connections to the MDM Server, verify the changes made to */etc/ssh/sshd_config* and repeat step 6 and step 7 to restart the SSH daemon.

This is the end of the procedure "Installing and activating SSH software on the MDM Server" (page 30).

Variable Value

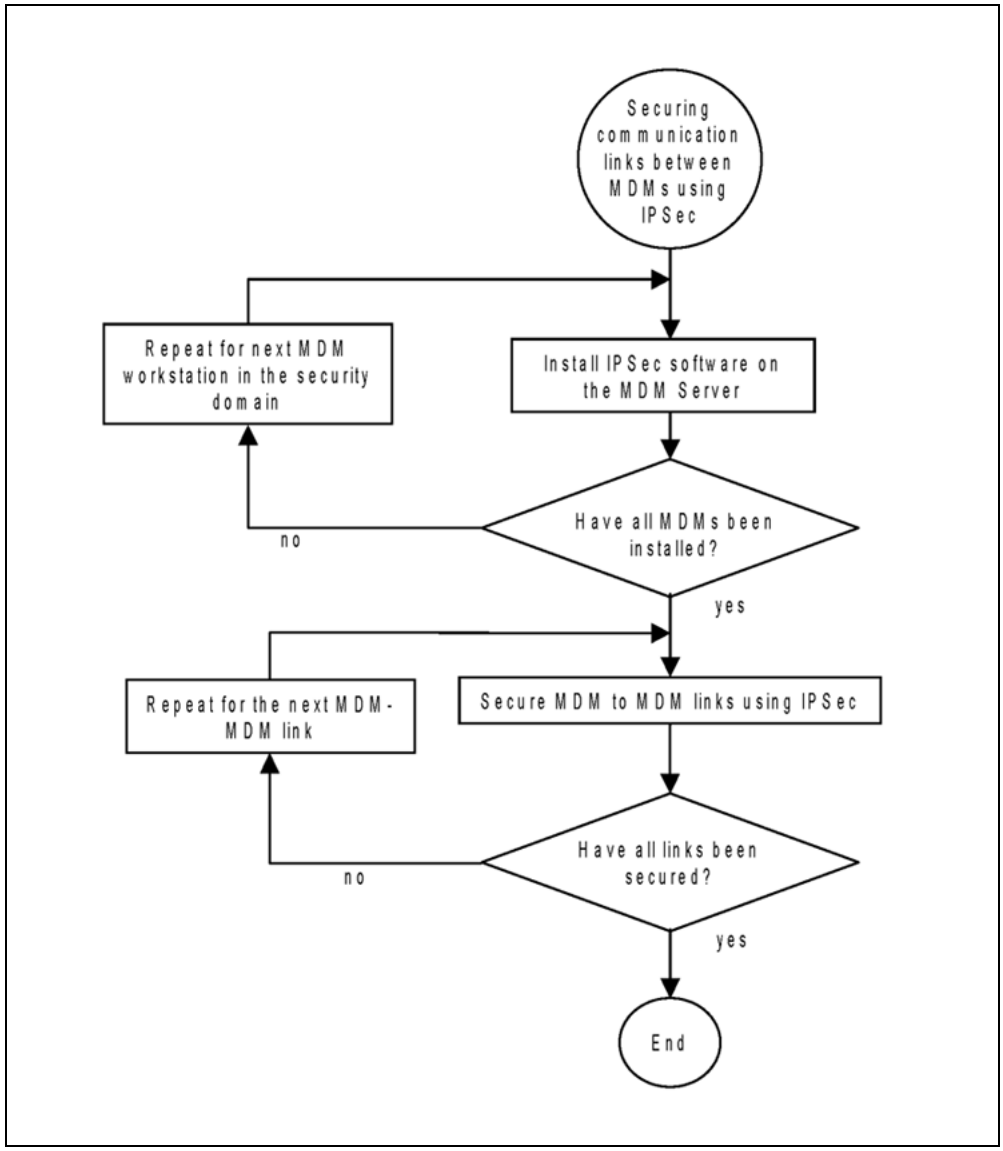
Variable	Value
<ssh_pid>	is the process id returned by the **`pgrep sshd`** command. This id is used in the **`kill`** command to identify the process to be stopped.

—End—

Securing links between MDM Servers using IPSec

The following task flow shows the procedures to use to secure communication links between the MDM servers in the security domain.

Task flow for securing links between MDM Servers using IPSec



Installing IPSec software on the MDM Server

CAUTION
This procedure requires rebooting of the MDM Server.

Prerequisites

Before using this procedure:

- The MDM Server must have an SN08 or later release installed. The Solaris 9 IPSec application software is installed as a part of the upgrade procedure.

  Note: Once IPSec is installed and configured, RADIUS authentication cannot be used. If you wish to use RADIUS authentication to the IEMS, you must configure a RADIUS bypass policy. For more information, refer to "Provisioning a RADIUS bypass policy on MG15000" (page 38)

IPSec installation and configuration

This procedure must be repeated for every MDM Server in the security domain.

Step	Action

Using a secure desktop connection:

1 Log in to the MDM Server as root.

2 Verify that the IPSec software and Sun Solaris 9 Data Encryption Supplement 1.0.1 has been installed by executing the following command:

```
pkginfo | grep -i cry
```

The following output is expected:

```
# pkginfo | grep -i cry
system SUNWcrman Encryption Kit On-Line Manual Pages
system SUNWcry Crypt Utilities
system SUNWcry64 Prototype package for Crypt Library (64-bit)
system SUNWcryr Solaris Root Crypto
system SUNWcryrx Solaris Root Crypto (64-bit)
```

If the IPSec software and Data Encryption Supplement has not been installed:

- For Sun Netra 240 platforms with SPFS, contact Nortel support for installation instructions.
- For Sun V480 platforms, install the required Solaris 9 software using the Solaris 9 CD.

3 Configure the MDM Server to start IPSec automatically:

```
cp /etc/inet/ipsecinit.sample
/etc/inet/ipsecinit.conf
```

4 Reboot the MDM Server:

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

—End—

This is the end of the procedure "Installing IPSec software on the MDM Server" (page 36).

Provisioning a RADIUS bypass policy on MG15000

Prerequisites

Before using this procedure:

- Confirm that IPSec is provisioned

Step	Action

1 Add the policy component under the Spd attribute.

```
add Vr/m Ip Spd/s Policy/i
add Vr/m Ip Spd/s Policy/i+1
```

2 Set the direction attribute under the inbound policy.

```
set Vr/m Ip Spd/s Policy/i direction inbound
set Vr/m Ip Spd/s Policy/i action bypass
set Vr/m Ip Spd/s Policy/i srcIpAddr <radius server ip>
set Vr/m Ip Spd/s Policy/i destIpAddr <MSS OAM ip>
set Vr/m Ip Spd/s Policy/i srcPort 1812
set Vr/m Ip Spd/s Policy/i destPort any
```

3 Set the direction attribute under the outbound policy.

```
set Vr/m Ip Spd/s Policy/i+1 direction outbound
set Vr/m Ip Spd/s Policy/i+1 action bypass
set Vr/m Ip Spd/s Policy/i+1 srcIpAddr <MSS OAM ip>
set Vr/m Ip Spd/s Policy/i+1 destIpAddr <radius server
ip>
set Vr/m Ip Spd/s Policy/i+1 destPort 1812
set Vr/m Ip Spd/s Policy/i+1 srcPort any
```

4 Repeat steps 1-3 for each RADIUS server.

—End—

Variable values

Variable	Value
m	the management Vr instance
s	the Spd instance under the management Vr
i	an available policy instance in the range 0-9999
<MSS OAM ip>	ip address of the OAM enet
<radius server ip>	ip address where the RADIUS server resides. This is typically the IEMS ip address

Securing an MDM to MDM connection with IPSec

Use the following procedure to activate the IPSec protocol to secure the link between two MDM Servers.

Note: If the MDM Server has two IP addresses, then both IP addresses must be secured with IPSec. This procedure shows the steps for a single IP address.

For more information on the operation of IPSec, see *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

Prerequisites

Before using this procedure:

- Obtain the security association information for the link between the MDM Servers from the IPSec configuration record.
- Designate one MDM Server as MDM1 and the other MDM Server as MDM2 to use this procedure.

Secure the MDM to MDM connection

CAUTION
Configure both ends of the link with IPSec as soon as possible.
When IPSec is not active at both ends of the link, the link is not operational and errors will be logged to syslog causing the disk to fill up.

Step Action

Using a secure connection from the desktop

1 Log in to MDM1 as root.

2 Create AES and SHA1security keys:

```
/opt/MagellanNMS/bin/ipsec_keygen -aes
```

```
/opt/MagellanNMS/bin/ipsec_keygen -sha
```

The output of the two commands are the security keys <aes_key> and <sha_key>.

3 Execute the following command script to setup the IPSec security association on MDM1:

```
ipsec_newsa <MDM2_IPaddr> -inSPI <x> -outSPI <y>
-enc_alg aes <aes_key> -enc_auth sha
<sha_key>
```

<aes_key> is the AES encryption key generated in step 2.

<sha_key> is the SHA1 encryption key generated in step 2.

The following sample output displays the last few lines of output for a successful completion of the command.

Sample output for ipsec_newsa command

```
# ipsec_newsa 47.128.153.8 -inSPI 800 -outSPI 801 -enc_auth sha
-enc_alg des 0102030405060708090a0b0c0d0e0f00


peerAddr 47.128.153.8
localAddr 47.135.48.97
inSPI 800
outSPI 801
encrAuth sha -enc_alg
#--------------------Provisioning the Workstation----------------------#
.
.
.
#----------------------Successful Execution--------------------------#
Run the following command on the peer workstation if not already done.
./ipsec_newsa -outSPI 800 -inSPI 801 -enc_auth sha -enc_alg
47.135.48.97 47.128.153.8
```

At this point, the link with MDM2 is not operational.

Use the last line of the output of this command (shown in bold text in the sample) as the command to be executed in step 5.

4 Log in to MDM2 as root.

5 Copy the command output in step 3 to the command line on MDM2 and execute it to setup the IPSec security association on MDM2.

At this point, both ends of the link have IPSec activated.

6 Verify that the secured link is operating correctly by connecting from MDM2 to MDM1.

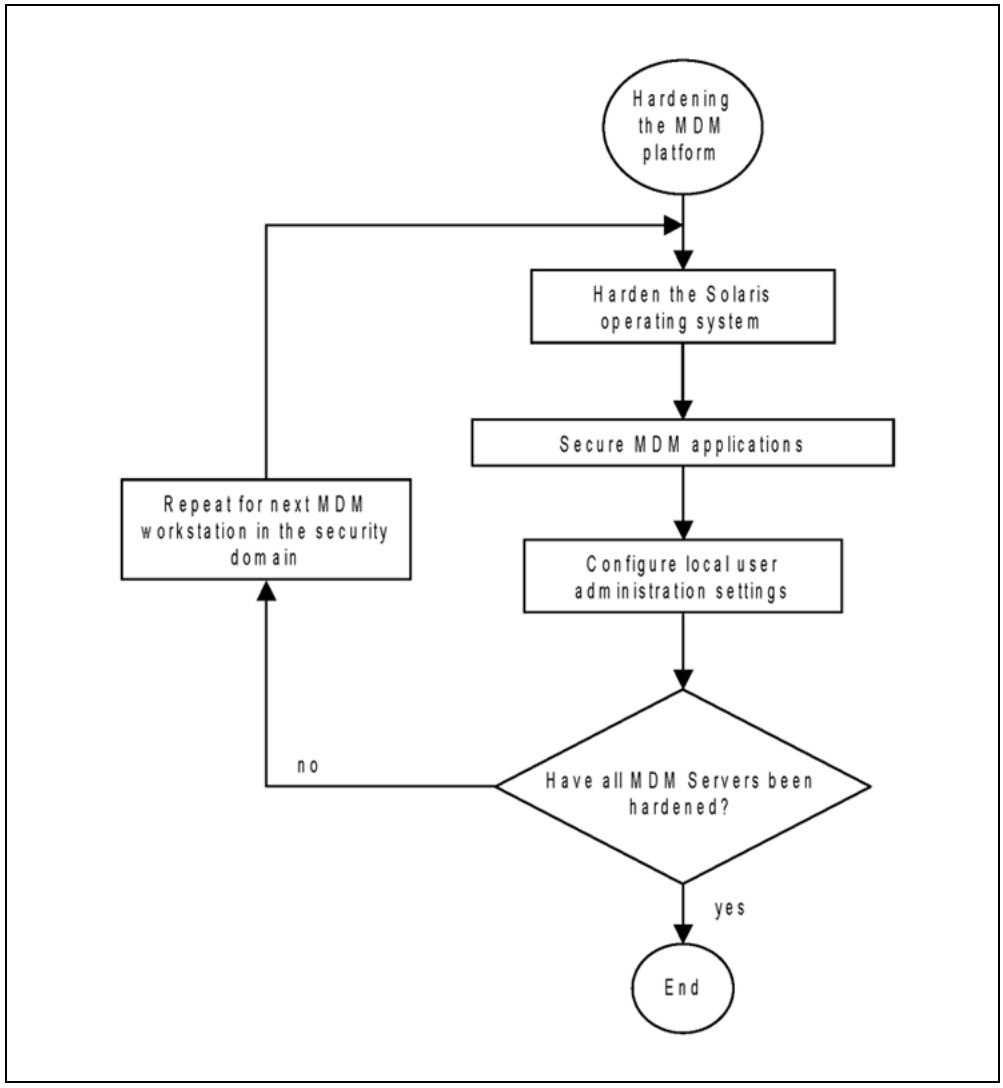
—End—

This is the end of the procedure "Securing an MDM to MDM connection with IPSec" (page 39).

Hardening the Multiservice Data Manager Server platform

The following task flow shows the procedures to follow to harden the MDM Server platform.

Task flow for hardening the MDM Server platform



The procedures must be repeated for each MDM Server in the security domain.

Hardening the Solaris operating system

ATTENTION

IEMS must be able to connect to the MDM Server using SSH before the MDM Server platform is hardened and telnet access is restricted.

Hardening the Solaris operating system involves:

- removing unused functions from the Solaris operating system and restricting access to other functions

- setting up support for central user authentication and authorization using IEMS
- restricting access to MDM Server IP ports and inetd services such as sshd and telnet

Prerequisites

Before performing this procedure:

- SSH must be installed and operational.
- Connect to the MDM Server using the SUN operator port.

Harden the Solaris operating system

The hardening script for the Solaris operating system used in this procedure is provided as part of the MDM Server installation. Additional changes are recommended for VoIP solutions.

Note: Running the MDM script to harden the Solaris operating system will result in a reboot of the MDM Server.

ATTENTION

The MDM script for hardening the Solaris 0S is not executed on MDM deployed on N240 servers with SPFS. For MDM servers deployed on N240 with SPFS, begin this procedure at step 15.

The MDM hardening script must be performed on the V480 platform.

Step	Action

Using the Sun operator port on the MDM Server:

1 Log in to the MDM Server as root.

2 Restart the system in single user mode:

```
sync; sync; sync; init s
```

Enter the root password when prompted.

3 Issue the following command to execute the MDM script for hardening the Solaris operating system:

```
/opt/MagellanNMS/bin/Solaris_OsHarden
```

Follow the instructions presented during the execution of the script. Refer to the section "Hardening the Solaris operating system" in *241-6001-303 Nortel Multiservice Data Manager Administration* for the responses required by the script. The MDM Server will restart in multiuser mode.

Using the Sun operator port on the MDM Server or a secure connection from the desktop

4 Log in to the MDM Server as root and continue with the following steps.

5 Execute the following command to allow only the root userid to execute the **traceroute** command:

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

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

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

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

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

8 To enable IEMS userids to access MDM functionality, link the IEMS default home directory name to the MDM default home directory:

```
ln -s /localdisk /export/home
```

9 For Sun Fire V480 platforms, set up the shell directories for IEMS support:

```
ln -s /usr/bin/sh /usr/bin/rash
ln -s /usr/bin/false /usr/bin/nash
```

10 Using the editor, restrict the range of dynamically allocated IP ports:

```
vi
/opt/MagellanNMS/cfg/private/IPCPortRange.cfg
```

Set the following range of values in this file:

```
11200 11700
```

Save and close the file.

11 Using the editor, link the MDM servers to specific ports:

```
vi /opt/MagellanNMS/cfg/private/IPCNameMap.cfg
```

Set the following values in this file:

```
NMAGENT 3456
RTACAGENT 3457
GMDRAGENT 3458
CCAGENT 3459
PSVAGENT 3460
NSVAGENT 3461
PMAGENT 3462
CONFIGMAN 3463
TOMCAT 8006
APACHE 8090
```

Save and close the file.

12 Turn on the TCP wrappers which restrict access to MDM inetd services (such as SSHd and Telnet) by IP addresses:

vi /etc/default/inetd

In this file, remove the '#' character from the front of the line and modify the line as shown:

```
ENABLE_TCPWRAPPERS=YES
```

Save and close the file.

Execute the following commands to restart the **inetd** process:

pgrep inetd

kill -1 <inetd_pid>

The output of the pgrep command is used as the <inetd_pid> parameter in the **kill** command.

13 Configure the IP addresses for the remote systems that are allowed access to the MDM Server.

The */etc/hosts.allow* file contains the IP addresses for the systems that are allowed access to the MDM and is searched first.

The */etc/hosts.deny* file contains the IP addresses of the systems that are denied access to the MDM and is searched last. If a system's IP address is contained in neither file, then by default it is allowed access to the MDM.

a. Using the editor, edit the */etc/hosts.allow* file:

vi /etc/hosts.allow

to contain the following lines:

```
sshd:  LOCAL <IP_network_addr>/<mask>|<IP_address
1>...<IP_addressN>
in.ftpd:  <MSSMG1_IPaddr> ...  <MSSMGn_IPaddr>
<MDM1_IPaddr> <MDM2_IPaddr> <IEMS_IPaddr>
```

Save and close the file.

Note: Each MG15000 switch, MSS15000 switch, MDM Server including the local MDM server and IEMS should be listed in the "in.ftpd" line.

b. Using the editor, edit the */etc/hosts.deny* file:

`vi /etc/hosts.deny`

to contain the following line:

```
ALL: ALL
```

Save and close the file.

14 Turn off telnet access:

`vi /etc/inetd.conf`

Place a "#" character at the beginning of the line starting with "telnet" to comment out the line. Note that this line of text appears as a single line in the file.

```
#telnet stream tcp6 nowait root
/usr/sbin/in.telnetd in.telnetd
```

Save and close the file.

Execute the following commands to restart the *inetd* process:

`pgrep inetd`

`kill -1 <inetd pid>`

The output of the pgrep command is used as the <inetd_pid> parameter in the **`kill`** command.

Note: This step can be deferred until the IEMS has been configured to access an SN09 MDM Server.

This is the end of the procedure.

Using the Sun operator port on the MDM Server or a secure connection from the desktop (for MDM servers deployed on N240 with SPFS only)

15 Log in to the MDM Server as root and continue with the following steps

16 Using the editor, restrict the range of dynamically allocated IP ports:

`vi /opt/MagellanNMS/cfg/private/IPCPortRange.cfg`

17 Set the range of values in this file as follows:

`11200 11700`

18 Save and close the file

19 Using the editor, link the MDM servers to specific ports:

```
vi /opt/MagellanNMS/cfg/private/IPCNameMap.cfg
```

20 Set the following values in this file:

```
NMAGENT 3456
RTACAGENT 3457
GMDRAGENT 3458
CCAGENT 3459
PSVAGENT 3460
NSVAGENT 3461
PMAGENT 3462
CONFIGMAN 3463
TOMCAT 8006
APACHE8090
```

21 Save and close the file.

—End—

This is the end of the procedure."Harden the Solaris operating system" (page 45).

Variable values

Variable	Value
<mdpgroup>	is the name assigned to the MDP group.
<inetd_pid>	is the process id returned by the **pgrep** command. This id is used in the **kill** command to identify the process to be stopped.
<network>/<netmask>	is the network identifier and netmask for the host.
MSSMG[1-n]_IPaddr	is the IP address of an MSS15000 or MG15000 switch.
MDM[1,2]_IPaddr	is the IP address of an MDM Servers.
IEMS_IPaddr	is the IP address of the IEMS.

Securing MDM administration applications

There are a number of MDM security features that ensure administration tools can only be accessed by privileged operators.

Note: The following security features should have been applied as part of the normal MDM installation procedures. If they were not applied during installation, apply them now.

It is recommended that the following MDM tools are password protected to ensure that only authenticated and authorized users may use them:

- Network Model Edit server
- Server Administration (SVM) tool
- GMDR Administration
- Service selection tool

A number of servers may have their associated passwords stored in encrypted format so that they are not visible during the log in process. It is recommended that the following servers are protected with password encryption:

- FMDR server
- PMSP server
- Backup and restore server
- SALC configuration file

For more information on setting passwords for these tools, see *241-6001-310 Nortel Multiservice Data Manager Server Reference*.

Configuring local user administration settings

The following settings apply to userids configured locally on the MDM Server:

- "MDM password length and password aging" (page 50)
- "Login retries for local MDM userids" (page 51)
- "Login messages" (page 52)

For more information about these functions, see *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*.

MDM password length and password aging

The password length for local userids in between six and eight characters. The longer the password length, the less likely that it can be deciphered.

A minimum and a maximum time period can be set before the password for a locally configured userid expires. A warning message can be sent prior to password expiry.

Step	Action

Using a secure connection from the desktop

1 Log in to the MDM Server as root.

2 Edit the file /etc/default/passwd:

```
vi /etc/default/passwd
```

3 Set the password length variable as follows:

```
passlength=8
```

> ***Note:*** If you use a number greater than eight, only the first eight characters will be used in the password comparison.

4 Set the minimum and maximum number of weeks before the password for a locally defined userid expires as follows:

```
maxweeks=12
minweeks=2
```

These parameters are customer defined. The values shown are the recommended values.

5 Save and close the */etc/default/passwd* file.

> **ATTENTION**
> If the MDM Solaris 0S hardening script has been executed to harden the MDM, the Solaris Management Console (SMC) will not be running. Use the Sun Admintool.

6 Use the Solaris Management Console (smc) to enable the warning message for passwords approaching expiry:

```
smc &
```

In the GUI window, select Users from the Browse menu, select the userid to change, and then select Modify from the Edit menu to bring up the Edit screen. Set the warning value. Repeat for every local userid for which you want to have the warning issued.

—End—

This is the end of the procedure "MDM password length and password aging" (page 50).

Login retries for local MDM userids

After the specified number of attempts to login, the userid is locked out.

Step	Action

Using a secure connection from the desktop

1 Log in to the MDM Server as root.

2 Edit the file */etc/default/login*:

```
vi /etc/default/login
```

3 Set the retry variable as follows. The current default is 3.

```
retries=3
```

This parameter is customer defined. The value shown is the recommended value.

4 Set the log variable as follows:

```
SYSLOG_FAILED_LOGINS=0
```

5 Save and close the file.

—End—

This is the end of the procedure "Login retries for local MDM userids" (page 51).

Login messages

Provide warning banners to inform the users that they are accessing a restricted system.

Step	Action

Using a secure connection from the desktop

1 Log in to the MDM as root.

2 Create a message of the day. Edit the file */etc/motd*:

```
vi /etc/motd
```

and type in the message. Save and close the file.

This message is shown as part of the login sequence for a local userid.

3 Set the banner for FTP sessions. Edit the file */etc/default/ftpd*:

```
vi /etc/default/ftpd
```

At the line starting with the word Banner, enter the desired text inside double quotes. Input is restricted to eighty characters of text.

Save and close the file.

A sample banner could be "Unauthorized access prohibited."

4 Create a pre-login message that is displayed prior to login. Edit the file */etc/issue*:

```
vi /etc/issue
```

At the line starting with the word Banner, enter the desired text inside double quotes.

Save and close the file.

A sample banner could be "Use is restricted to authorized users. Usage is monitored; unauthorized users will be prosecuted."

5 Set the banner for telnet sessions. Edit the file */etc/default/telnetd*:

```
vi /etc/default/telnetd
```

Edit the line starting with the word Banner as follows:

```
Banner = /etc/issue
```

Save and close the file.

—End—

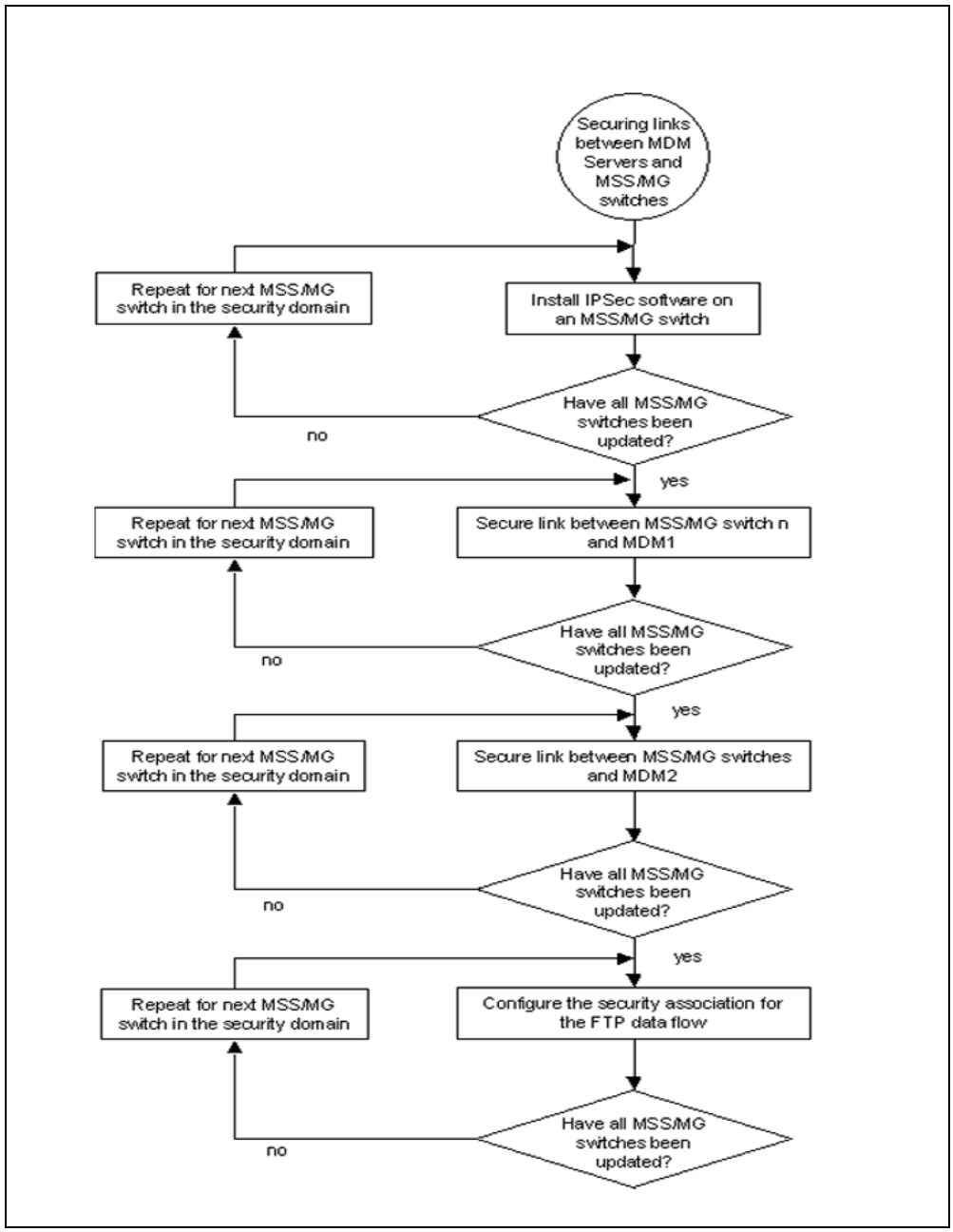
This is the end of the procedure "Login messages" (page 52).

This is the end of the procedures for "Configuring local user administration settings" (page 50).

Securing links between MDM Servers and MSS/MG15000 switches using IPSec

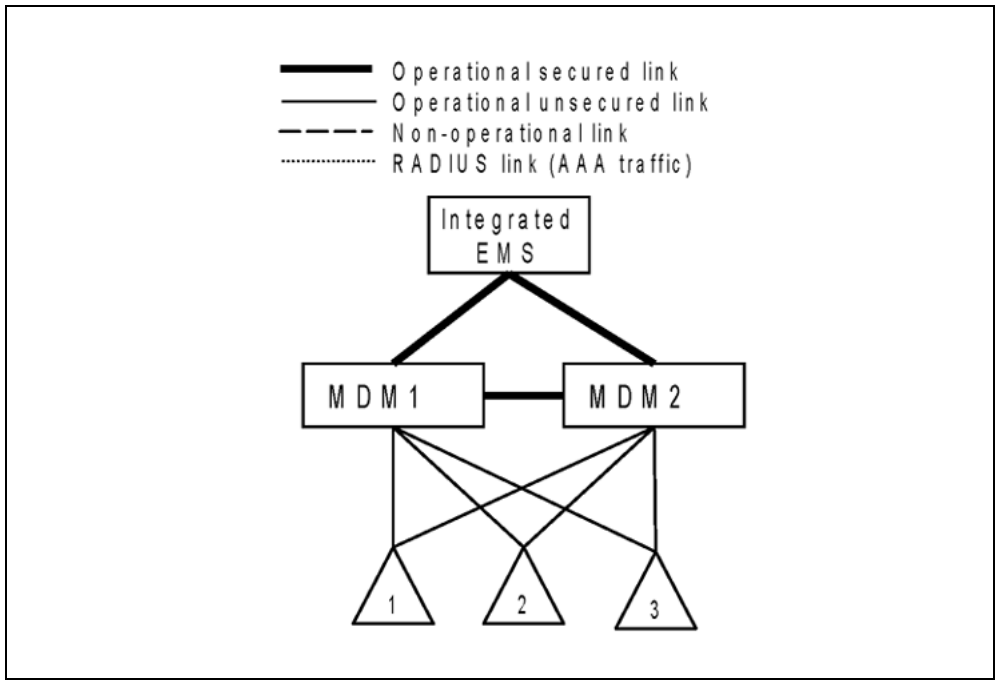
The following task flow shows the procedures to secure communication links between MDM Servers and MSS/MG15000 switches.

Task flow for securing links between MDM Servers and MSS/MG15000 switches using IPSec



The following reference figure will be used to show the progression of securing the links. As a link is secured, it will be shown as bold.

Reference figure for securing links between MDM Servers and MSS/MG15000 switches using IPSec



Prerequisites

Before using the procedures in this section:

- Designate one MDM Server as MDM1 and the other MDM Server as MDM2 according to the planned order for securing the links.
- Designate the MSS/MG15000 switches as MSSMG, MSSMG2,... MSSMGn according to the planned order of securing the links.

Installing IPSec software on an MSS/MG15000 switch

Repeat this procedure for every MSS/MG15000 switch in the security domain.

Prerequisites

Before using this procedure:

- Verify that the IPSec software package for the MSS/MG15000 switch is available on the software distribution site (SDS). For more information on the IPSec software file to be downloaded, refer to the release notes.

Install IPSec software on the MSS/MG15000

CAUTION
Activating IPSec on the MSS/MG15000 switch disrupts the flow of OAM traffic.
Once IPSec is active on the switch, all OAM traffic is disrupted until security policies and security associations have been provisioned. Provision the security policies and associations as quickly as possible.

Step	Action
1	Log in to the MSS/MG15000 as system administrator.
2	Download the IPSec software package from the SDS site following your standard procedures.

CAUTION
Activating a provisioning view can affect service.
Activating a provisioning view can result in a CP reload or restart, causing all services on the Multiservice Switch 15000 node to fail. See *NN10600-050 Nortel Multiservice Switch 7400/15000/20000 Command Reference* for more information.

3 In provisioning mode, add the IPSec software to the MSS/MG15000 software AVL and feature list:

```
start prov
copy prov
set Software avList !  <ipsec_xxxx>
set software Lpt/Cp featurelist ipsec
check prov
save -f(<IPSecInstallViewName>) -portable prov
activate prov
confirm prov
commit prov
```

For more information on provisioning mode, refer to *NN10600-710 Nortel Multiservice Switch 7400/15000/20000 ATM Configuration Management*.

—End—

This is the end of the procedure "Install IPSec software on the MSS/MG15000" (page 58).

Variable values

Variable	Value
<ipsec_xxxx>	is the name of the IPSec software module. xxxx specifies the version of the software and can be obtained from the release notes.
<IPSecInstallViewName>	is the name of the file to contain the saved provisioning view with IPSec installed.

Securing links between MDM1 and MSS/MG15000 network elements

The OAM IP links between the MSS/MG15000 switches and MDM1 are secured first.

Prerequisites

Before using these procedures:

- IPSec software must be installed on MDM1 and the MSS/MG15000 switches.
- The ipsec feature must be configured in the software AVL.
- To ensure absolute protection, the MSS/MG15000 IPSec policy database (SPD) must be initialized by connecting directly to the serial port on the MSS/MG15000 using a Vt100 terminal so that the encryption keys cannot be monitored.
- To simplify the key distribution to multiple sites, the same security keys are used to set the security associations on all the MDMs and all the MSS/MG15000 switches in the security domain to simplify the key distribution. Once all links are secured, security keys can be updated and distributed over the links. For more information on key management, refer to *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*.
- Obtain the security association information for links between MDM1 and the MSS/MG15000 switches from the IPSec configuration record.
- Designate each MSS/MG15000 switch in the security domain as MSSMG1, MSSMG2, ..., MSSMGn according to the order that the links will be secured.
- For the procedures in this section, the following convention will be used for the MSS/MG15000 switches in the security domain:
  - <yn>: *inSPI* for the SA on MDM1 to MSSMGn
    outSPI for the SA on MSSMGn to MDM1
  - <xn>: *outSPI* for the SA on MDM1 to MSSMGn

inSPI for the SA on MSSMGn to MDM1

Configure security associations on the MDM1 for the MSS/MG15000 switches

CAUTION
Configure both ends of a link with IPSec as soon as possible.
When IPSec is not active on both ends of the link, the link is not operational.

Step	Action

Using a secure connection from the desktop

1 Login in to MDM1 as root.

2 Create AES and SHA1 security keys for use in securing links with the MSS/MG15000 switches:

```
ipsec_keygen -aes
```

```
ipsec_keygen -sha
```

The output of the two commands are the values <aes_key> and <sha_key>.

Note: Retain these keys as they will be used to activate the IPSec connections on all the MSS/MG15000 switches. Once activation of IPSec is complete for the security domain, you can centrally administer different IPSec security keys using an MDM Server.

3 Repeat the following command for each MSS/MG15000 in the security domain. Substitute the appropriate IP address, inSPI and outSPI values for MSS/MG15000 switch n:

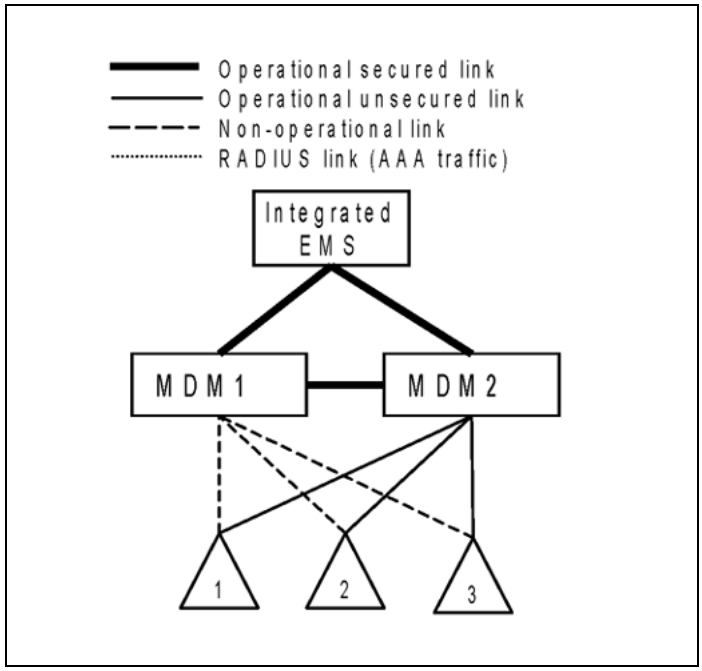
```
ipsec_newsa <MSSMGn_IPAddr> -inSPI <yn> -outSPI <xn>
-enc_alg aes <aes_key> -enc_auth sha <sha_key>
```

Note: Ignore the instruction output at the end of this script as it does not apply for links between MDM Servers and MSS/MG15000 switches.

Upon completion of the command, the link between MDM1 and MSS/MG15000 <n> is not operational as IPSec has been activated for only one end of the link.

—End—

At this point, the links between all the MSS/MG15000 switches and MDM1 are not operational. All MSS/MG15000 management data and commands must flow through MDM2. See the following reference figure.



This is the end of the procedure "Configure security associations on the MDM1 for the MSS/MG15000 switches" (page 60).

Variable values

Variable	Value
<MSSMGn_IPaddr>	is the IP address of MSS/MG15000 switch <n>. Switches in the security domain are designated 1 to n.
<aes_key>	is the data encryption key used for initial securing of all links between MSS/MG15000 switches and MDM Servers.
<sha_key>	is the data authentication key used for initial securing of all links between MSS/MG15000 switches and MDM Servers.
<yn>	is the MDM1 *inSPI* value for the association to MSS/MG15000 switch <n>.
<xn>	is the MDM1 *outSPI* value for the association to MSS/MG15000 switch <n>.

Configure security associations on the MSS/MG15000 switch for MDM1

The security policy data base and initial security associations on the MSS/MG15000 node must be set up manually. For more information about manually configuring IPSec on MSS/MG15000 switches, see *NN10600-601 Multiservice Switch Security Management*.

Repeat this procedure for each MSS/MG15000 switch in the security domain.

Prerequisites

Before you use this procedure:

- Ensure the MDM side of the link has already been configured with IPSec
- Connect a VT100 to the local port of the MSS/MG15000 switch
- Obtain the AES and SHA1 security keys used to configure the security association on MDM1. If the MSS/MG15000 switch is at a different site than MDM1, use a secure method of communicating the keys.
- If the MSS/MG15000 switch is at a different site than MDM1, provide a method of communicating between the MDM operator and the operator at the MSS/MG15000 site to coordinate testing of the secured links.
- Know the management Vr on the MSS/MG15000 switch
- Obtain the security association data for links between MDM1 and the MSS/MG15000 switches from the IPSec configuration record.

Step	Action

Using a VT100 terminal connected to the local port on the MSS/MG15000 switch

1 Log in to the MSS/MG15000 as system administrator.

2 Create the IPSec policy database for the management Vr:

```
add Vr/<z> Ip Spd/1
```

3 Create the policy for inbound traffic coming to the node from MDM1:

```
add Vr/<z> Ip Spd/1 Policy/30010
```

4 Create the policy for outbound traffic going from the node to MDM1:

```
add Vr/<z> Ip Spd/1 Policy/30020
```

5 Specify the action and direction for the inbound traffic policy:

```
set Vr/<z> Ip Spd/1 Policy/30010 action apply,
direction in
```

6 Specify the action and direction for the outbound traffic policy:

```
set Vr/<z> Ip Spd/1 Policy/30020 action apply,
direction out
```

7 Specify the selector attributes for the inbound traffic policy:

```
set Vr/<z> Ip Spd/1 Policy/30010 srcIpAddr <MDM1_IPaddr
>, dstIpAddr <MSSMGn_IPaddr>
```

8 Specify the selector attributes for the outbound traffic policy:

```
set Vr/<z> Ip Spd/1 Policy/30020 srcIpAddr <MSSMGn_IPad
dr>, dstIpAddr <MDM1_IPaddr>
```

9 Add the initial security association for inbound traffic from MDM1:

```
add Vr/<z> Ip Spd/1 Policy/30010
Sa/<MSSMGn_IPaddr>,esp,<xn>
```

10 Add the initial security association for outbound traffic to MDM1:

```
add Vr/<z> Ip Spd/1 Policy/30020
Sa/<MDM1_IPaddr,esp,<yn>
```

11 Set the encryption algorithms and security keys for the inbound security association:

```
set Vr/<z> Ip Spd/1 Policy/30010
Sa/<MSSMGn_IPaddr>,esp,<xn> ManEspSa authAlg sha,
authKey <sha_key>, encAlg aes, encKey <aes_key>
```

Note: <aes_key> and <sha_key> are the security keys generated when configuring the SAs on MDM1.

12 Set the encryption algorithms and security keys for the outbound security association:

```
set Vr/<z> Ip Spd/1 Policy/30020
Sa/<MDM1_IPaddr>,esp,<yn> ManEspSa authAlg sha, authKey
<sha_key>, encAlg aes, encKey <aes_key>
```

Note: <aes_key> and <sha_key> are the security keys generated when configuring the SAs on MDM1.

13 Verify that the changes are acceptable:

```
check prov
```

14 Save the provisioning information to file:

```
save -f(<initialIPSecViewName>) -Portable prov
```

15 Activate the new view:

```
activate prov
```

Note: Once the new provisioning view has been activated, only the links configured with IPSec security associations will be operational.

16 Confirm the changes so that the system will not roll back:

```
confirm prov
```

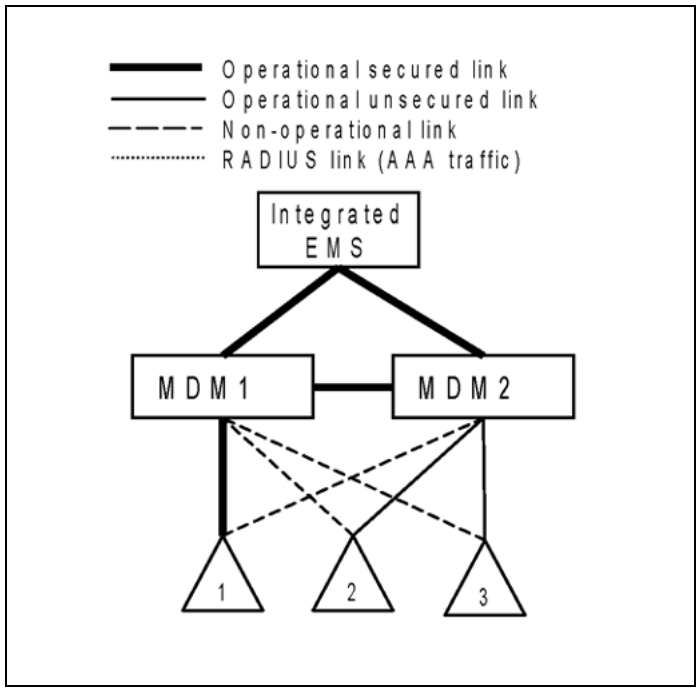
17 Test the secured link between MSSMGn and MDM1 by using the telnet command on MDM1 to access the switch.

18 Commit the changes to be the default view:

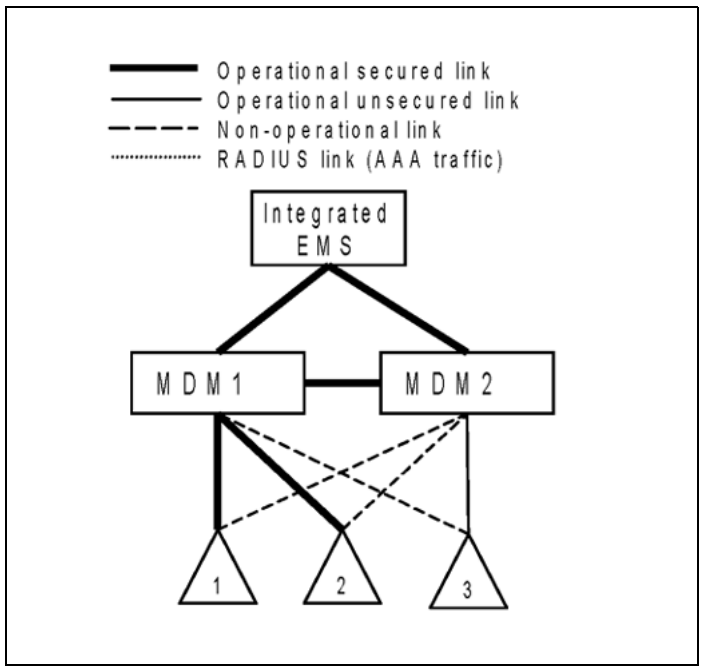
```
commit prov
```

—End—

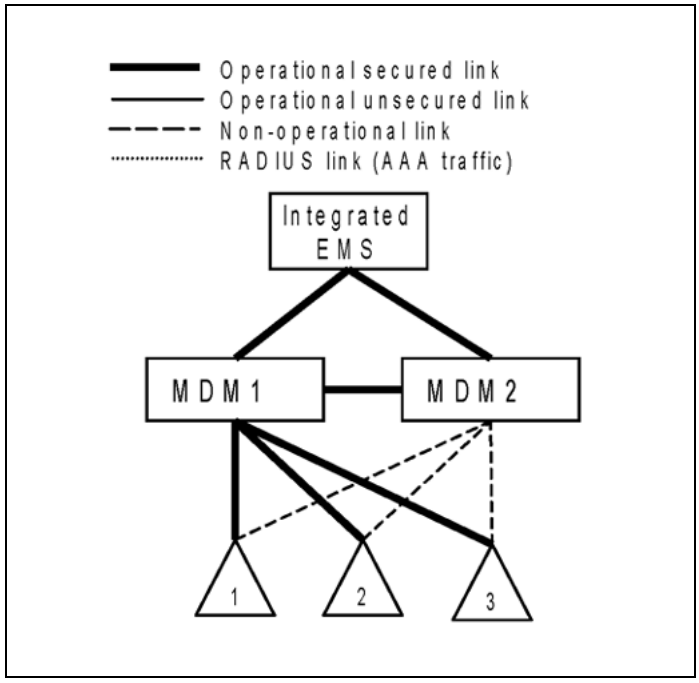
The following figure shows the state of the network after the link between MDM1 and MSSMG1 has been secured.



The following figure shows the state of the network after the link between MDM1 and MSSMG2 has been secured.



The following figure shows the state of the network after the link between MDM1 and MSSMG3 has been secured.



This is the end of the procedure "Configure security associations on the MSS/MG15000 switch for MDM1" (page 61).

This is the end of the procedures for "Securing links between MDM1 and MSS/MG15000 network elements" (page 59).

Variable values

Variable	Value
<MSSMGn_IPaddr>	is the IP address of MSS/MG15000 switch <n>. Switches in the security domain are designated 1 to n.
<aes_key>	is the data encryption key used for initial securing of all links between MSS/MG15000 switches and MDM Servers.
<sha_key>	is the data authentication key used for initial securing of all links between MSS/MG15000 switches and MDM Servers.
<xn>	is the MSSMGn *inSPI* value for the association to MDM1.
<yn>	is the MSSMGn *outSPI* value for the association to MDM1.
<MDM1_IPaddr>	is the IP address of MDM1.
<initialIPSecViewName>	is the name of file containing the provisioning view with the initial IPSec configuration.
<z>	is the management Vr identifier.

Securing links between MSS/MG15000 switches and MDM2 for all channels

Once a secure connection is operational between MDM1 and an MSS/MG15000 switch, all the IPSec configuration for links between MDM2 and the MSS/MG15000 switch can be done from MDM2. The pp_ipsecsetup command script operates using a secure path through MDM1 to the switch.

The pp_ipsecsetup command script automatically defines the security associations and SPIs, and generates security keys for the data flows on the link as follows:

- The FTP data channel is secured with data authentication.
- The RADIUS channel used by central AAA uses the IPSec bypass option since the RADIUS protocol already incorporates security measures.
- All other channels are secured with data encryption.

Prerequisites

Before using this procedure:

- Obtain the group, userid and password for system administration access for each MSS/MG15000 switch
- Obtain the IPSec configuration record ready for updating the security association information for the link between MDM2 and the MSS/MG15000 switches.
- Obtain the IP address of the IEMS.

Configure the security associations on the MSS/MG15000 switch and MDM2

Step	Action

Using a secure desktop connection to MDM2

1 Log in to MDM2 as root.

2 Set up the security associations for the link between MDM2 and the MSS/MG15000 switch, using the secure link through MDM1 to access the MSS/MG15000 switch:

```
pp_ipsecsetup <MSSMGn_IPddr> -Rad1
<IEMS_IPaddr> -pp <MDM1_IPaddr> <MSSMGn_group>
<MSSMGn_userid> <MSSMGn_pwd>
```

3 Test the secured connection between MDM2 and the switch by using the **ping** command.

```
ping <MSSMGn_IPaddr>
```

4 Repeat step 2 and step 3 for all MSS/MG15000 switches connecting to MDM2.

5 Display the IPSec configuration information on MDM2 to show the *inSPI* and *outSPI* values assigned by the pp_ipsecsetup command.

```
ipseckey dump
```

The following figure shows a sample command output for one security association.

Sample output for ipseckey command

```
ipseckey dump
>>Base message (version 2) type DUMP, SA type ESP.
>>Message length 144 bytes, seq-1, pid-19315.
>>SA: SADB_ASSOC spi=0x1f8, replay=0, state=MATURE.
>>SA: Encryption algorithm = 3DES-CBC
>>SA: flags=0x0 < >
>>SRC: Source address (proto=0/<unspecified>)
>>SRC: AF_INET: port = 0, 47.138.183.45 (wcary0km.c
a.nortel.com).
>>DST: Destination address (proto=0/<unspecified>)
>>DST: AF_INET: port = 0 47.135.211.28 (zcars0ws).
>>EKY: Encryption key.
>>EKY: 3bef5d16df7aa1347361f12a2545d68a91fdcb13c64
5e1a/192
>> LT: Lifetime information
>>CLT: 0 bytes protected, 0 allocations used.
>>CLT: SA added at time Thu Jul 08 13:44:33 2004
```

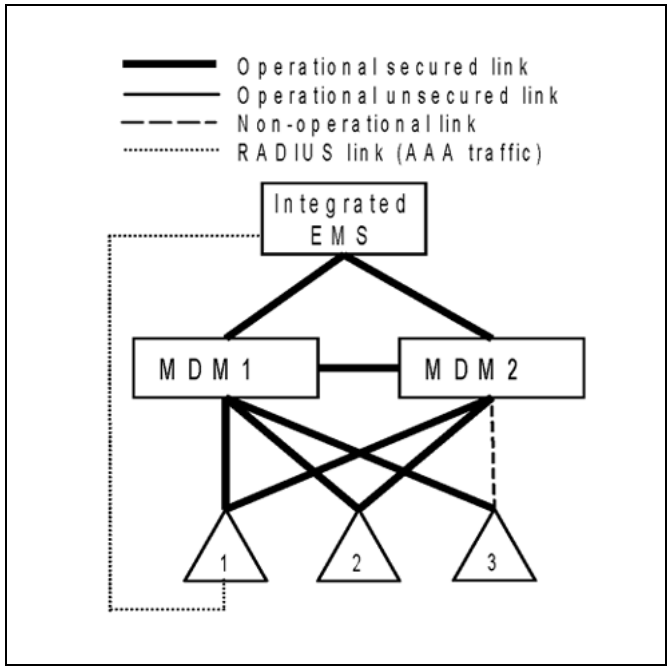
```
>>CLT: Time now is Thu Jul 08 14:43:55 2004
```

Note: The security association index (SPI) is shown as bold, underlined text in the sample output. This value is in hexadecimal format, and must be converted to decimal for use in other commands.

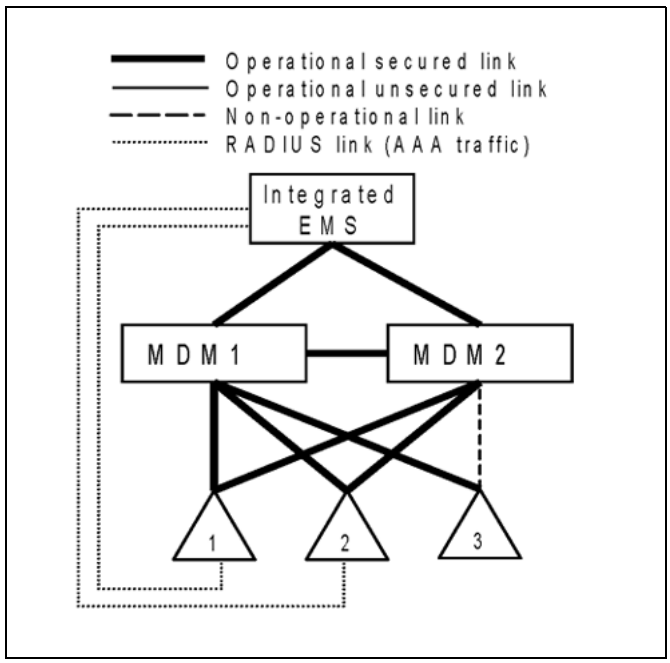
6 Record the *inSPI* and *outSPI* for each link between MDM2 and the MSS/MG15000 switches in the IPSec configuration record.

—End—

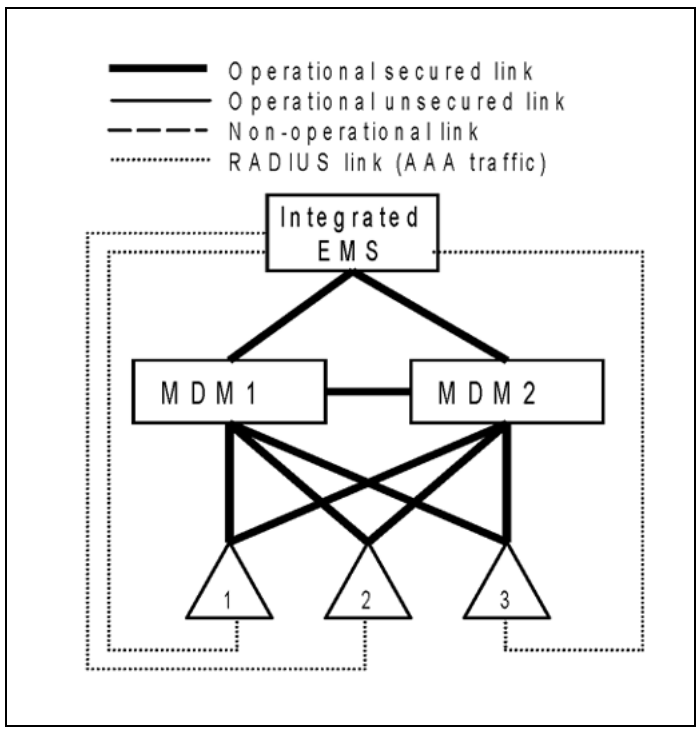
The following figure shows the state of the network after the link between MDM2 and MSSMG1 has been secured.



The following figure shows the state of the network after the link between MDM2 and MSSMG2 has been secured.



The following figure shows the state of the network after the link between MDM2 and MSSMG3 has been secured.



This is the end of the procedure for "Securing links between MSS/MG15000 switches and MDM2 for all channels" (page 66).

Variable values

Variable	Value
<MSSMG_IPaddr>	is the IP address of the MSS/MG15000 switch at the end of the link being secured.
<IEMS_Radius_IPaddr>	is the IP address of the IEMS that will providing centralized user authentication and authorization to the MSS/MG15000 switch.
<MDM1_IPaddr>	is the IP address of the MDM Server that has secured links to the MSS/MG15000 switch.
<MSSMG_group>	is the MSS/MG15000 group identifier.
<MSSMG_userid>	is the MSS/MG15000 userid with system administration impact.

Securing the FTP data channel between MDM1 and MSS/MG15000 switches

Once all the links between the MSS/MG15000 switches and MDM2 have been secured, the IPSec configuration for the FTP data channel between MDM1 and the MSS/MG15000 switches must be completed. Since none of the data in the FTP data channel is sensitive, and encrypting and decrypting the volume of data in the flow can have performance impacts, only IPSec data authentication using the AH protocol is applied.

Prerequisites

Before using the following procedure:

- Obtain a group, userid and password that provides system administrator access for each MSS/MG15000 switch.
- Obtain the security association data for links between MDM1 and the MSS/MG15000 switches from the IPSec configuration record.

  Note: Ensure that the SPIs assigned for these security associations are unique on both MDM1 and the MSS/MG15000 switch. Review the IPSec configuration record after it has been updated with the SPIs generated when the link between MDM2 and the MSS/MG15000 is secured.

Configure the security associations for the FTP data channel

Step	Action
	Using a secure connection from the desktop to MDM1
1	Log in to MDM1 as root.
2	Generate a data authentication security key using MD5:

```
/opt/MagellanNMS/bin/ipsec_keygen -md5
```

The output of the command is a value <md5_key> that is used to activate the AH protocol on the connection.

3 Configure the security association to authenticate the FTP data channel between MDM1 and the MSS/MG15000 switch:

```
ipsec_newsa <MSSMGn_IPaddr> -inSPI <yn> -outSPI
<xn> -destPort ftp-data -enc_auth md5 <md5_key>
-pp <MDM2_IPaddr> <MSSMGn_group> <MSSMGn_userid>
<MSSMGn_pwd>
```

4 To test the link between MDM1 and the MSS/MG15000 switch, wait for the next scheduled MDP activity and monitor that data is transferring properly.

5 Repeat step 3 and step 4 for each MSS/MG15000 switch in the security domain.

—End—

This is the end of the procedure for "Securing the FTP data channel between MDM1 and MSS/MG15000 switches" (page 70).

Variable values

Variable	Value
<MSSMG_IPaddr>	is the IP address of the MSS/MG15000 switch at the end of the link being secured.
<yn>	is the *outSPI* on MDM1 for the FTP data channel security association with MSSMGn.
<xn>	is the *inSPI* on MDM1 for the FTP data channel security association with MSSMGn.
<md5_key>	is the MD5 security key.
<MDM2_IPaddr>	is the IP address of MDM2.
<MSSMG_group>	is the MSS/MG15000 user group.
<MSSMG_ userid>	is the MSS/MG15000 userid with impact of system administration.
<MSSMG_pwd>	is the MSS/MG15000 password.

Sending security audit logs from an MDM Server to IEMS

VoIP solutions, all security audit logs from the MDM Servers and the MSS/MG15000 switches are sent to the IEMS.

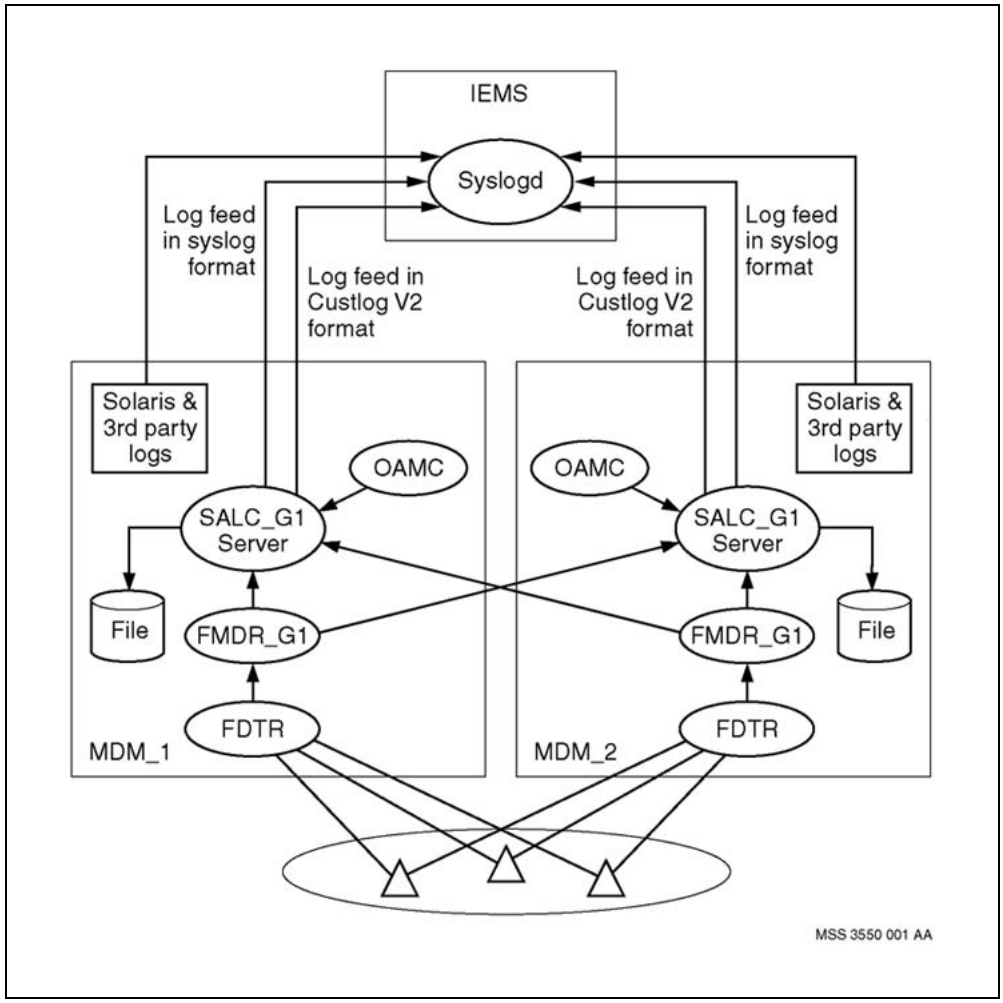
A security log is the complete set of events used to track activities impacting the security of the network. Some alarm events are duplicated in to the security log stream if they are classified as directly impacting security. Specifically, this includes alarm logs where alarm type is "security" or "operator".

An audit log refers to an event that tracks user activity including logins/logouts, commands executed, and/or GUI-initiated actions. Audit logs are considered to be a subset of security logs.

The SALC server on an MDM Server acts as the central collector for MDM application security events (received from the OAMC server) and MSS/MG15000 switch security events (received through the FMDR servers). The SALC server is configured to send the MDM and MSS/MG15000 security logs in Custlog V2 format, syslog format, or both formats to the syslog daemon on the IEMS. These logs are also stored on the MDM Server. Solaris UNIX operating system events are also sent to the syslog daemon on IEMS.

The following figure shows the security audit log logical flow.

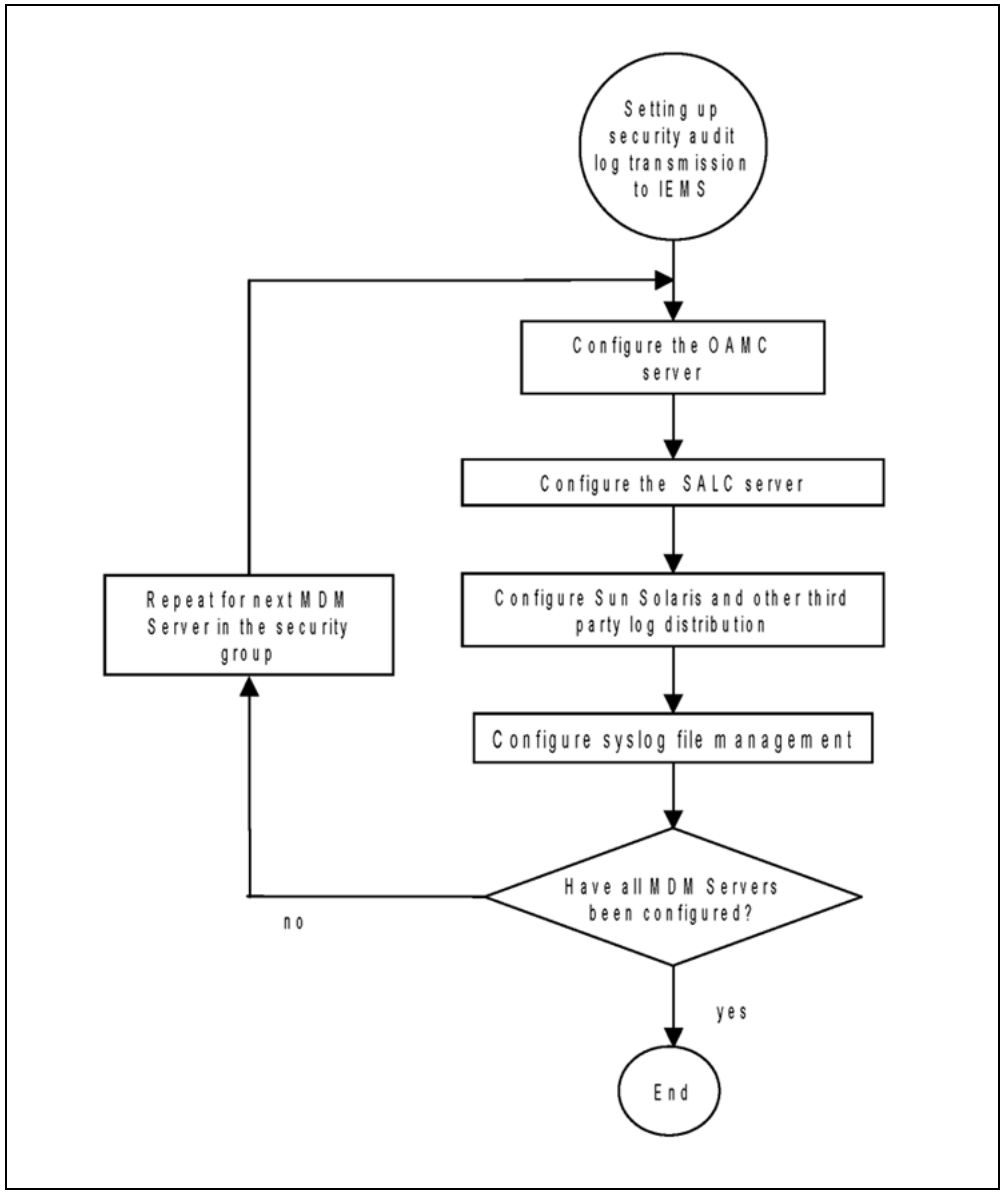
Log flows to the higher level management system



For more information on security audit logs, see *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

The following task flow describes the procedures required to configure the OAMC and SALC servers on the MDM Servers to send the security audit logs to IEMS.

Task flow for sending security audit logs to IEMS



Prerequisites

Before using these procedures:

- Know which syslog log stream formats are to be sent to IEMS for this deployment: custlog V2, syslog or both.
- For each MDM Server, verify that the GMDR server was configured during the upgrade procedure to have an OAMC server for each MDM Server that connects to it. For more information, see NN10440-450 Upgrading the Carrier Voice over IP Network.

Repeat the following procedures for each MDM Server in the security domain.

Configuring the OAMC server on the MDM Server

Step	Action

Using a secure desktop connection

1 Log in to the MDM Server as root.

2 View the default configuration file */opt/MagellanNMS/lib/cfg/OAMLog.cfg* and check that the variables systemWideLogLevel and systemWideAuditLevel have the following values shown as bold text:

```
#[FATAL,ALERT,CRIT,ERROR,WARN,CLEARED,NOTICE]

systemWideLogLevel:
FATAL,ALERT,CRIT,CLEARED,NOTICE

#[FATAL,ALERT,CRIT,ERROR,WARN,CLEARED,NOTICE,INFO,DEBUG,TRACE]

systemWideAuditLevel:
FATAL,ALERT,CRIT,CLEARED,NOTICE
```

These values indicate the types of logs that will be collected.

Note: Changing the default values is not recommended as it can cause performance degradation. If, however, you need to change the default values assigned to these two variables, do the following:

a. Create a customized configuration file from the default version:

```
cp /opt/MagellanNMS/lib/cfg/OAMLog.cfg /opt/MagellanNMS/cfg/OAMLog.cfg
```

b. Edit the variables appropriately using the values contained in the line above the variable definition line. Save and close the file.

This version of the configuration file is automatically used instead of the default configuration file.

3 Configure the retention time for the log files that are stored on the MDM Server. Older files must be deleted periodically to prevent the MDM disk from filling up.

Create a customized version of the configuration file from the default version:

```
cp /opt/MagellanNMS/lib/cfg/MDMClean.cfg
```

/opt/MagellanNMS/cfg/MDMClean.cfg

Edit the file and change the *RetentionDays* variables as follows:

```
Directory:  /opt/MagellanNMS/data/log/oamc
RetentionDays:  7
Directory:  /opt/MagellanNMS/data/log/svmdmn
RetentionDays:  7
Directory:  /opt/MagellanNMS/data/log/MDMAgents
RetentionDays:  7
Directory:  /opt/MagellanNMS/data/log/csvr
RetentionDays:  7
Directory:  /opt/MagellanNMS/data/log/ipm
RetentionDays:  7
Directory:  /opt/MagellanNMS/data/log/nat
RetentionDays:  7
Directory:  /opt/MagellanNMS/data/log/osh
RetentionDays:  7
Directory:  /opt/MagellanNMS/data/log/pcms
RetentionDays:  7
Directory:  /opt/MagellanNMS/data/security
RetentionDays:  7
Directory:/opt/MagellanNMS/data/log/salcserver
RetentionDays:  7
```

Save and close the file.

4 Edit the root crontab:

```
EDITOR=vi
export EDITOR
crontab -e
```

and add the following line to enable removal of log files after the specified retention time:

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

—End—

This is the end of the procedure for "Configuring the OAMC server on the MDM Server" (page 76).

Configuring the SALC server on the MDM Server to send custlogs and syslogs to IEMS

Use this procedure to send the security audit log custlog V2 stream and/or syslog stream from the MDM Server to the IEMS.

ATTENTION

If you are enabling logging on MDM (using the -outputFile option); and there is more than one SDM/IEMS northbound of the MDM, you must only use the -outputFile option on one of the SALC servers. If you use the -outputFile option on both of the SALC servers, duplicate logs will be retained on the MDM.

Prerequisites

Before using this procedure:

- Obtain the root userids /passwords, host name and MSS/MG15000 group server name for each MDM Server.
- Obtain the MSS/MG15000 userid and password for the MSS/MG15000 group that provides access to the MSSMG log stream. The userid must have an impact of system administrations and a scope of device.
- Obtain the node name and IP address for IEMS
- If the logs are to be sent to the IEMS in custlog V2 format, verify that the SALC custlog configuration file exists with the name:
  - `/opt/MagellanNMS/cfg/SALCServer_cust-log_<IEMS_nodename>.cfg`
- If the logs are to be sent to the IEMS in syslog format, verify that the SALC syslog configuration file exists with the name:
  - `/opt/MagellanNMS/cfg/SALCServer_syslog_<IEMS_node-name>.cfg`

  Note: If both the custlog V2 format and syslog format log feeds to the IEMS have been configured, then omit the -outputFile parameter from one of the SVM tool commands to start an instance of the SALC server. Including this command in both cases causes the log stream to be duplicated in the MDM storage files.

Configure the custlog V2 log flow

Step	Action
	Using a secure desktop connection
1	Log in to the MDM Server as root.
2	Edit the custlog configuration file to contain the MSS/MG15000 switches in the security domain: **`vi /opt/MagellanNMS/cfg/SALCServer_custlog_<IEMS_nodename>.cfg`**

3 In the file, provide an entry for the MSS/MG15000 group that connects to the MDM Server to provide fault, performance and security data. A sample entry follows:

```
Hostname:  <MDM_hostname>
Servername:  FMDR_<MSSMG_group>
UserId:  <MSSMG_group_name>
Password:  <MSSMG_group_password>
EncryptedPassword:
```

For added reliability, also provide an entry to collect the log information for this group from the other MDM Server.

```
Hostname:  <other_MDM_hostname>
Servername:  FMDR_<MSSMG_group>
UserId:  <MSSMG_group_name>
Password:  <MSSMG_group_password>
EncryptedPassword:
```

Lastly, you provide entries to collect all the events that occur on the MDM Server itself:

```
Hostname:  <MDM_hostname>
Servername:OAMC
```

For added reliability, you collect all the events that occur on the other MDM Server:

```
Hostname:<other_MDM_name>
Servername:OAMC
```

Save and close the file.

4 Using the SVM tool, enter the following string to start an instance of the SALC server to send the custlog stream to the IEMS:

```
/opt/MagellanNMS/bin/salcserver -OAMCFacility
local1 -passportFacility local1 -outputSyslog
<IEMS_IPaddr> -outputFile -logfile <log_level> -name
custlog_<IEMS_nodename> -nodeId
<MDM_nodename>
```

This command sets up the custlog distribution as follows:

- All MDM and MSS/MG15000 security audit logs in custlog V2 format are directed to facility *local1* on the IEMS.
- The logs are written to the MDM file /opt/MagellanNMS/data/security/security_custlog_ <IEMS_nodename>.nlog
- Logs of the levels defined in <log_level> are written to the file /opt/MagellanNMS/data/log/salcserver/salcserver_cust-log_<IEMS_nodename>.alog.

The list of log levels that may be used are:

```
DEBUG, INFO, NOTICE, CLEARED, WARN, ERROR,
CRIT, ALERT, FATAL
```

If no values are specified, the default log levels used are:

```
NOTICE, CLEARED, CRIT, ALERT, FATAL
```

—End—

Configure the syslog log flow

The syslog feed to the IEMS is configured in the same way as the custlog feed.

Step	Action

Using a secure desktop connection

1 Log in to the MDM Server as root.

2 Create the syslog configuration file by copying the custlog configuration file:

```
cp
/opt/MagellanNMS/cfg/SALCServer_custlog_<IEMS_nodenam
e>.cfg
/opt/MagellanNMS/cfg/SALCServer_syslog_IEMS_
nodename>.cfg
```

3 Using the SVM tool, enter the following string to start an instance of the SALC server to send the syslog stream to the IEMS:

```
/opt/MagellanNMS/bin/salcserver -OAMCFacility
local3 -passportFacility local3 -outputSyslog
<IEMS_IPaddr> -outputFile -logfile <log_level> -name
syslog_<IEMS_nodename>
```

This command sets up the syslog distribution as follows:

- All MDM and MSS/MG15000 security audit logs in syslog format are directed to facility *local3* on the IEMS.
- The logs are written to the MDM file /opt/MagellanNMS/data/security/security_syslog_ <IEMS_nodename>.nlog
- Logs of the levels defined in <log_level> are written to the file /opt/MagellanNMS/data/log/salcserver/salcserver_syslog_ <IEMS_nodename>.alog.

  The list of log levels that may be used are:

```
DEBUG, INFO, NOTICE, CLEARED, WARN, ERROR,
CRIT, ALERT, FATAL
```

If no values are specified, the default log levels used are:

```
NOTICE, CLEARED, CRIT, ALERT, FATAL
```

—End—

This is the end of the procedures for "Configuring the SALC server on the MDM Server to send custlogs and syslogs to IEMS" (page 77).

Variable values

Variable	Value
<IEMS_IPaddr>	is the IP address of the IEMS receiving the log stream.
<log_level>	is the list of log levels to be written to the local file. If no values are specified, the defaults NOTICE, CLEARED, CRIT, ALERT, AND FATAL are used.
<IEMS_nodename>	is the IEMS node name to be appended to the file name.
<MDM_nodename>	is the MDM Server node name to be incorporated in the SCC2 logs.
<MDM_hostname>	is the host name of the MDM Server.
<MSSMG_group>	is the name of the server for the MSS/MG15000 group.
<MSSMG_group_name>	is the userid of the MSS/MG15000 group.
<MSSMG_group_password>	Password for the MSS/MG15000 group userid.

Configuring the MDM Server to send Solaris and other third party logs to IEMS

This procedure configures the MDM Server to send Solaris and other third party software security logs to IEMS and to write them to a local MDM file.

Prerequisites

Before using this procedure:

- have the IP address of the IEMS

Configure the MDM Server for sending Solaris and third party logs

Step	Action

Using a secure desktop connection

1 Log in to the MDM Server as root.

2 Backup the current version of the Solaris syslog configuration file:

```
cp /etc/syslog.conf /etc/syslog.conf.OSharden
```

3 Copy the default syslog configuration file:

```
cp /etc/syslog.conf.MDMorig /etc/syslog.conf
```

4 Edit the syslog configuration file:

```
vi /etc/syslog.conf
```

Edit the file contents to contain the following:

```
*.crit <tab> /var/adm/emerglog
*.info <tab> /var/adm/messages
local0.info <tab> /var/adm/messages
local0.info <tab> @<IEMS_IPaddr>
local1.info <tab> /var/adm/local1
local3.info <tab> /var/adm/local3
auth.info <tab> /var/log/authlog
auth.info <tab> @<IEMS_IPaddr>
```

Note: <tab> indicates that a tab character was used as the field separator.

Save and close the file.

5 Create the following files and set their ownership:

```
touch /var/log/authlog
touch /var/adm/emerglog
touch /var/adm/local1
touch /var/adm/local3
chmod 644 /var/log/authlog
chmod 644 /var/adm/emerglog
chmod 644 /var/adm/local1
chmod 644 /var/adm/local3
```

This results in the following log distribution:

- Logs relating to local or central user authentication and authorization are written to /var/log/authlog and sent to the IEMS syslog daemon.
- SSH and IPSec logs and general UNIX logs are written to /var/adm/messages and sent to the IEMS syslog daemon.

6 Restart the syslog daemon:

```
/etc/init.d/syslog stop; /etc/init.d/syslog
start
```

—End—

This is the end of the procedure for "Configuring the MDM Server to send Solaris and other third party logs to IEMS" (page 81).

Syslog file management configuration

To ensure that syslog files do not fill up entire disk partitions, limit the amount of data that is retained.

Step	Action

Using a secure desktop connection

1 Log in to the MDM Server as root.

2 Edit the file */etc/logadm.conf:*

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

3 Find the line starting "/var/log/syslog" and change the following two parameters as shown:

```
-S 10m
-p 1d
```

4 Find the line starting "/var/ladm/messages" and change the following two parameters as shown:

```
-S 10m
-p 1d
```

5 After the line starting with "/var/adm/messages", add the following lines:

```
/var/log/authlog -C 4 -P 'Thu Sep 16 07:10:00
2004' -S 10m -a 'kill -HUP `cat
/var/run/syslog.pid`' -p 1d
/var/adm/emerglog -C 4 -P 'Thu Sep 16 07:10:00
2004' -S 10m -a 'kill -HUP `cat
/var/run/syslog.pid`' -p 1d
/var/adm/local1 -C 4 -P 'Thu Sep 16 07:10:00
2004' -S 10m -a 'kill -HUP `cat
/var/run/syslog.pid`' -p 1d
/var/adm/local3 -C 4 -P 'Thu Sep 16 07:10:00
2004' -S 10m -a 'kill -HUP `cat
/var/run/syslog.pid`' -p 1d
```

Save and close the file.

For more information on the entries in */etc/logadm.conf*, refer to the Sun UNIX documentation.

Note: If additional log types are added to the */etc/syslog.conf* file, they must also be included in the */etc/logadm.conf* file.

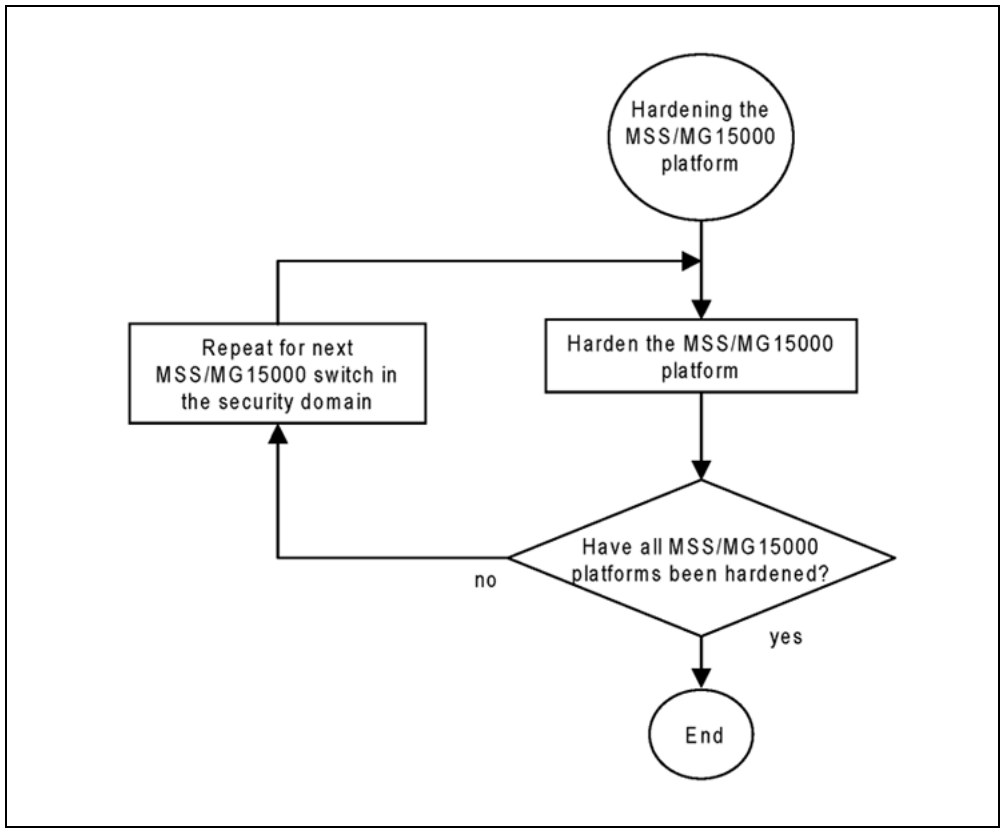
—End—

This is the end of the procedure for "Syslog file management configuration" (page 83).

Hardening the Multiservice Switch 15000 or Media Gateway 15000 platform

The following task flow describes the procedures required to harden the MSS/MG15000 platforms in the security domain.

Task flow for hardening the MSS/MG15000 platform



Repeat this procedure for every MSS/MG15000 switch in the security domain.

Prerequisites

Before using this procedure:

- Obtain a system administration userid and password for the MSS/MG15000 switch.
- Obtain the list of userids that must remain configured on the switch after other userids have migrated to IEMS. See "Transferring userids from MSS/MG15000 to IEMS" (page 101).

For more information on local security features, see *NN10600-601 Multiservice Switch Security Management*.

Harden the MSS/MG15000 platform

Step	Action
	Using a secure desktop connection to the MSS/MG15000
1	Log in to the MSS/MG15000 as system administrator.
2	Configure a console session on the MSS/MG15000 to timeout after it has remained idle for 10 minutes: `set nmis local timeoutperiod 10`
3	Configure a telnet session on the MSS/MG15000 to timeout after it has remained idle for 10 minutes: `set nmis telnet timeoutperiod 10`
4	Enable the new timeout periods for the specified local userid: `set ac userid/<userid> timeoutprotocol enabled` Repeat the command for each locally configured userid that will be retained on the switch. The timeout period will be applied to new sessions only. Existing sessions will not be affected.

5	Set the list of IP addresses that are allowed to log into the MSS/MG15000:
	`add AC IPAccess`
	`<MDM1_IPaddr>,<MDM2_IPaddr>,<IEMS_IPaddr>`

	—End—

Note: There are no commands on the MSS/MG15000 for changing the length of userids or passwords.

This is the end of the procedure for "Hardening the Multiservice Switch 15000 or Media Gateway 15000 platform" (page 85).

Variable values

Variable	Value
<userid>	is a locally configured userid on the MSS/MG15000.
<MDM1_IPaddr>	is the IP address of MDM1.
<MDM2_IPaddr>	is the IP address of MDM2.
<IEMS_IPaddr>	is the IP address of the IEMS.

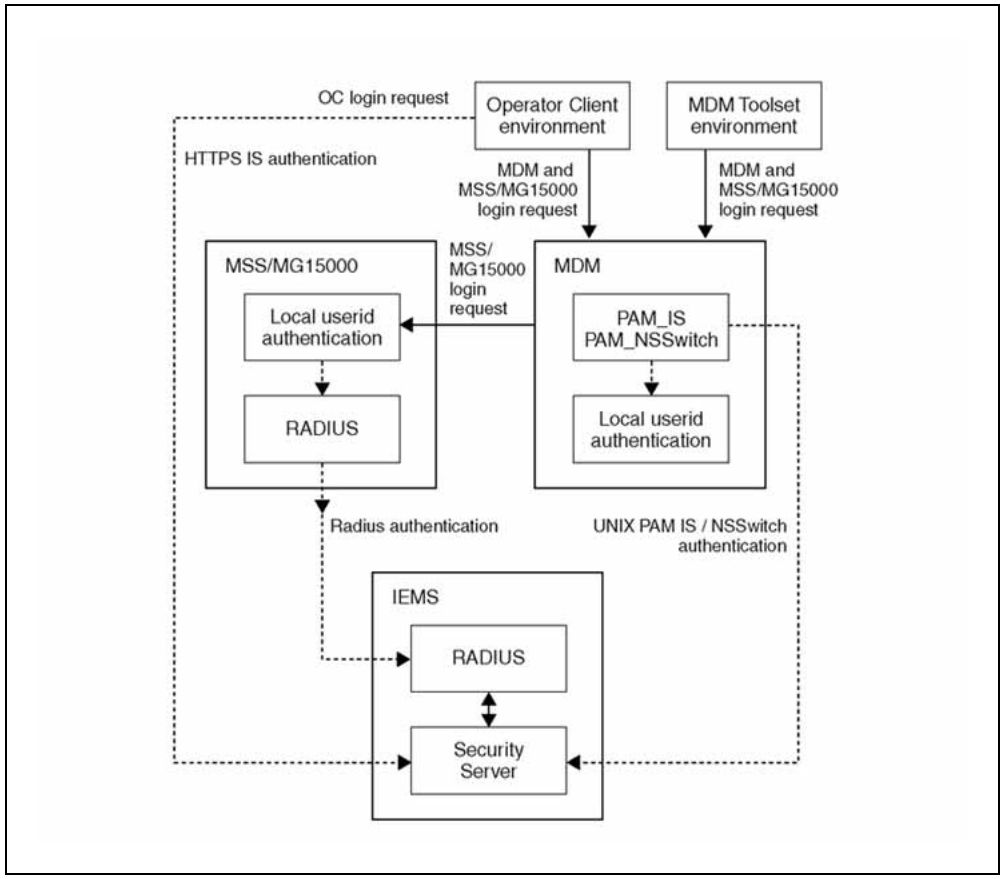
Securing user access for the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager network elements

User access security is enhanced by having all users authenticated and authorized through a central security server. In VoIP networks, IEMS provides the central authentication and authorization of users.

Userids and passwords entered into the MDM or MSS/MG15000 applications are sent to the IEMS for authentication. Upon successful authentication, IEMS sends back the appropriate group and scope information. The MDM Servers and the MSS/MG15000 switches map the IEMS information onto the MDM Server and MSS/MG15000 switch access privileges.

The following figure shows the logical flow of authentication data.

Logical flow of authentication data



PAM IS and PAM NSSwitch interfaces provides the authentication path between the MDM Server and the IEMS central security server. The PAM IS and NSSwitch modules allow UNIX users on the MDM server to be centrally administered by the IEMS. A RADIUS client interface on the MSS/MG15000 switch provides the authentication path with the IEMS central security server. The Operator Client application connects directly to the IEMS central security server for authentication.

MDM userids are compared first to the central userids on the IEMS Server. If no match is found, then the locally defined userids are compared.

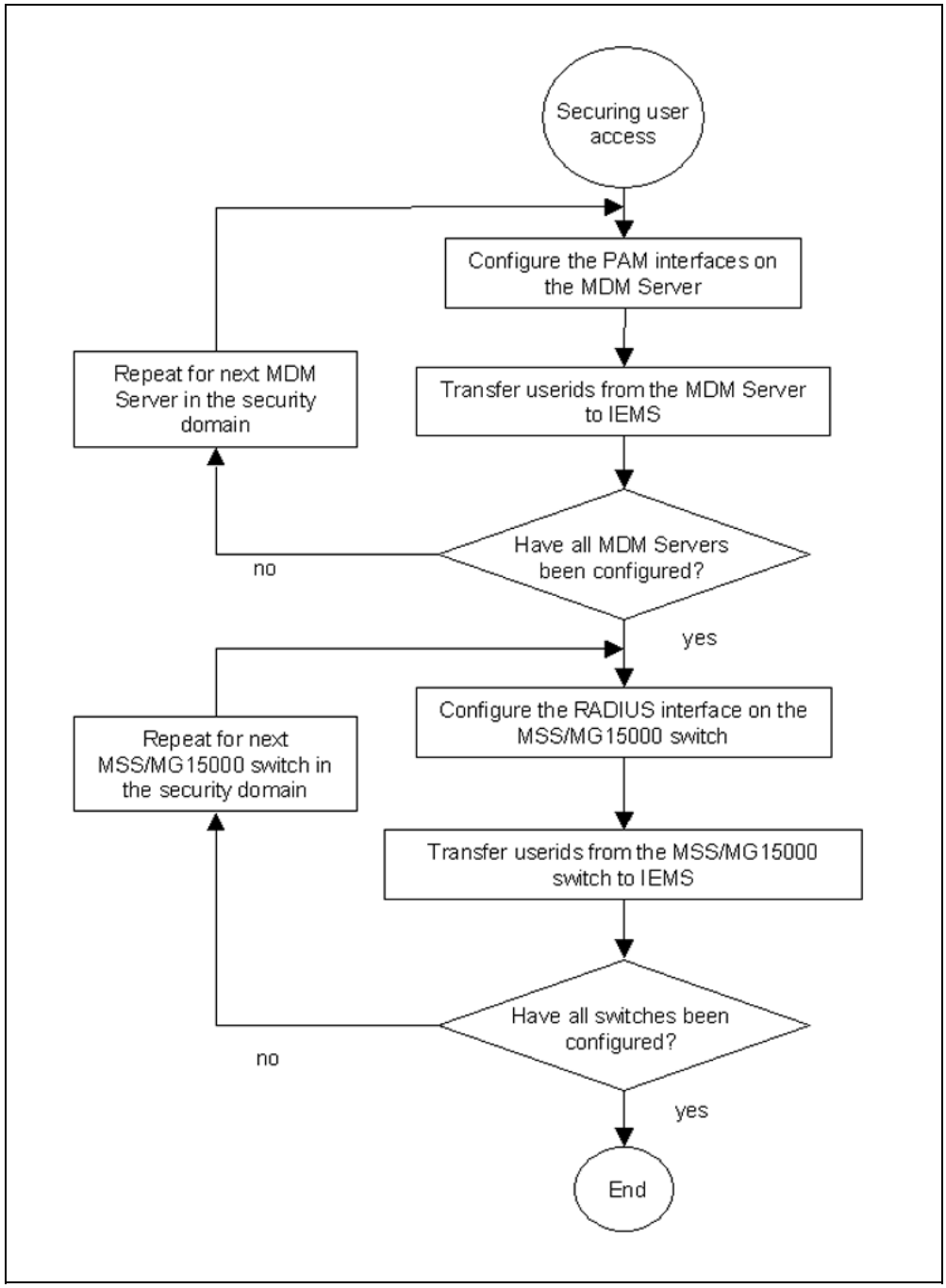
MSS/MG15000 userids are compared first to the locally defined userids. If no match is found, then the central userids on the IEMS Server are compared.

For more information on the mapping between the IEMS authorization levels and the MDM and MSS/MG15000 authorization levels, please see *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

The MDM Servers and MSS/MG15000 switches each must retain some locally configured userids. See "Transferring userids from MDM to IEMS" (page 97) and "Transferring userids from MSS/MG15000 to IEMS" (page 101).

The following task flow describes the procedures required to transfer MDM and MSS/MG15000 userids to the IEMS.

Task flow for transferring MDM and MSS/MG15000 userids to the IEMS



For more information on the operation of centralized user authentication and authorization, refer to *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

There are three areas of user access that need to be configured to use the IEMS centralized authentication and authorization service:

- MDM UNIX-based user access
- MSS/MG15000 user access
- Operator Client user access

Prerequisites

Before using the following procedures:

- Ensure the IEMS has been configured to access an SN09 MDM Server
- Ensure the IEMS has been configured to act as a central AAA server
- Ensure the IEMS has been configured with RADIUS shared secrets for all MSS/MG15000 switches in the security domain. These shared secrets should be transmitted via a secure method.
- Obtain the FQDN for the IEMS and the MDM Servers
- Obtain the current password for the IEMS userid amadmin.

  Obtain the Carrier VoIP SN09 Security Software CD.

Migrating MDM UNIX userids to IEMS

Repeat the following procedures for each MDM Server in the security domain.

Set up MDM Toolset restricted access

Use the following procedure to install the MDM Toolset restricted access menus and set-up the restricted access user groups.

Step	Action

Using a secure desktop connection

1 Log in to the MDM Sun workstation as root.

2 Backup the tsets directory before installing the new files:

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

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

3 Install the restricted access MDM toolset menus from the Carrier VoIP SN09 Security Software CD:

```
cp <CVoIP CD>/tsets.C.tar
/opt/MagellanNMS/cfg/tsets/tsets.C.tar
```

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

```
tar xvf tsets.C.tar
```

ATTENTION

If the MDM Solaris 0S hardening script has been executed to harden the MDM, the Solaris Management Console (SMC) will not be running. Use the Sun Admintool.

4 Use the Sun administration tool or Solaris Management Console (SMC) to create the following user group names and numbers:

```
1021 emsadm
1022 emsrw
1023 emssprov
1024 emsmtc
1025 emsro
```

—End—

This is the end of the procedure for "Set up MDM Toolset restricted access" (page 93).

Configure the PAM interfaces on the MDM Server

Use the following procedure to configure the PAM Radius and PAM NSSwitch SAML interfaces on the MDM Server.

Step	Action

Using a secure desktop connection

1 Log in to the MDM Sun workstation as root.

2 Install the PAM client software from the from the MDM installation CDs:

```
pkgadd -d /cdrom/cdrom0 NNnsssam1
```

```
pkgadd -d /cdrom/cdrom3 NNpamradclt
```

3 Activate the PAM Radius client software on the MDM Server:

```
cd
/opt/nortel/applications/security/pamradclt_1.1.0/sw
mgmt/bin
```

```
cd
/opt/nortel/applications/security/pamradclt_1.2.0/sw
mgmt/bin
```

```
./activate_pamradclt.sh
```

The following sample output should display:

```
IEMS Security PAM+ radius Client 1.2.0 activated.
```

4 Activate the NSSwitch SAML software on the MDM Server:

cd /opt/nortel/applications/security/nsssaml_1.2.0/swmgmt/bin

./activate_nsssaml.sh

The following sample output should display:

```
current_link is:
/opt/nortel/applications/security/current_nasssaml
and LUPATH is:
NOTE: Activation of freshly installed nsssaml 1.2.0
component
NOTE: Operation succeeded.
```

5 Configure the PAM Radius client software on the MDM:

cd /opt/nortel/applications/security/pamradclt_1.2.0/swmgmt/bin

./configure_pamradclt.sh -subcomponent libs

6 Create copies of the /etc/pam.conf and /etc/nsswitch.conf files for rollback use if required.

cp /etc/pam.conf /etc/pam.conf_presecurity

cp /etc/nsswitch.conf/etc/nsswitch.conf_presecurity

7 Configure the NSSwitch SAML software on the MDM Server:

cd /opt/nortel/applications/security/current_nsssaml/swmgmt/bin

./configure_nsssaml.sh -subcomponent nsssaml

The configuration application will prompt for input (default values are shown in []). Enter the values shown below (shown in bold after the colon):

```
NOTE: Configuring component nsssaml
NOTE: Setting up nsswitch.conf.is.
NOTE: Setting up nss_saml.so.1.
NOTE: Configuring nsssaml subcomponent

Enter the SAML servlet server Protocol [http]:
https

Enter the SAML servlet server Port [58080]: 58081

Enter the SAML servlet server Host:
<IEMS FQDN>

Enter the connection timeout value [100]:
```

```
<select default>

Enter the request timeout value [40]:
<select default>

Enter the connection pool max value [64]:
<select default>

Enter the file descriptor max value [8192]:
<select default>

Enter the servlet backend value - nsswitch or
nds_only [nsswitch]:
<select default>
NOTE: Operation succeeded.
```

8 Copy the pam.conf and nsswitch.conf files from the Carrier VoIP SN09 Security Software CD:

```
cp <CVoIP CD>/pam.conf /etc/pam.conf

cp <CVoIP CD>/pam.conf /etc/nsswitch.conf
```

This overwrites the existing pam.conf file.

9 Edit the file /etc/nsswitch.conf to add in the entries required to link MDM to IEMS for UNIX authorization. Change the lines:

```
passwd:  files
group:  file
```

to:

```
passwd:  files saml
group:  files saml
```

10 Reinitialize the name service cache daemon (nscd):

```
/etc/init.d/nscd stop

/etc/init.d/nscd start
```

11 Test that the NSSwitch SAML software is working by executing the following command for both a locally defined userid and a userid defined on IEMS and verify the output:

```
id <userid>
```

The following shows a sample command output:

```
> id chrisro          <-- Integrated EMS userid
uid=10003(chrisro) gid=1024
> id root             <-- local userid
uid=0(root) gid=1(other)
```

If the command response "User not found" is received, the authentication path with the IEMS is not working. Verify the configuration on the IEMS.

—End—

This is the end of the procedure for "Configure the PAM interfaces on the MDM Server" (page 94).

Variable values

Variable	Value
<CVoIP CD>	is the path name for the files contained on the Carrier VoIP SN09 Security Software CD.
<installation directory>	is the path name for installation directory on the MDM Server.
<IEMS radius shared secret>	is the Radius shared secret generated by the Radius server.
<IEMS amadmin password>	is the password for IEMS amadmin userid.
<IEMS FQDN>	is the fully qualified domain name for IEMS.

Transferring userids from MDM to IEMS

Prerequisites

Before using this procedure:

- Obtain the IEMS administrator userid.
- Ensure the IEMS central AAA server RADIUS interface should already be configured for the MDM Servers in the security domain. For more information on configuring the IEMS, refer to *NN10330-511 IEMS Configuration Management*.
- Identify all the MDM userids and groups to be moved to the IEMS.

Note: The following userids and groups cannot be centrally located, and must be resident on the MDM Server in the /etc/passwd file:

Local userids and groups to be retained on the MDM server

local userids		local groups		
root	daemon	root	adm	sysadmin
bin	noaccess	staff	noaccess	nortel
adm	nobody	other	uucp	sys
sys	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 userid and group "patcher" are only required to be retained on the MDM server if it hosts the Network Patch Manager.

- For each userid to be moved, determine the correct authorization level to be used on the IEMS. Refer to the table in *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP* that shows the mapping of MDM authorization levels to IEMS groups.

Transfer the userids from the MDM Server

Step	Action

Using a secure desktop connection to the IEMS

1 Log in to the IEMS as administrator.

2 Create the new userids on the IEMS. For information on creating IEMS userids, refer to *NN10336-611 IEMS Security and Administration*.

3 Check that the IEMS userids can access all MDMs in the security domain before proceeding to step 4.

Using a secure desktop connection

4 Log to the MDM Server as root.

5 Run the Solaris Management Console:

```
smc &
```

For information on using the Solaris Management Console, refer to the Solaris on-line help documentation.

6 List all the userids.

7 Delete the userids just created on the IEMS.

Note: Do not delete any of the userids listed in "Prerequisites" (page 97).

8 Identify the local userids that are used to access the MDM Toolset. Assign each userid to one of the following groups according to the access privileges required:

```
emsadm
emsrw
emssprov
emsmtc
emsro
```

See *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP* for the mapping of IEMS groups to MDM tools access and MSS/MG15000 access privileges.

—End—

This is the end of the procedure for "Transferring userids from MDM to IEMS" (page 97).

Migrating MSS/MG15000 userids to IEMS

Repeat the following procedure for each MSS/MG15000 switch in the security domain.

Prerequisites

The IEMS central security server RADIUS interface should already be configured for the MSS/MG15000 switches in the group. For more information on configuring the IEMS, refer to *NN10330-511 IEMS Configuration Management*.

Configure the RADIUS client interface on the MSS/MG15000 switch

Use the following procedure to configure the RADIUS interface to the IEMS.

Step	Action

Using a secure desktop connection

1 Log in to the MSS/MG15000 switch as system administrator.

2 Save a copy of the current provisioning view in the event that use of IEMS central authentication and authorization needs to be disabled:

```
start prov

save -current -f(<preRadCfgViewName>) -portable prov
```

3 Add the OAMRadius to the LPT/CP feature list:

```
set software lpt/cp featurelist oamRadius

check prov

activate prov

confirm prov
```

4 Add a Radius server:

```
add Ac Radius
```

5 Specify the MSS/MG15000 IP address used to communicate with the IEMS. This will be the IP address of the MSS/MG15000 management Vr.

```
set ac Radius nasIdentifier <MSSMG nas IP address>
```

6 Set the attributes for the Radius server:

```
set ac radius server/0 sharedSecret
<IEMS_radius_shared_secret>, serverPortNumber
<MSSMG_UDP_port>, serverIpAddress <IEMS IP address>,
ipstack VrIp
```

> ***Note:*** The shared secret will be originated by the IEMS installation. This shared secret should be transmitted by a secure method only.

7 Save the new view:

```
check prov

save -f(<postRadiusViewName>) -portable prov

activate prov

confirm prov

commit prov
```

—End—

This is the end of the procedure for "Configure the RADIUS client interface on the MSS/MG15000 switch" (page 100).

Variable values

Variable	Value
<MSSMG nas IP address>	is the IP address of the management Vr.
<MSSMG UDP port>	is the MSS/MG15000 UDP port number.
<IEMS radius shared secret>	is the Radius shared secret generated by the IEMS.
<IEMS IP address>	is the IP address of the IEMS Radius server.
<postRadiusViewName>	is the filename for saved provisioning view containing the Radius client configuration.

Transferring userids from MSS/MG15000 to IEMS

Prerequisites

Before using this procedure:

- Identify all the MSS/MG15000 userids and groups to be moved to the IEMS.

  Note 1: Every MSS/MG15000 switch must retain one local emergency userid with an impact of debug so that the node can be accessed in case communication with the IEMS central AAA system is lost. It is recommended that this userid have an impact of debug.

  Note 2: The userids for MDP, FMDR and PMSP must remain configured locally to allow access and permit the transfer of surveillance data in the case of loss of communication with the IEMS central AAA system.

- For each userid to be moved, determine the correct authorization level to be used on the IEMS. Refer to the table in *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP* that shows the mapping of MSS/MG15000 authorization levels to IEMS groups.

Transfer the userids from the MSS/MG15000 switch

Step	Action
	Using a secure desktop connection

1 Log in to the IEMS as administrator.

2 Create the new userids on the IEMS. For information on creating IEMS userids, refer to *NN10336-611 IEMS Security and Administration*.

3 Verify that the userids work for accessing all MSS/MG15000 switches in the group before proceeding to remove the old MSS/MG15000 userids.

Using a secure desktop connection to the MSS/MG15000 switch

4 Log in to the MSS/MG15000 switch as system administrator.

5 List the current MSS/MG15000 userids:

```
l ac userid/*
```

6 Delete the userids just created on the IEMS except for the userids to be retained locally. See "Prerequisites" (page 101).

```
start prov
copy prov
del ac userid/<userid>
```

Note: Repeat this command for each userid to be deleted.

```
check prov
save -f(<postUserMigration>) -portable prov
activate prov
confirm prov
commit prov
```

—End—

This is the end of the procedure for "Transferring userids from MSS/MG15000 to IEMS" (page 101).

Variable values

Variable	Value
<userid>	is the MSS/MG15000 userids to be removed from the MSS/MG15000 node.
<postUserMigration>	is the filename of saved provisioning view after the userids have been migrated to the IEMS.

Configuring MDM Servers for Operator Client users

Repeat this procedure for each MDM Server that has the Java Web Start (JWS) software installed.

Prerequisites

Before using the following procedures:

- Obtain the fully qualified domain name (FQDN) for the IEMS
- If the MDM server is a consolidated management (CM) server, determine the IEMS in the network partition that will be providing the central AAA services for the Operator Client users. Only one IEMS in the partition may be selected.

Configure the MDM Server

Use the following procedure to configure the JWS software on the MDM Server to send authentication requests to the central IEMS security server.

Step	Action

Using a secure desktop connection

1 Log in to the MDM Server as root.

2 Configure the isclient component:

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

./configure_isclient.sh
```

The configuration application will prompt for input (default values are shown in square brackets). Enter the values shown below (shown in bold after the colon) when prompted:

```
NOTE: Configuring component isclient
NOTE: Configuring isclient subcomponent

Enter the SunONE ID Protocol [http]: https

Enter the SunONE IS Port [58080]: 58081

Enter the SunONE IS Host 1
[wcary3r6.ca.nortel.com]: <IEMS FQDN>
Enter the SunONE IS Host 2 (or .  to end the hostlist)
[No Default]:  .

Enter the Directory Suffix [ca.nortel.com]:
<Nortel domain name>
NOTE: Operation succeeded.
```

3 Configure the authentication component:

```
cd
/opt/nortel/applications/desktop/current_authen/swmg
mt/bin

./configure_authen.sh -subcomponent isconfig
```

The configuration application will prompt for input (default values are shown in square brackets). Enter the values shown below (shown in bold after the colon) when prompted:

```
NOTE: Configuring authen component
NOTE: Configuring local authen subcomponent

Reconfigure the local and JWS security
configuration [no]: yes
NOTE: Operation succeeded.
```

—End—

This is the end of the procedure for "Configuring MDM Servers for Operator Client users" (page 103).

Note: To launch the Operator Client application from the operator's desktop, use the following URL.

- For MDM Servers using the Sun Fire V480 platform:

  http://<MDM Server name>:8080/UI

- For MDM Servers using the Sun Netra 240 platform:

  http://<MDM Server name>:8090/UI

  Select a heap size of 256MB when prompted.

For more information on launching the Operator Client application, see the section "Starting Operator Client" in *241-6001-122 Nortel Multiservice Data Manager Using MDM Tool Set and Operator Client Interfaces*

Variable values

Variable	Value
<IEMS FQDN>	is the fully qualified domain name of the IEMS.
<MDM Server name>	is the name of the MDM Server hosting the JWS software

Disabling security features on Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager components

It is not possible to disable all the security measures without any disruption to service. However, the order of the procedures in this section minimizes disruptions to service. The high level approach is to:

- disable security on MDM1
- change configuration setting on IEMS
- disable security on the MSS/MG15000 switches
- disable security on MDM2

Task table for disabling security features

	task	outcome
1	Disable the security features on MDM1. See "Disabling security features on an MDM Server" (page 106)	• X11 desktops do not require SSH to communicate with the MDM1. • Operator Client is no longer active • All links to MDM2 and the MSS/MG15000 switches are non-operational • All surveillance data flow and management access with the switches is through the secured links with MDM2
2	Configure IEMS to access MDM1 without SSH.	• IEMS is configured to access an SN07 MDM Server. This re-enables telnet access to the MDM Server.

	task	outcome
3	Disable the security features on MSS/MG15000 switches 1-n. See "Disabling security features on an MSS/MG15000 switch" (page 107).	• All MSS/MG15000 switches are communicating through MDM1
4	Disable the security features on MDM2. See "Disabling security features on an MDM Server" (page 106).	• All connections between all MDM Servers, MSS/MG15000 switches, and IEMS should be operating normally in pre-security mode.

Disabling security features on an MDM Server

Step	Action
	Using a desktop connection
1	Log in to the MDM Server as system administrator.
2	Determine all the userids that are required to access the MDM Server using the MDM Toolset interface. Note that the desktop Operator Client applications will not work once the central AAA security service is disabled.
3	Create local userids on the MDM Server and disable the PAM_RADIUS and PAM_NSSwitch interfaces. See "Disabling central user authentication and authorization for an MDM Server" (page 107).
4	Disable sending of security audit logs to IEMS. See "Disabling transmission of security audit logs on an MDM Server" (page 112). Security audit logs continue to be written to file on the MDM Server.
5	Remove any third party firewall configuration.
6	Remove all the security associations on the MDM Server for other MDM Servers and for the MSS/MG15000 switches. See "Disabling IPSec on an MDM Server" (page 114). Once all the security associations are removed, the MDM Server can no longer communicate with the other MDM Server or with the MSS/MG15000 switches. All surveillance data from and management commands to the MSS/MG15000 switches will use the other MDM Server.
7	Unharden the MDM platform. See "Disabling MDM platform hardening" (page 111).

8 As there is no impact for leaving SSH on the MDM Server, there is no need to disable SSH functionality.

—End—

This is the end of the procedure for "Disabling security features on an MDM Server" (page 106).

Disabling security features on an MSS/MG15000 switch

Step	Action
	Using a desktop connection
1	Log in to the MSS/MG15000 switch as system administrator.
2	Determine all the userids that are required to access the switch.
3	Create local userids on the MSS/MG switch and disable the RADIUS client interface to IEMS. See "Disabling central user authentication and authorization for an MSS/MG15000 switch" (page 109).
4	Unharden the MSS/MG platform. See "Disabling MSS/MG15000 platform hardening" (page 110).
5	Remove all the security associations on the MSS/MG15000 switch. See "Disabling IPSec on an MSS/MG15000 switch" (page 113). Once all the security associations are removed, the MSS/MG switch can only communicate with an MDM Server that is not using IPSec.

—End—

This is the end of the procedure for "Disabling security features on an MSS/MG15000 switch" (page 107).

Disabling central user authentication and authorization for an MDM Server

Prerequisites

Before using this procedure:

- Determine all the userids and access privileges for the MDM Toolset user environment. This should include Operator Client users since the desktop Operator Client applications will no longer function once central user AAA is disabled.

Disable central user authentication and authorization

Step	Action

From a desktop connection

1 Log in to the MDM Server as root.

2 Add all the users requiring access to the MDM Toolset user environment. See "Adding a new MDM local user" in *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*

3 Make each user an NMS user. For each userid, execute the following command:

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

4 Create a copy of the current security configuration settings to facilitate future re-enabling of the PAM interfaces:

```
cp /etc/pam.conf /etc/pam.conf_postsecurity

cp /etc/nsswitch.conf

/etc/nsswitch_postsecurity
```

5 Disable the PAM interfaces so that authentication requests are no longer sent to IEMS. Do this by restoring the configuration files to the previous versions:

```
cp /etc/pam.conf_presecurity /etc/pam.conf

cp /etc/nsswitch.conf_presecurity
/etc/nsswitch.conf
```

6 Restore MDM Toolset access menus to the unrestricted ones:

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

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

—End—

This is the end of the procedure for "Disabling central user authentication and authorization for an MDM Server" (page 107).

Disabling central user authentication and authorization for an MSS/MG15000 switch

Disable central user authentication and authorization on an MSS/MG15000 switch by restoring the provisioning view saved at the start of the procedure "Configure the RADIUS client interface on the MSS/MG15000 switch" (page 100).

Step	Action

Using a desktop connection

1 Log in to the MSS/MG15000 switch as system administrator.

2 Enter provisioning mode:

```
start prov
```

CAUTION
Activating a provisioning view can affect service.
Activating a provisioning view can result in a CP reload or restart, causing all services on the Multiservice Switch 15000 node to fail. See *NN10600-050 Nortel Multiservice Switch 7400/15000/20000 Command Reference* for more information.

3 Activate the provisioning view saved at the start of the configuration of the Radius client on the MSS/MG15000:

```
load -file(<preRadCfgViewName>) prov
```

4 Check the provisioning changes:

```
check prov
```

5 Activate the provisioning changes:

```
activate prov
```

6 Confirm the provisioning view:

```
confirm prov
```

7 Commit the provisioning changes:

```
commit prov
```

8 Exit provisioning mode after the commit is complete:

```
end prov
```

—End—

This is the end of the procedure for "Disabling central user authentication and authorization for an MSS/MG15000 switch" (page 109).

Variable Value

Variable	Value
<preRadCfgViewName>	is the name of the provisioning file saved prior to the start of configuring the Radius client software and migrating MSS/MG15000 userids to the IEMS.

Disabling MSS/MG15000 platform hardening

It is highly recommended that the MSS/MG15000 platform remain hardened. If required, the following procedure will unharden the platform by removing idle session timeout periods, and allowing any IP address to access the platform.

Step	Action

Using a desktop connection

1 Log in to the MSS/MG15000 switch as system administrator.

2 To remove the timeout period for idle telnet sessions, execute the following command:

```
set nmis telnet timeoutperiod 0
```

3 Turn off the TCP wrappers to allow access to MDM inetd services such as Telnet:

```
vi /etc/default/inetd
```

In this file, place the '#' character at the front of the line as shown:

```
#ENABLE_TCPWRAPPERS=YES
```

Save and close the file.

Execute the following commands to restart the inetd process:

```
pgrep inetd
```

```
kill -1 <inetd_pid>
```

The output of the pgrep command is used as the <inetd_pid> parameter in the **kill** command.

4 To remove the timeout period for idle local userid sessions, execute the following command:

```
set nmis local timeoutperiod 0
```

5 To allow any IP address to log into the MSS/MG15000, execute the following command:

```
delete AC IPAccess/<ip_address>
```

—End—

This is the end of the procedure for "Disabling MSS/MG15000 platform hardening" (page 110).

Disabling MDM platform hardening

It is highly recommended that the MDM platform remain hardened. If required, the following procedure will unharden the key platform functions.

Step	Action

Using a desktop connection to the MDM Server

1 Log in to the MDM Server as root.

2 Re-enable telnet access by executing the following command:

```
vi /etc/inetd.conf
```

Find the line beginning with "#telnet" and remove the "#" character. Save and close the file.

Determine the process id for the inet daemon:

```
pgrep inetd
```

The value <inetd pid> output by this command is used as input for the next command.

Stop the inet daemon:

```
kill -1 <inet pid>
```

Note: At this point, IEMS must be configured to access an SN07 MDM Server so that it will use telnet instead of SSH to access the MDM Server.

3 Restore access to the ping and traceroute functions by executing the following commands:

```
chmod 511 /usr/sbin/ping
```

```
chmod 511 /usr/sbin/traceroute
```

ATTENTION
This step does not apply to MDM servers deployed on N240 servers with SPFS.

4 Reboot the MDM in single user mode:

```
sync; sync; sync; init s
```

Enter the root password when prompted to do so.

ATTENTION
This step does not apply to MDM servers deployed on N240 servers with SPFS.

5 Run the MDM script to unharden the Solaris operating system by executing the following command:

```
/opt/MagellanNMS/bin/Solaris_OSUnHarden
```

Follow the instructions presented during the execution of the script. Refer to the section "Unhardening the Solaris operating system" in *241-6001-303 Nortel Multiservice Data Manager Administration* for the responses required by the script. The MDM Server will restart in multiuser mode.

—End—

This is the end of the procedure for "Disabling MDM platform hardening" (page 111).

Disabling transmission of security audit logs on an MDM Server

Disable the transmission of security audit logs to the IEMS by:

- restoring the syslog.conf file to the pre-security version
- stopping all instances of SALC servers that are running
- starting a single SALC server

Step	Action

Using a desktop connection

1 Log in to the MDM Server as root.

2 Create a copy of the current configurations to facilitate future re-enabling of Solaris log transmission to the IEMS:

```
cp /etc/syslog.conf
/etc/syslog.conf_postsecurity
```

3 Restore the syslg.conf file to its pre-security activation content:

```
cp /etc/syslog.conf.MDMorig /etc/syslog.conf
```

4 Save the current versions of the SALC custlog V2 and syslog configuration files to facilitate future re-enabling of security audit log transmission to the IEMS:

```
cp
```

```
/opt/MagellanNMS/cfg/SALCServer_custlog_<IEMS_nodename>
/opt/MagellanNMS/cfg/SALCServer

cp
/opt/MagellanNMS/cfg/SALCServer_syslog_<IEMS_ nodename>
/opt/MagellanNMS/cfg/SALCServer
```

5 Using the SVM Administration tool, find all the SALC server instances that are running and stop them.

6 Using the SVM Administration tool, enter the following string to start a new instance of the SALC server:

```
/opt/MagellanNMS/bin/salcserver -outputFile -logfile
```

At this point, security audit logs are no longer sent to the IEMS.

—End—

This is the end of the procedure for "Disabling transmission of security audit logs on an MDM Server" (page 112).

Disabling IPSec on an MSS/MG15000 switch

Disable IPSec on an MSS/MG15000 switch by restoring the provisioning view that was saved after IPSec software was installed but before IPSec software was activated.

Step	Action

Using a desktop connection to the MSS/MG15000 switch

1 Log in to the MSS/MG15000 switch as system administrator.

2 Enter provisioning mode:

```
start prov
```

3 Save the current provisioning view with IPSec active to facilitate future enabling of the feature:

```
save -f(<postIPSecViewName>) -portable prov
```

4 Remove the security policy database:

```
del Vr/0 Ip Spd/1
```

5 Verify the provisioning change:

```
check prov
```

6 Activate the change:

```
activate prov
```

7 Confirm the provisioning change:

```
confirm prov
```

8 Commit the provisioning change:

```
commit prov
```

9 Exit provisioning mode after the commit is complete:

```
end prov
```

—End—

At this point, the MSS/MG15000 switch can only communicate with an MDM Server over unsecured links.

This is the end of the procedure for "Disabling IPSec on an MSS/MG15000 switch" (page 113).

Disabling IPSec on an MDM Server

IPSec on an MDM Server is disabled by removing the security databases. The IPSec software should remain installed to facilitate re-enabling IPSec functionality at a future date.

Step	Action

Using a desktop connection to the MDM Server

1 Log in to the MDM Server as root.

2 Remove the security databases from the MDM Server with the following commands:

```
ipsecconf -f
rm /etc/inet/ipsecinit.conf
touch /etc/inet/ipsecinit.conf
ipsecconf -a /etc/inet/ipsecinit.conf
ipseckey flush
rm /etc/inet/secret/ipseckeys
touch /etc/inet/secret/ipseckeys
ipseckey -f /etc/inet/secret/ipseckeys
```

—End—

This is the end of the procedure for "Disabling IPSec on an MDM Server" (page 114).

Adding or restoring network elements in a secured network

Use the following procedures for restoring Multiservice Data Manager, Media Gateway 15000 and Multiservice Switch 15000 network elements in a secured network:

- "Restoring an MDM Server in a secured network" (page 117)
- "Restoring an MSS/MG15000 switch in a secured network" (page 124)

Use the following procedure to add a Media Gateway 15000 or a Multiservice Switch 15000 network element to a secured network:

- "Adding an MSS/MG15000 switch to a secured network" (page 128)

Use the following procedures to display security association data maintained on the Media Gateway 15000 / Multiservice Switch 15000 and the Multiservice Data Manager Server network elements:

- "Viewing MSS/MG15000 IPSec information" (page 131)
- "Viewing MDM IPSec information" (page 133)

Restoring an MDM Server in a secured network

When an MDM Server is restored from backup, the security association information on the server may be out of synchronization with the rest of the security domain. To restore the IPSec links to the other network elements, the existing IPSec configuration data must be deleted before new security associations are created.

Prerequisites

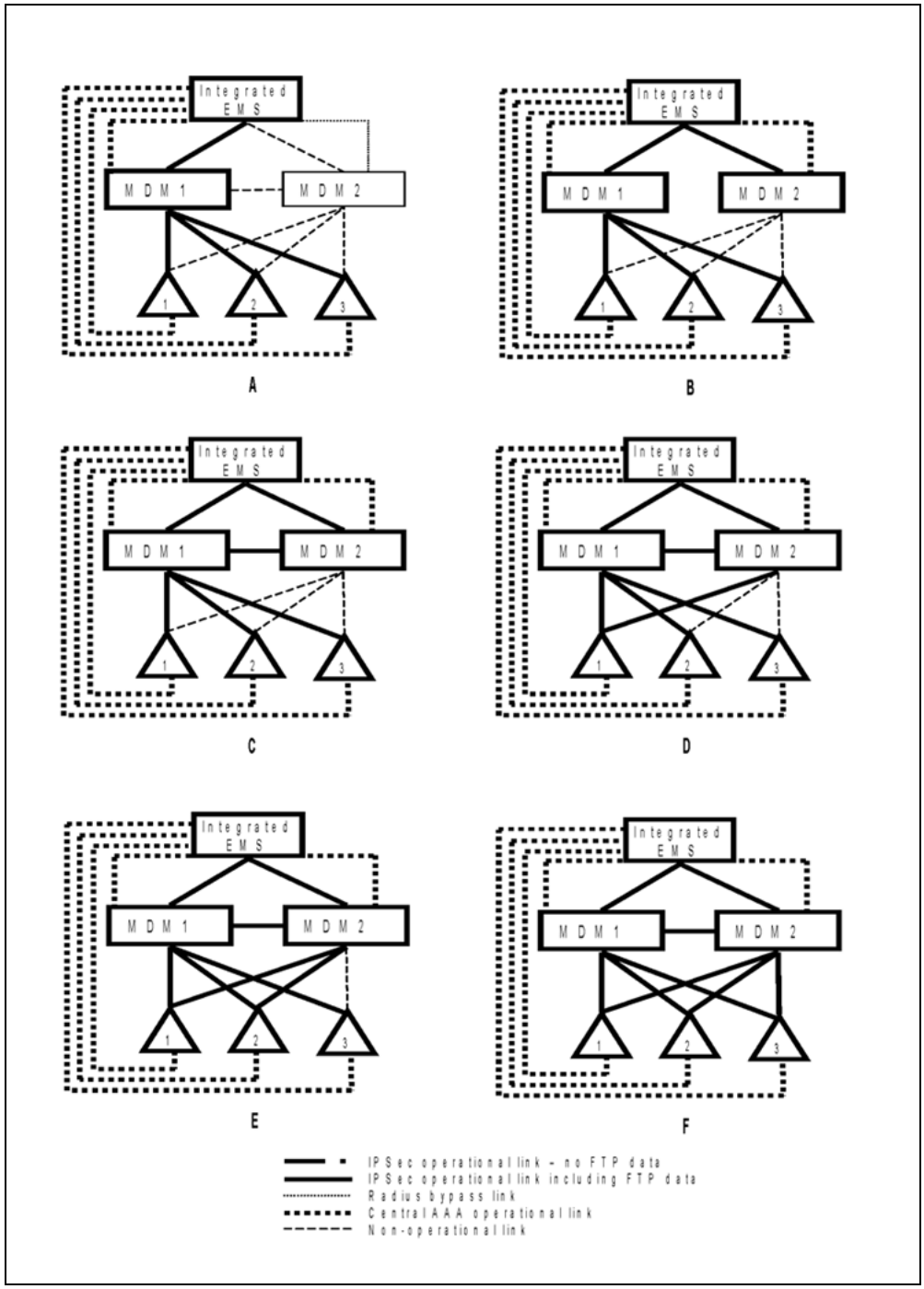
Before using the following procedure:

- Restore the MDM Server from a backup taken when the MDM Server was fully secured.
- Designate the operational MDM Server as MDM1; designate the recovering MDM Server as MDM2.

- Designate the MSS/MG15000 switches from 1 to n in the order that they will be reconnected to MDM2.
- Ensure that the IPSec configuration record is available.
- Be able to log into MDM1 and MDM2 as root.
- Have the group, system administration userid and password for MSSMGn.

Refer to "Reference figures for restoring an MDM Server in a secured network" (page 119) for the sequence of operations performed in the procedure steps.

Reference figures for restoring an MDM Server in a secured network



CAUTION
Incorrect command syntax may result in deletion of wrong IPSec information.
Incorrect syntax or failure to include required parameters in the ipsec_deletesa command may result in deletion of the wrong security association information. Review the ipsec_deletesa command carefully before executing.

Step	Action

1 Refer to "Reference figures for restoring an MDM Server in a secured network" (page 119), figure A. The MDM Server has had a complex failure requiring a disk restore.

- All fault, performance and security data from the MSS/MG15000 switches flows through MDM1.
- All management access to MSS/MG15000 switches is through MDM1.
- IEMS central AAA is operational for MDM1 and MSS/MG15000 switches.

2 Refer to "Reference figures for restoring an MDM Server in a secured network" (page 119), figure B. The MDM Server has been restored from a backup taken when the Server was fully secured.

- SSH link to IEMS remains operational.
- Authentication link from MDM2 to IEMS remains operational.
- MDM Server platform remains hardened.
- IPSec links between MDM1 and MDM2 and between MDM2 and the MSS/MG15000 switches are not operational.
- MDM2 has not been synchronized with MDM1.

3 Refer to "Reference figures for restoring an MDM Server in a secured network" (page 119), figure C. Restore the IPSec link between MDM2 and MDM1. This requires deletion of the existing security associations and creation of new ones for the link.

- Refer to the IPSec configuration record for the configuration information for the security associations between MDM1 and MDM2.
- Delete the SAs for the link between MDM2 and MDM1.
  - — See "Preparing to delete IPSec configuration data" (page 130).

— On MDM2, remove the security association information for the link to MDM1. Use the parameter information obtained in the previous step.

```
/opt/MagellanNMS/bin/ipsec_deletesa <MDM1_Ipaddr>
-inSPI <x> -outSPI <y>
```

Note: Review the syntax of the command carefully before executing to make sure that all parameter keywords and values are correctly specified.

The following figure shows a sample output for the ipsec_deletesa command.

Sample output for the ipsec_deletesa command

```
#/opt/MagellanNMS/bin/ipsec_deletesa 10.35.16.2 -inSPI 506
-outSPI 507
peerAddr 10.35.16.2
localAddr 10.47.0.5
inSPI 506
outSPI 507
#--------------------Provisioning the Workstation----------------------#
Deleting the following policy:
#INDEX 90 {saddr 10.47.0.5 daddr 10.35.16.2 } apply {
encr_algs aes sa shared}
Deleting the following policy:
#INDEX 89 {saddr 10.35.16.2 daddr 10.47.0.5 } permit {
encr_algs aes }
/usr/sbin/ipseckey delete esp spi 506 dst 10.47.0.5
/usr/sbin/ipseckey delete esp spi 507 src 10.47.0.5
Committing the IPSEC configuration on the workstation.
#----------------------Successful Execution---------------------------#
Run the following command on the peer workstation if not
already done.
/opt/MagellanNMS/bin/ipsec_deletesa -outSPI 506 10.47.0.5
10.35.16.2
```

Review the policy index numbers and SPIs output by the ipsec_deletesa command and verify that the correct policies have been deleted.

Note: If the wrong policies have been deleted, do not continue with this procedure. Re-check the command syntax and parameters. Restore the IPSec configuration files before re-executing the procedure.

The last line of the ipsec_deletesa command output is the command to be executed on MDM1.

— On MDM1, execute the command output by the previous step to remove the corresponding security associations for the link.

Review the policy index numbers output by the ipsec_deletesa command and verify that the correct policies have been deleted.

Note: If the wrong policies have been deleted, do not continue with this procedure. Re-check the command syntax and parameters. Restore the IPSec configuration files before re-executing the procedure.

- Create new SAs for the link between MDM1 and MDM2. Follow the procedures in "Securing an MDM to MDM connection with IPSec" (page 39).
- When the IPSec link between MDM1 and MDM2 is operational, synchronize the MDM Servers. For more information, see NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP.

4 Refer to "Reference figures for restoring an MDM Server in a secured network" (page 119), figures D, E, F. Restore the IPSec link between MDM2 and MSSMGn. This requires deletion of the security associations for the link on MDM2 and on the MSS/MG15000 switch before creation of new ones for the link. Repeat this step for every MSS/MG15000 switch 1 to n.

- See "Preparing to delete IPSec configuration data" (page 130).
- On MDM2, remove the security associations for the ftp-data channel between MDM2 and MSSMGn.

```
/opt/MagellanNMS/bin/ipsec_deletesa <MSSMGn_IPaddr>
-inSPI <MSSMGn_ftp_inSPI> -outSPI <MSSMGn_ftp
_outSPI> -destPort ftp-data -pp <MDM1_IPaddr>
<MSSMGn_group> <MSSMGn_userid> <MSSMGn_pwd>
```

Note: Review the syntax of the command carefully before executing to make sure that all parameter keywords and values are correctly specified.

Review the index numbers and SPIs output by the ipsec_deletesa command and verify that the correct policies have been deleted.

Note: If the wrong policies have been deleted, do not continue with this procedure. Re-check the command syntax

and parameters. Restore the configuration files before executing the procedure again.

As the other end of the link is on an MSS/MG15000 switch, ignore the instruction at the end of the command output.

- On MDM2, remove the security associations for the other channels between MDM2 and MSSMGn:

```
/opt/MagellanNMS/bin/ipsec_deletesa
<MSSMGn_IPaddr> -inSPI <MSSMGn_oth_inSPI>
-outSPI <MSSMGn_oth_outSPI> -pp
<MDM1_IPaddr> <MSSMGn_group> <MSSMGn_userid>
<MSSMGn_pwd>
```

Note: Review the syntax of the command carefully before executing to make sure that all parameter keywords and values are correctly specified.

Review the index numbers and SPIs output by the ipsec_deletesa command and verify that the correct policies have been deleted.

Note: If the wrong policies have been deleted, do not continue with this procedure. Re-check the command syntax and parameters. Restore the IPSec configuration files before re-executing the procedure.

As the other end of the link is on an MSS/MG15000 switch, ignore the instruction at the end of the command output.

- Create new security associations for the link between MDM2 and MSSMGn. On MDM2, execute the following command:

```
pp_ipsecsetup <MSSMGn_IPaddr> -Rad1
<IEMS_IPaddr> -pp <MDM1_IPaddr>
<MSSMGn_group> <MSSMGn_userid> <MSSMGn_pwd>
```

5 Test that all the IPSec links between MDM2 and the MSS/MG15000 switches are operational.

—End—

This is the end of the procedure for "Restoring an MDM Server in a secured network" (page 117).

Restoring an MSS/MG15000 switch in a secured network

When an MSS/MG15000 switch is restored from backup, the security association information on the switch may be out of synchronization with the rest of the security domain. To restore the IPSec links to the other network elements, the existing IPSec configuration data must be deleted before new security associations are created.

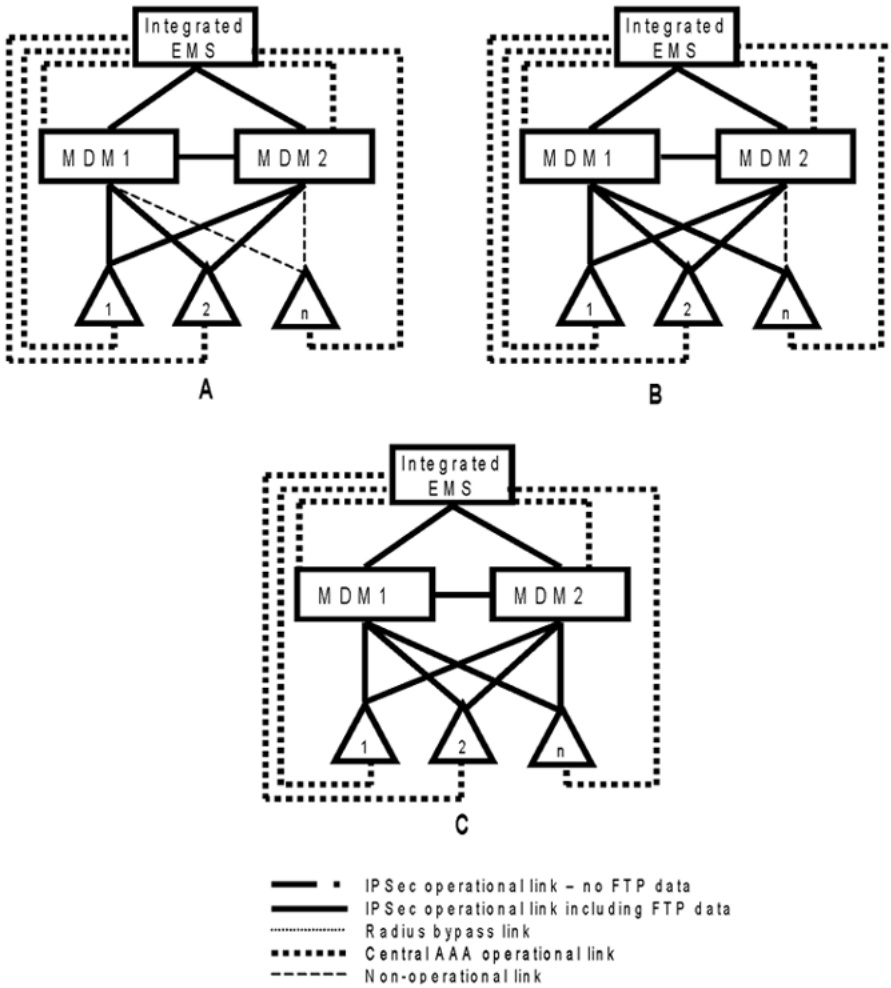
Prerequisites

Before using the following procedure:

- Restore the MSS/MG15000 switch from a backup taken when the switch was fully secured.
- Designate the MDM Servers MDM1 and MDM2.
- Designate the recovering MSS/MG15000 switch as MSSMGn.
- Ensure the IPSec configuration record is available.
- Be able to log into MDM1 and MDM2 as root.
- Have the group, system administration userid and password for MSSMGn.

Refer to "Reference figures for restoring an MSS/MG15000 switch in a secured network" (page 125) for the sequence of operations performed in the procedure steps.

Reference figures for restoring an MSS/MG15000 switch in a secured network



CAUTION
Incorrect command syntax may result in deletion of wrong IPSec information.
Incorrect syntax or failure to include required parameters in the ipsec_deletesa command may result in deletion of the wrong security association information. Review the ipsec_deletesa command carefully before executing.

Step	Action
1	Refer to "Reference figures for restoring an MSS/MG15000 switch in a secured network" (page 125), figure A. The MSS/MG15000 switch has had a complex failure requiring a disk restore.

- All fault, performance and security data from the other MSS/MG15000 switches continues to flow through MDM1 and MDM2.
- All management access to the other MSS/MG15000 switches is through MDM1 and MDM2.
- The RADIUS client is still configured to exchange authentication data with IEMS.

2 Delete the SAs for the IPSec links between the MDM Servers (MDM1 and MDM2) and MSSMGn. This requires deleting the security associations on the MDM Servers and on the MSS/MG15000 switch.

- Delete the four SAs on MDM1 for the link to MSSMGn.
  - See "Preparing to delete IPSec configuration data" (page 130).
  - On MDM1, execute the following commands to remove the security associations for the link to MSSMGn.

    Note: Review the syntax of the ipsec_deletesa commands carefully before executing to make sure that all parameter keywords and values are correctly specified.

    To remove the ftp-data channel security associations, execute:

    ```
    /opt/MagellanNMS/bin/ipsec_deletesa
    <MSSMGn_IPaddr> -inSPI <MDM1_ftp_inSPI>
    -outSPI <MDM1_ftp_outSPI> -destPort ftp-data
    ```

    To remove the security associations for the other data channels, execute:

    ```
    /opt/MagellanNMS/bin/ipsec_deletesa
    <MSSMGn_IPaddr> -inSPI <MDM1_oth_inSPI>
    -outSPI <MDM1_oth_outSPI>
    ```

    Review the index numbers output by the ipsec_deletesa commands and verify that the correct policies have been deleted.

    Note: If the wrong policies have been deleted on the MDM Server, do not continue with this procedure. Re-check the command syntax and parameters. Restore the IPSec configuration files before re-executing the procedure.

    As the other end of the link is on an MSS/MG15000 switch, ignore the instruction at the end of the command output.
- Delete the four SAs on MDM2 for the link to MSSMGn.

— See "Preparing to delete IPSec configuration data" (page 130).

— On MDM2, execute the following commands to remove the security associations for the link to MSSMGn.

Note: Review the syntax of the ipsec_deletesa command carefully before executing to make sure that all parameter keywords and values are correctly specified.

To remove the ftp-data channel security associations, execute:

```
/opt/MagellanNMS/bin/ipsec_deletesa
<MSSMGn_IPaddr> -inSPI <MDM2_ftp_inSPI>
-srcPort ftp-data -outSPI <MDM2_ftp_outSPI>
-destPort ftp-data
```

To remove the security associations for the other data channels, execute:

```
/opt/MagellanNMS/bin/ipsec_deletesa
<MSSMGn_IPaddr> -inSPI <MDM2_oth_inSPI>
-outSPI <MDM2_oth_outSPI>
```

Review the index numbers output by the ipsec_deletesa command and verify that the correct policies have been deleted.

Note: If the wrong policies have been deleted on the MDM Server, do not continue with this procedure. Re-check the command syntax and parameters. Restore the IPSec configuration files before re-executing the procedure.

As the other end of the link is on an MSS/MG15000 switch, ignore the instruction at the end of the command output.

- Delete the SAs on MSSMGn for the links with the MDM Servers. To do this, delete the security policy database.

Note: The IPSec policy database must be deleted by connecting directly to the serial port on the switch using a Vt100 terminal.

On MSSMGn, execute the following commands:

```
del Vr/0 Ip Spd/1

check prov

activate prov

confirm prov
```

```
commit prov
```

3 Refer to "Reference figures for restoring an MSS/MG15000 switch in a secured network" (page 125), figures B and C. Create new security associations between MDM1, MDM2 and MSSMGn. Use the procedure "Securing links between MDM1 and MSS/MG15000 network elements" (page 59).

—End—

This is the end of the procedure for "Restoring an MSS/MG15000 switch in a secured network" (page 124).

Adding an MSS/MG15000 switch to a secured network

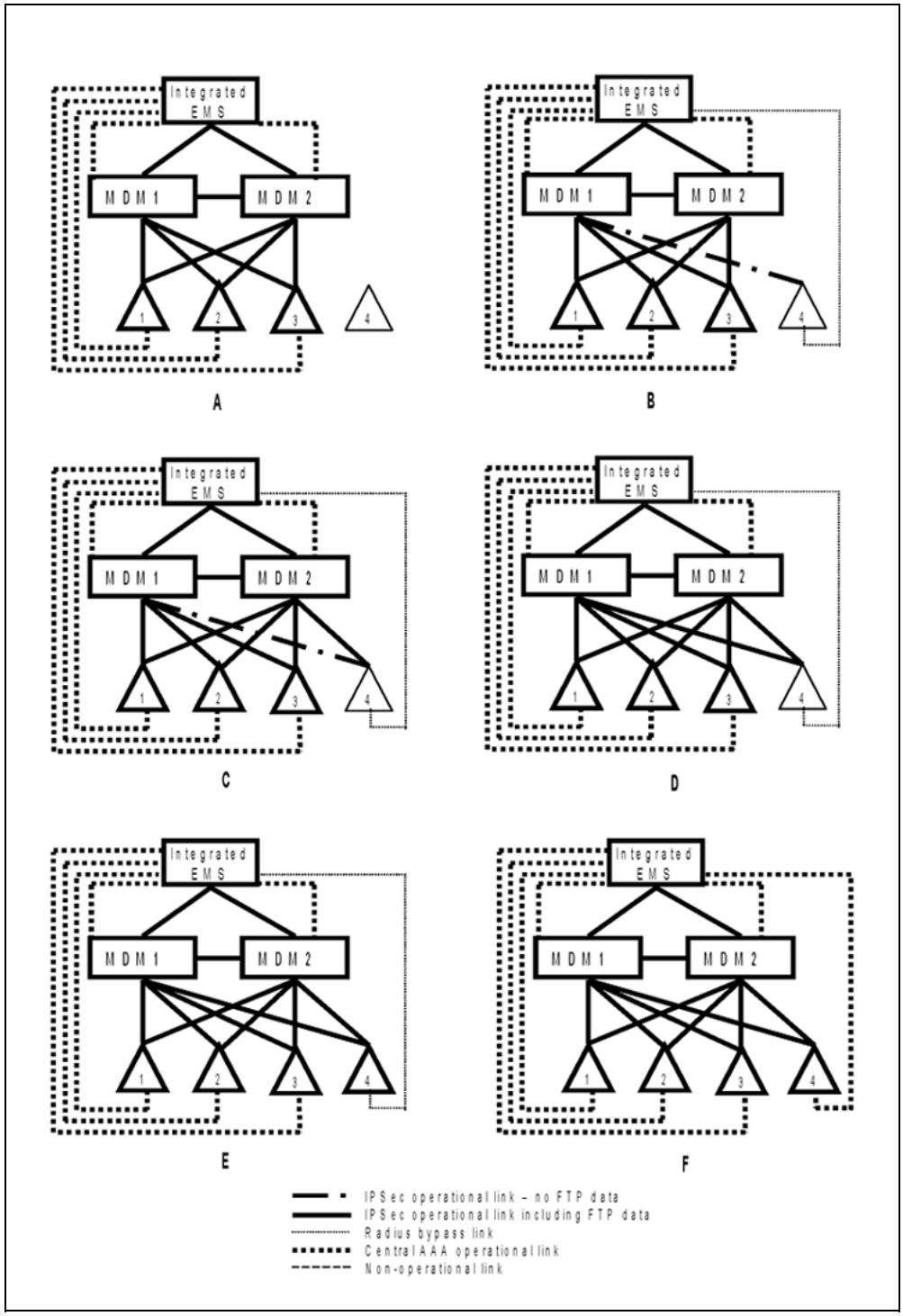
Prerequisites

Before using the following procedure:

- Ensure the new switch has migrated to SN08.
- Designate the MDM Servers MDM1 and MDM2.
- Designate the new MSS/MG15000 switch MSSMGn.
- Define the new IPSec security associations required between MSSMGn and MDM1 and MDM2, and record them in the IPSec configuration record.
- Be able to log into MDM1 and MDM2 as root
- Have the group, system administration userid and password for MSSMGn.

Refer to "Reference figures for adding an MSS/MG15000 switch to a secured network" (page 129) for the sequence of operations performed in the procedure steps.

Reference figures for adding an MSS/MG15000 switch to a secured network



Step	Action
1	Refer to "Reference figures for adding an MSS/MG15000 switch to a secured network" (page 129), figure A. Install the IPSec software on the switch using the procedure "Installing IPSec software on an MSS/MG15000 switch" (page 57).
2	Refer to "Reference figures for adding an MSS/MG15000 switch to a secured network" (page 129), figures B, C and D. Use the procedures in "Securing links between MDM Servers and MSS/MG15000 switches using IPSec" (page 55) to configure the IPSec security associations between MDM1, MDM2 and MSSMGn. Where commands are to be repeated for multiple MSS/MG15000 switches, execute only once for MSSMGn.
3	Refer to "Reference figures for adding an MSS/MG15000 switch to a secured network" (page 129), figure E. Harden the MSSMGn platform. Use the procedures in "Hardening the Multiservice Switch 15000 or Media Gateway 15000 platform" (page 85).
4	Refer to "Reference figures for adding an MSS/MG15000 switch to a secured network" (page 129), figure F. Configure MSSMGn to use the IEMS central AAA service. Use the procedures in "Migrating MSS/MG15000 userids to IEMS" (page 99).
	—End—

This is the end of the procedure for "Adding an MSS/MG15000 switch to a secured network" (page 128).

Preparing to delete IPSec configuration data

Failure to use the correct syntax and supply all the required parameters for the ipsec_deletesa command may result in the wrong security association information being deleted. Before using the ipsec_deletesa command, execute the following steps.

Step	Action
	Using a secure connection to the MDM Server and MSS/MG15000 switch
1	Before deleting any security information on an MDM Server, backup the following files in case the security information needs to be restored: • /etc/inet/ipsecinit.conf • /etc/inet/secret/ipseckeys

2 Before deleting any security information on an MSS/MG15000 switch, retain the name of the current provisioning view in case the security information needs to be restored.

3 On the MDM Server, display all the IPSec configuration information. See "Viewing MDM IPSec information" (page 133). Determine the security policy index numbers, IP addresses, SPIs and port data type, if specified, for the link. Retain the complete IPSec configuration information to be used later to verify that the correct security associations were deleted.

4 If deleting security information on an MSS/MG15000 switch, display the full IPSec configuration information. See "Viewing MSS/MG15000 IPSec information" (page 131). Retain the complete IPSec configuration information to be used later to verify that the correct security associations were deleted.

—End—

This is the end of the procedure for "Preparing to delete IPSec configuration data" (page 130).

Viewing MSS/MG15000 IPSec information

Use the following procedure to view IPSec configuration information on an MSS/MG15000 switch.

Step	Action

Using a secure desktop connection to the MSS/MG15000 switch

1 Log in as system administrator.

2 Display all the security policies defined on the switch, showing the direction of data flow and the associated source IP address and destination IP address:

```
display -p Vr/0 Ip Spd/1 Policy/*
```

Sample command output

```
> display -p Vr/0  Ip Spd/1 Policy/*
Vr/0 Ip Spd/1 Policy/*
Use -noTabular to see hidden attributes: description and action.
+======+--------------+--------------+-----+-------+-------+-----
|Policy| sAddr        | dAddr        |proto| sPort |dPort  |direction
+======+--------------+--------------+-----+-------+-------+-----
| 10010|47.135.48.80   |47.138.183.103 | any | any   | ftpdat|in
| 10020|47.138.183.103 |47.135.48.80   | any | ftpdat| any   |out
| 30010|47.135.48.80   |47.138.183.103 | any | any   | any   |in
| 30020|47.138.183.103 |47.135.48.80   | any | any   | any   |out
```

A pair of in/out entries with reciprocal source and destination addresses and matching source and destination ports constitutes a security association pair. The policy ids are used in the next step to determine the SPIs.

3 Display the *inSPI, outSPI,* encryption algorithm and authentication algorithm for the security associations:

```
display -p Vr/0 Ip Spd/1 Policy/* Sa/*,*,* man
```

Sample command output

```
> display -p Vr/0 Ip Spd/1 Policy/* Sa/*,*,* Man
Vr/0 Ip Spd/1 Policy/* Sa/*,*,* ManEspSa
+======+===============+=========+=======+-------+----
|Policy|secDestination |secProto |spiALg |encAlg |auth
+======+===============+=========+=======+-------+----
| 10010|47.135.48.80   |     esp |    294|   none|sha1
| 10020|47.138.183.103 |     esp |    293|   none|sha1
| 30010|47.135.48.80   |     esp |    400|   aes |sha1
| 30020|47.138.183.103 |     esp |    296|   aes |sha1
```

Note: The security keys cannot be displayed.

4 Using the policy id, direction and port information from step 2 and 3, determine the *inSPI* and *outSPI* for the security association pair. The following table shows the security associations on the MSS/MG for the sample command output.

—End—

Security association information from the sample command output

NE	direction	src IP addr	dest IP addr	in-SPI	out-SPI
MSG	in	47.135.48.80 (MDM)	47.138.183.103 (MSSMG)	294	
MSG	out	47.138.183.103 (MSSMG)	47.135.48.80 (MDM)		293

This is the end of the procedure for "Viewing MSS/MG15000 IPSec information" (page 131).

Variable values

Variable	Value
<Vr/0>	The management virtual router. This Vr is used for handling OAM traffic to the nodes. This includes TCP sessions such as FMIP, telnet, or FTP, and UDP traffic such as NTP time synchronization with the Multiservice Data Manager workstations.
<x>	The instance value of the policy for inbound or outbound traffic.
<y>	The security parameter index (SPI) for the security association.
<a.b.c.d>	The IP address for the security association.

Viewing MDM IPSec information

When an IP packet is received, the IPSec security association index file is scanned to determine if any encryption is applicable based on the source address (saddr) and destination address (daddr) in the packet. If a valid address match is found, the data type (IP, udp, icmp) of the source or destination port (ftp-control, ftp-data, etc) is checked. When a match is found, the action (permit, apply, bypass) is applied to the encryption rule enclosed in braces. The encryption information is used to search the IPseckey.conf file to determine the SPI and encryption key to be used to validate the security association.

Use the following procedure to view IPSec configuration information on an Multiservice Data Manager Server.

Step	Action
	Using a secure desktop connection to the MDM Server
1	Log in as root.
2	Execute the following command to display the IPSec security association index file:

ipsecconf

Sample output for ipsecconf command

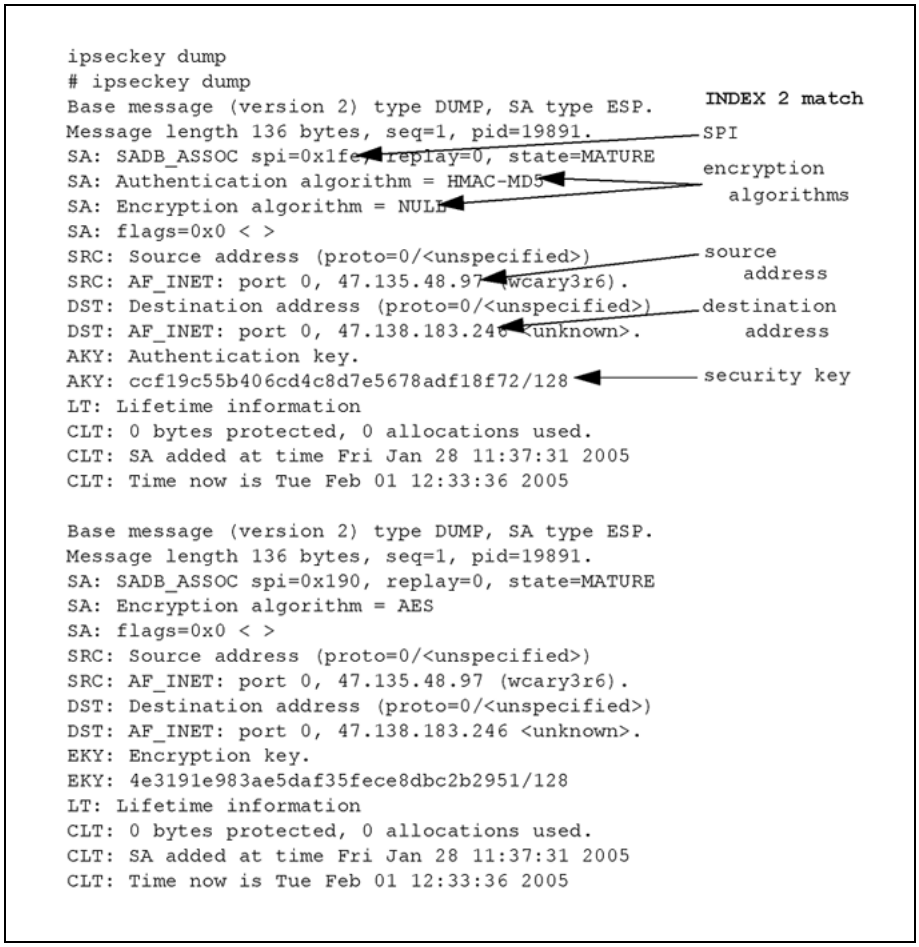
```
ipsecconf
#INDEX 1
{saddr 47.138.183.246 daddr 47.135.48.97 dport ftp-data } permit {
encr_algs NULL encr_auth_algs md5 }
#INDEX 2
{saddr 47.135.48.97 daddr 47.138.183.246 sport ftp-data } apply {
encr_algs NULL encr_auth_algs md5 sa shared}
#INDEX 3
{saddr 47.128.153.8 daddr 47.135.48.97 } permit { encr_algs NULL
encr_auth_algs sha }
#INDEX 4
{saddr 47.135.48.97 daddr 47.128.153.8 } apply { encr_algs NULL
encr_auth_algs sha sa shared}
#INDEX 5
{saddr 47.138.183.246 daddr 47.135.48.97 } permit { encr_algs aes }
#INDEX 6
{saddr 47.135.48.97 daddr 47.138.183.246 } apply { encr_algs aes sa
shared}
```

A pair of in/out entries with reciprocal source and destination addresses, matching source and destination ports, and matching algorithms constitutes a security association pair. The source and destination addresses and the encryption algorithms are used in the next step to determine the SPIs and security keys.

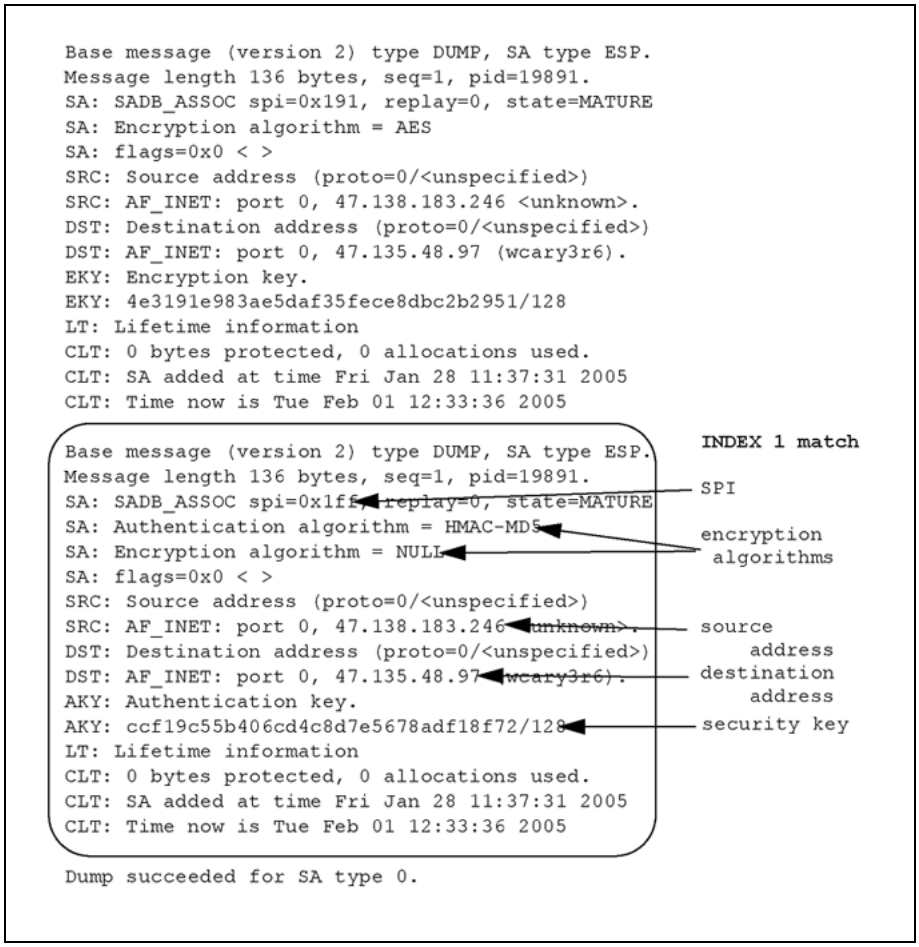
3 Execute the following command to display the information in the IPseckey.conf file:

ipseckey dump

Sample output for the ipseckey command, part 1



Sample output for the ipseckey command, part 2



Using the source and destination addresses and the encryption and authentication algorithms, locate the ipseckey.conf record that matches the security association index record.

Note: The SPI value is displayed in hexadecimal format and must be converted to decimal format for use in commands.

—End—

This is the end of the procedure for "Viewing MDM IPSec information" (page 133).

Carrier VoIP

MSS15K, MG15K and MDM in Carrier VoIP Networks - Securing Network Elements

Publication: NN10180-612
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.