



ATM/IP Solution-level Security and Administration

ATTENTION

This document addresses all Nortel Networks Succession solutions. Some statements may not apply to your solution. The North American IAW solution is not included in the (I)SN08 release.

Solutions

This document describes security and administration for the following solutions.

Solution name	
International IP solutions	Integrated Access Wireline (IAW)
	Integrated Access-Cable Media (IAC)
	Packet Transit-IP (PT-IP)
	Universal Access-IP (UA-IP)
International ATM solutions	Packet Transit-AAL2 (PT-AAL2)
North American IP solutions	Packet Trunking-IP (PT-IP) or Packet Trunking-AAL2 (PT-AAL2)
	Integrated Access-Cable Media (IAC)
	Universal Access-IP (UA-IP)
North American ATM solutions (see Note)	Universal Packet Access (UA-AAL1)

Solution name
Packet Trunking-AAL1 (PT-AAL1) There are three distinct architectures supported within the PT-AAL1 solution: - Packet Trunking-AAL1 (PT-AAL1) - Packet Trunking on XA-Core (PT-XA Core) - Packet Trunking on SN70EM (PT-SN70) Note: Collectively, these two Succession solutions are referred to as ATM solutions.

What's New

The following table highlights the features introduced in this release. Refer to the OSS Advanced Feature Guide for more information about new features in this release.

Note: The terms Passport and PVG have been re-branded in conjunction with the new Nortel Networks brand simplified format. Passport is now referred to as the Nortel Networks Multiservice Switch and PVG is now Media Gateway 7480/15000. Passport 8600 is now referred to as Ethernet Routing Switch 8600. The term Passport Preside MDM has been re-branded in conjunction with the new Nortel Network's brand simplified naming format. MDM is now referred to as the Nortel Networks Multiservice Data Manager.

(I)SN08 features (Sheet 1 of 4)

Feature descriptions
PP8600 and Integrated EMS feature A00006757 -- IEMS secure launch to Ethernet Routing Switch 8600

(I)SN08 features (Sheet 2 of 4)**Feature descriptions**

This feature defines security measures that are applied to communications between VoIP management applications and the Passport 8600 Routing Switch. The management applications include Integrated EMS and the PP8600 graphical configuration and management tool known as the Device Manager. All communications between OAM applications and the Ethernet Routing Switch 8600 must be authenticated and encrypted. The means for doing this are provided by SNMPv3 and SSHv2.

Configuration is required for Integrated EMS, Ethernet Routing Switch 8600, and Device Manager. The configuration in the Ethernet Routing Switch 8600 must be completed before the configuration of Integrated EMS or Device Manager. There is no interaction between Integrated EMS and Device Manager, hence, the configuration of one is independent of the other.

(I)SN08 features (Sheet 3 of 4)**Feature descriptions****CS 2000 features****A00006979 - Centralized synchronization and Backup Manager (PT-IP, UA-AAL1, UA-IP, Int'l IAW)**

This feature provides a centralized mechanism that allows the user to initiate a synchronous backup for the core components of the Call Server. Providing this capability reduces the possibility of error caused by manual backup procedures on the various component platforms spread across the Call Server solution.

In (I)SN08, the Backup Manager will provide synchronous centralized control of the backup functionality resident within the following Call Server components:

- CS 2000 Management Tools server
- MG9000 Element Manager server
- Supernode Data Manager (SDM) / Core Billing Manager (CBM) server
- Integrated Element Management System server
- Session Server

A00007300 - IPSEC integration with PVG, MG9K and RTP Portal (PT-IP, UA-IP)

This feature enables IPsec on all GWC profiles that do not currently have the IPsec capability. As a result of enabling IPsec on all remaining GWC profiles, the IPsec provisioning tab will now be available in the CS 2000 Management Tools GUI for all GWC profiles.

Integrated EMS feature**A00006348- Secure centralized user accounts in IEMS**

This feature addresses the following components of the SSPFS.

- HTTP proxy servlet. This component provides reliability to the http proxy servlet (that performs login authentication for numerous clients) so clients will not be shut out for long periods of time and deals with the clustered SSPFS machine only. The following clients use the proxy for authentication: Integrated EMS, CICM EM, APS, USP.
- Security keys. This feature ensures that the security keys that are managed by the SSPFS have the correct permissions. This feature will ensure that the directory that the keys are stored in are located in have their permissions set correctly

(I)SN08 features (Sheet 4 of 4)**Feature descriptions****A00006756 - IEMS Security enhancements**

This feature introduces enhancements to Integrated EMS security. The feature implements NSSwitch (Name Service Switch) in Integrated EMS. NSSwitch is a standard used in all Unix flavor operating systems, founded by Sun Micro Systems. The OS uses a number of databases of information about hosts, users (passwd/shadow), and groups. Data for these hostnames and addresses can be found in /etc/hosts, NIS, NIS+ or DNS.

A00007786 - IEMS Config Radius secret

The Integrated EMS currently requires provisioning of network elements, element managers, EMS platforms or EMS applications in one step. RADIUS secrets are provisioned through the CLI in a second step. This feature allows the user to provision RADIUS secrets directly through the Integrated EMS and in one step, eliminating the need of the CLI for RADIUS secrets. Integrated EMS will allow RADIUS secrets to be added, modified, and deleted from the Security Server. The purpose of this feature is to maintain the current functionality of all NEs, EMs, platforms, and applications from (I)SN07 and to add the ability to handle RADIUS secret provisioning.

SDM feature**A00007491 - System intrusion and file integrity detection**

This feature monitors the files on the SDM and records file change events to log files. File change events will be logged to one of two log files, auditlog, and securitylog. File changes resulting from regular configuration changes will be recorded in the auditlog file. File changes which are abnormal will be recorded in the securitylog file.

A00007489-Integration of SDM user authentication with the IEMS

This feature is designed to support SDM integration with Integrated EMS. It provides the following security functionality:

- Utilize the centralized security management of Integrated EMS to provide Authentication, Authorization, and Accounting (AAA) functions.
- Support PAM on SDM to allow AAA via Integrated EMS.
- Allow local emergency access when communication to Integrated EMS is down.
- Support AAA through local security management when Integrated EMS is not part of the SDM deployment.
- Enable access control based on user authorization.

Overview of Security Architecture

The network security architecture for the CVoIP solutions uses Internet Protocol Security (IPSec) to protect the traffic between several network devices. This section describes some basic concepts related to the IPSec services used in the network.

Note: For more detailed IPSec information, refer to the appropriate Internet Engineering Task Force (IETF) RFC documentation, which can be found at <http://www.ietf.org>.

IPSec services

IPSec offers a set of security services that provide data integrity, authentication, and confidentiality (encryption). These services are provided through the use of traffic security protocols. In this solution only the ESP (Encapsulating Security Payload) traffic security protocol is supported.

Security associations

IPSec services are defined and executed through security associations (SA). An SA is a one-way relationship between two secure network elements. The SA is negotiated and it describes how two network components will use IPSec to communicate securely. To create bi-directional communication between the two network elements, two IPSec SAs must be created (one in each direction). SAs specify security parameters, such as, the IPSec protocol (ESP), the authentication and encryption algorithm, the keys, the lifetime of the keys and the lifetime of the SA.

Supported paths

IPSec is used to secure the following network paths:

- Gateway Controllers (GWCs) to a Cable Modem Termination System (CMTS), third-party Trunk Gateway Control Protocol (TGCP) gateways, or a Multimedia Terminal Adapter (MTA) line gateway (IAC solutions only)
- Media Gateway 9000 (MG 9000) to MG 9000 Manager and GWCs (UA-IP solutions only)

Note: Secure File Transfer Protocol (SFTP) or IPSec secures the FTP client on the MG 9000. IPSec also secures basic packet filtering on the MG 9000.

- Media Gateway 7400/15000 or Multiservice Switch 15000 to MDM devices and GWCs (PT-IP and UA-IP solutions only)

- MDM devices to MDM devices (PT-IP and UA-IP solutions only)

Note: SSH also secures the interface between two MDM devices. In addition, SSH provides the following functionality:

- secures the interface between MDM and Integrated EMS
 - provides a secure, one-hop interface between the Integrated EMS client desktop and MDM
 - secures the interface between the Integrated EMS client desktop and Media Gateway 7400/15000 or Multiservice Switch 15000 CLUI access from MDM
- Call processing interfaces to and from the RTP Media Portal

Key management protocols

IPSec SAs are negotiated and established by exchanging security keys using one of the following key management protocols:

- Internet Key Exchange (IKE)

IKE creates an authenticated secure communication channel between two devices. This association is called an IKE SA. IKE then uses this secure association to negotiate IPSec SAs. IKE consists of two phases:

- Phase 1: a shared secret is negotiated through a Diffie-Hellman key exchange (IKE SA is created)
- Phase 2: IKE SA is used to negotiate IPSec. Only pre-shared key authentication is supported in the network (digital signature authentication or public key encryption authentication are not currently supported for IKE).

- Kerberos

Kerberos with Public Key support (using the PKINIT extension to the Kerberos IETF standard) is used to exchange keys and authenticate line gateways. MTA authentication process with the GWC requires a PacketCable Key Distribution Center (KDC) server, which grants authentication tickets to the line gateway. These tickets are used to authenticate the line gateway, and to establish a pair of IPSec SAs. The KDC is third-party equipment and must be integrated with the network. For more information on Kerberos with PKINIT please refer to the packetcable security specification :
<http://www.packetcable.com/specifications>

Security connection policies

Connection policies define which security services will be applied to messages exchanged between two secure nodes in the network

(identified by the IP address). Each connection policy associates an IP address (or a range of IP addresses) to one of the following actions:

- **BYPASS:** no IPSec services are applied to packets exchanged between the two nodes.
- **SECURE:** before an SA is established, an incoming packet is discarded, and an outgoing packet triggers key negotiation process (using IKE or Kerberos). When an SA is established, IPSec is applied to all incoming and outgoing packets. Incoming packets are authenticated and decrypted; outgoing packets are authenticated and encrypted before being sent.
- **DISCARD:** all packets are discarded between the two nodes.
- **FLEX:** this type of policy is not secure. The FLEX policy must only be used temporarily during the initial activation or de-activation of IPSec, when some gateways associated with the connection policy operate in a secure mode and some do not. The FLEX policy provides the flexibility of accepting secure and non-secure messages, so IPSec can be activated without a loss of service.

Each connection policy is identified by a policy ID number. The lower this number is, the greater is the priority of the policy.

Configuring the network with security

Purpose of this procedure

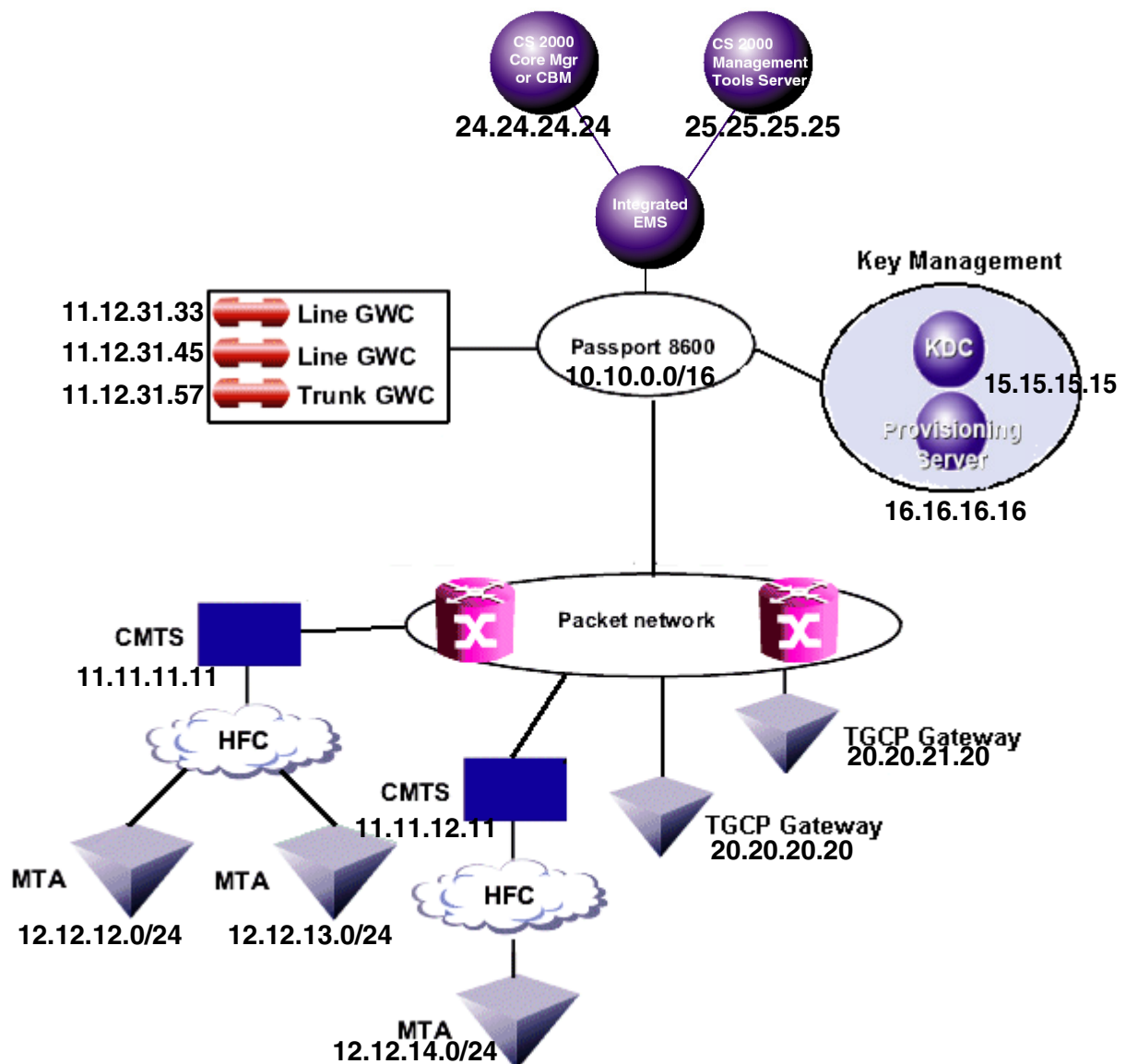
This procedure provides a high-level overview of the steps necessary to configure IP Security (IPSec) for CVoIP solutions.

IAC solutions

The following figure illustrates a sample IAC network and its components that are involved in IPSec.

Note: For simplicity, not all network elements are represented.

Sample IAC network architecture



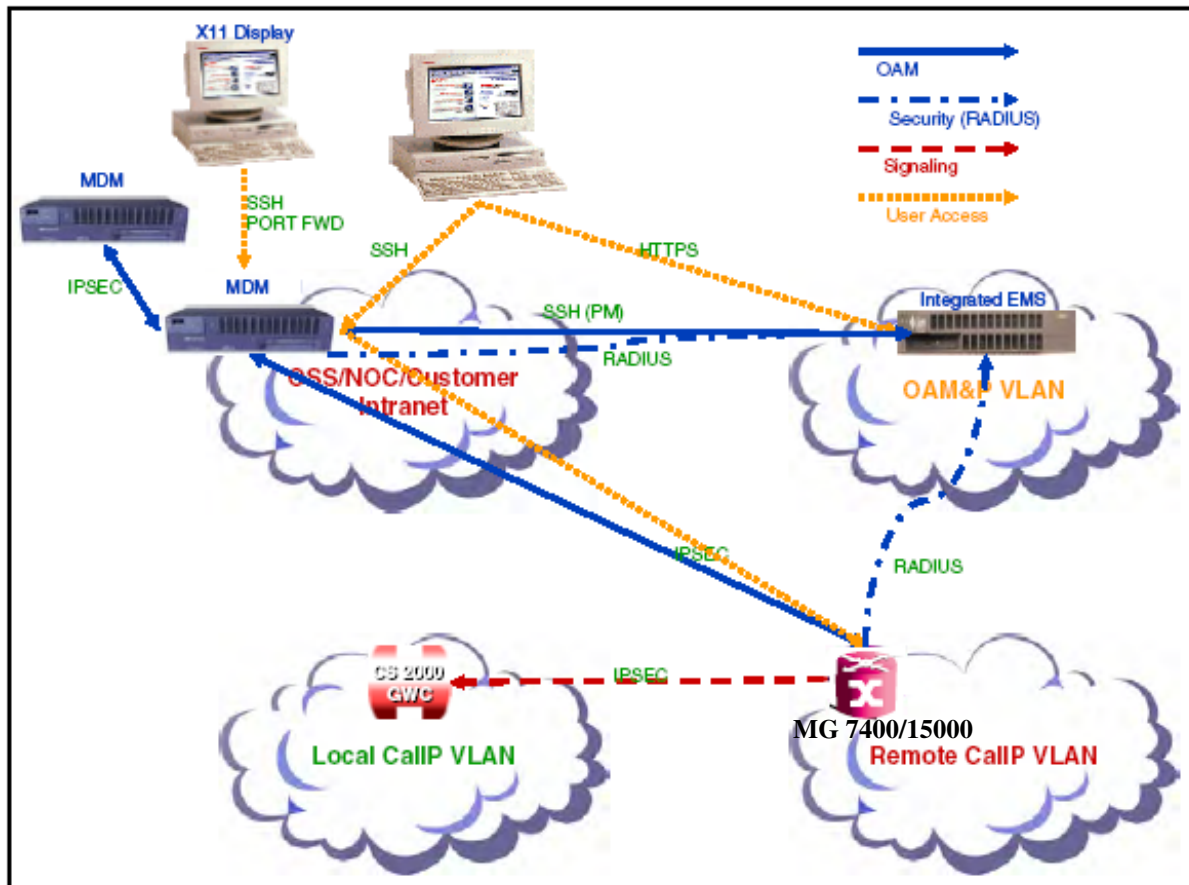
Identify all IP Addresses that need connect to the GWCs shown in the figure above. Populate the IPSEC Security Database using the following procedure.

PT-IP solutions

The following figure shows the (I)SN08 security architecture for the Media Gateway 7400/15000.

Note: For simplicity, not all network elements are represented.

Sample PT-IP network architecture

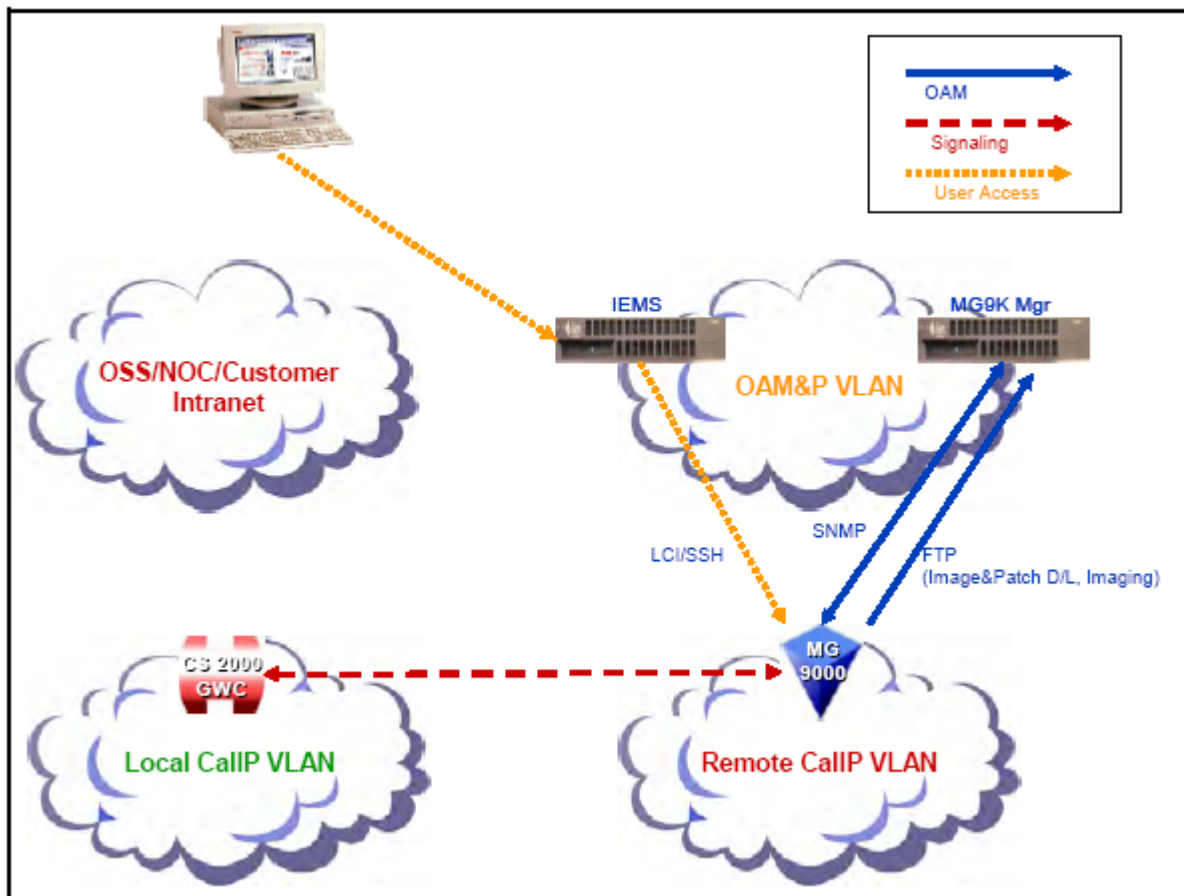


UA-IP solutions

The UA-IP solution supports the same security architecture for the Media Gateway 7400/15000 that is supported by PT-IP solutions. In addition, IPsec is supported for the MG 9000. The following figure shows the (I)SN08 security architecture for the MG 9000.

Note: For simplicity, not all network elements are represented.

Sample UA-IP network architecture



When to use this procedure

Use this procedure to create the initial IPSec policy table after the network has been upgraded to (I)SN08.

Prerequisites

The network must be upgraded to (I)SN08.

IPSec has not been configured on any components.

You must have the IP addresses available for each node in the network.

Action

Enabling IPSec in the network

- 1 Determine your network configuration.

If you are operating a(n)	Do
IAC network	step 2
UA-IP network	step 9
PT-IP network	step 11

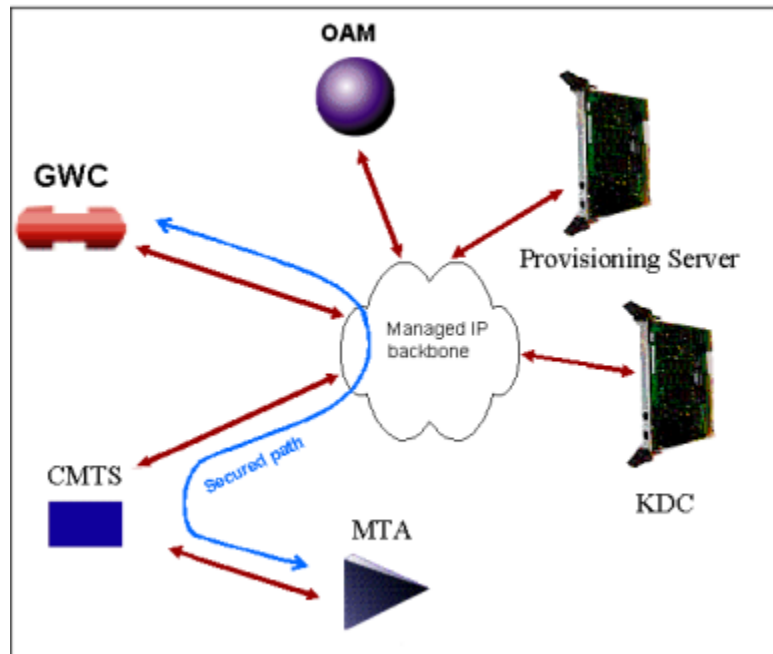
- 2 Configure a blanket DISCARD policy for all IP addresses: 0.0.0.0/1. Refer to the procedure "Configure a DISCARD connection policy" in *GWC Security and Administration*, NN10213-611.

- 3 Configure a BYPASS policy for the following IP addresses:
 - Range of IP addresses of the Passport 8600 or CS LAN
 - CS 2000 Core Manager or Core Billing Manager
 - CS 2000 Management Tools server

Refer to procedure "Configure a BYPASS connection policy" in *GWC Security and Administration*, NN10213-611.

- 4 Configure a Security policy for all network elements which require security.

- 5 To configure the MTA to Line GWC path for security, perform the following steps.

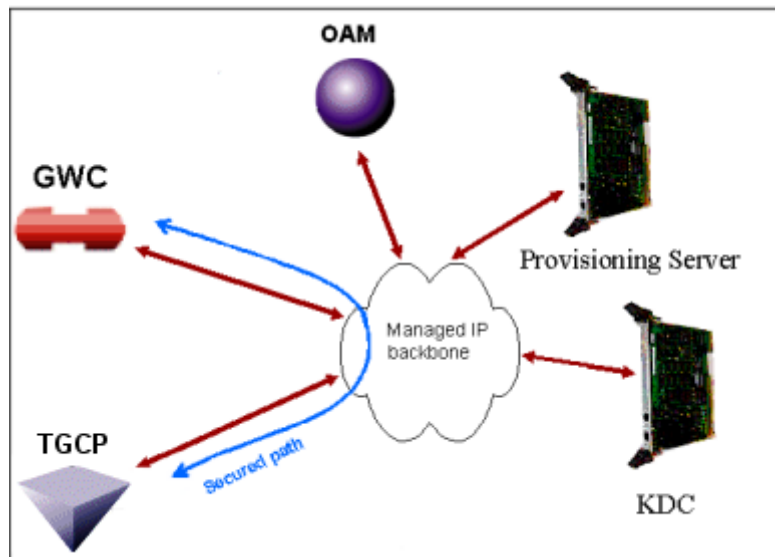
MTA to GWC path

- a Configure the GWC with Kerberos using the procedure "Configure Kerberos Key Management" located in *GWC Security and Administration*, NN10213-611.
- b Activate IPsec with Flex Policies using the procedure "Activating IPsec using Flex Policies" located in *GWC Security and Administration*, NN10213-611.

Note: Use the "Configure IPsec SECURE or FLEX connection policy with Kerberos" option in this procedure.

- 6 Secure the path from the TGCP GWs to the Trunk GWC by performing the following steps.

TGCP to GWC path

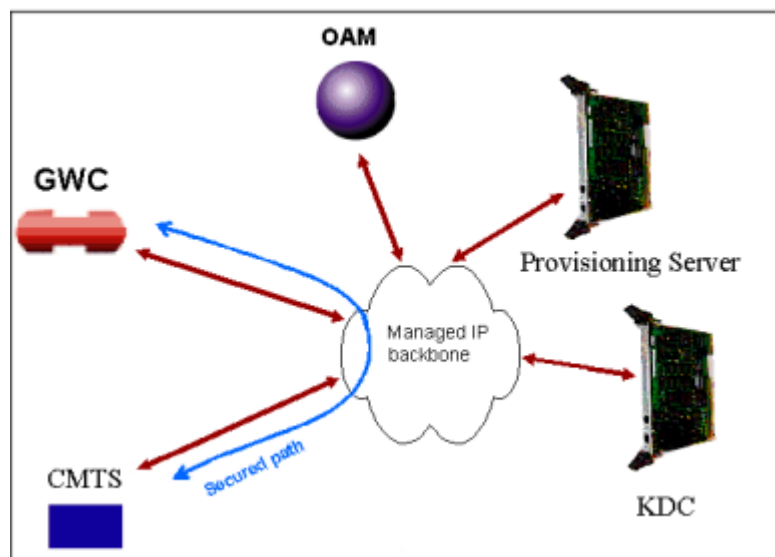


- a Activate IPSec with Flex Policies using the procedure "Activate or de-activate IPSec using FLEX policy" located in *GWC Security and Administration*, NN10213-611.

Note: Use the "Configure IPSec SECURE or FLEX connection policy with IKE" option in this procedure.

- 7 Secure the path from the CMTS to the Line GWC by performing the following steps.

CMTS to GWC path



- a Activate IPSec with Flex Policies using the procedure "Activate or de-activate IPSec using FLEX policy" located in *GWC Security and Administration*, NN10213-611.

Note: Use the "Configure IPSec SECURE or FLEX connection policy with IKE" option in this procedure.

- 8 Go to [step 12](#).
- 9 To secure the path between the MG 9000 and MG 9000 Manager, refer to the procedure "Setting up IPSec in the MG 9000 between the MG 9000 and MG 9000 Manager" in *MG 9000 Security and Administration*, NN10162-511.
- 10 To secure the path between the MG 9000 and the GWC, refer to the procedure "Setting up IPSec between the MG 9000 and the GWC" in *MG 9000 Security and Administration*, NN10162-511.
- 11 To secure the Media Gateway 15000 or MDM, refer to the following procedures in *Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Succession VoIP Networks Security and Administration - Securing Network Elements*, NN10180-612:
 - "Preparing to secure the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager network elements"
 - "Using SSH to secure X11 desktop and Integrated EMS connections with the MDM"
 - "Hardening the Multiservice Data Manager Server platform"
 - "Securing links between MDM Servers using IPSec"
 - "Securing links between MDM Servers and MSS/MG15000 switches using IPSec"
 - "Sending security audit logs from an MDM Server to Integrated EMS"
 - "Hardening the Multiservice Switch 15000 or Media Gateway 15000 platform"
 - "Securing user access for the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager components"
- 12 You have completed this procedure.

Deactivating Security in the network

Purpose of this procedure

This procedure provides a high-level overview of the steps necessary to deactivate IP Security (IPSec) in CVoIP solutions. This procedure does not disable security on any third-party devices. To deactivate security on third party devices, refer to the security documentation for the device.

Prerequisites

None

Action

Disabling IPSec in the network



CAUTION

Deactivating IPSec in the network will result in a loss of service until security has been deactivated on both network elements.

- 1 Determine your network configuration.

If you are operating a(n)	Do
IAC network	step 2
UA-IP network	step 4
PT-IP network	step 6
- 2 Identify all the network elements for which you want to deactivate security. Refer to the procedure "Activate or de-activate IPSec with FLEX policy" in GWC Security and Administration, NN10213-611.
- 3 Go to [step 7](#).
- 4 To remove the secure path between the MG 9000 and MG 9000 Manager, refer to the procedure "Removing IPSec between the MG 9000 and the MG 9000 Manager" in MG 9000 Security and Administration, NN10162-511.
- 5 To remove the secure path between the MG 9000 and the GWC, refer to the procedure "Removing IPSec between the MG 9000

and the GWC" in MG 9000 Security and Administration, NN10162-511.

- 6** To remove security on the Media Gateway 15000 or MDM, refer to procedure "Disabling security features on Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager components" in Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Succession VoIP Networks Security and Administration - Securing Network Elements, NN10180-612.
- 7** You have completed this procedure.

Backup and restore

Backup and restore operations for Succession solutions are performed at the component level. They are performed on the components at different intervals during periods of low service activity. No provisioning or configuration changes are to be made during the backup and restore window.

ATTENTION

Back up all related devices in the solution during the same window of time. No changes are allowed to any related devices during this period until all backups are completed or those changes will not be captured as part of the coordinated backup and would be lost in case of the need to restore the system. For example, the CS 2000, CS 2000 GWC Manager, and MG 9000 Manager all share line service data and must be backed up in the same window.

Correspondingly all related devices need to be restored together to return the system to a known state. No changes are allowed to the system until the restoration is completed or data mismatches will result.

Backup operations

There are two types of backup operations for components of Succession solutions: service data backup and fileset level backup.

Service data backup is typically performed once per day during a period of low activity. The following table lists components which are typically backed up using a service data backup.

Service data backup components

Component	Procedure (s)	Page
NETWORK INTELLIGENCE		
CS 2000	How to backup an XA-Core office image from disk to tape	102
Call Agent	Call Agent backup Backing up files to DVD-RW	114 117
SAM21	none (See Note 1)	
GWC	none (See Note 1)	

Service data backup components

Component	Procedure (s)	Page
Session Server	Perform a manual backup of the Session Server database Starting or stopping the automated synchronous backup restore manager service	127 95
Ethernet Routing Switch 8600	Saving the Ethernet Routing Switch 8600 boot configuration file	131
UAS	Backing up UAS configuration files	133
MS 2000 Series	Displaying the MS 2000 Series node configuration: Configuring automated INI file backups Changing the SNMP community string password for a Media Server 2010 node Changing the SNMP community string password for a Media Server 2020 node Backing up all MS 2000 Series node INI files: Backing up INI files for all nodes Configuring the MS 2000 Series CLUI tool: Displaying Media Server 2010 node current configuration Displaying Media Server 2020 node current configuration	136 138 142 146 148 151
APS	Backing up the APS-specific Oracle database and application files	154
USP	Administration: OAMP Workstation Backup	157
Real-time Transport Protocol (RTP) Media Portal	RTP Media Portal Basics, NN10367-111	
CICM	CICM Security and Administration, NN10252-611	
CORE NETWORK		
Multiservice Switch or Media Gateway devices	Backing up a Multiservice Switch or Media Gateway device	159
GATEWAYS		
MG 9000	none (See Note 1)	

Service data backup components

Component	Procedure (s)	Page
MG 4000	none (See Note 2)	
IW SPM	none (See Note 2)	
NETWORK MANAGEMENT		
CS 2000 Core Manager CBM	Starting or stopping the automated synchronous backup restore manager service	95
Core Element Manager	Starting or stopping the automated synchronous backup restore manager service	95
CS 2000 Management Tools	Performing a backup of oracle data on an SSPFS-based server	168
	Performing a backup of file systems on an SSPFS-based server	174
	Starting or stopping the automated synchronous backup restore manager service	95
Integrated Element Management System	Performing a backup of oracle data on an SSPFS-based server	168
	Performing a backup of file systems on an SSPFS-based server	174
	Starting or stopping the automated synchronous backup restore manager service	95
Integrated EMS centralized security server	Backing up the central security server	178
	Backing up an SSPFS-based security client	180
MG 9000 Manager	Performing a backup of oracle data on an SSPFS-based server	168
	Performing a backup of file systems on an SSPFS-based server	174
	Starting or stopping the automated synchronous backup restore manager service	95

Service data backup components

Component	Procedure (s)	Page
Preside MDM	none (See Note 3)	
Note 1: Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures. Note 2: Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up. Note 3: Preside MDM backups are performed by copying the files to tape or an off box storage system through UNIX commands or CRON jobs. Note 4: A script purgeTempData.sh is provided in the /opt/nortel/iems/current/bin directory. This script will purge all event, alarm and performance data from the Integrated EMS database. After purging the data it can't be retrieved. It deletes all events, alarms and performance data. To reduce the time taken to backup/restore, a user must stop the Integrated EMS server and execute the purgeTempData.sh script to purge the events, alarms and performance data from the database.		

Fileset level backups back up the software as well as configuration data. This type of backup is performed after hardware changes, software updates or patches, or major reconfigurations. Fileset backup also need to be performed before a major upgrade. The following table provides a list of components with fileset level backup procedures.

Fileset level backup components

Component	Procedure (s)	Page
NETWORK INTELLIGENCE		
GWC	Create a backup of the GWC load file	181
USP	Administration: Manual Backup	183
GATEWAYS		
Multiservice Switch or Media Gateway devices	Backing up a Multiservice Switch or Media Gateway device	159

Fileset level backup components

Component	Procedure (s)	Page
NETWORK MANAGEMENT		
CS 2000 Core Manager or CBM	Creating system image backup tapes (S-tapes) manually	185
	Configuring SBA backup volumes on the core	199
USP Manager	Administration: Creating Disaster Recovery Floppy Disks	216

Frequency of backup operations

The following table lists each component along with how often backup operations are recommended to be performed.

Component backup frequency

Component	Backup Frequency
NETWORK INTELLIGENCE	
CS 2000	Weekly
Call Agent	Weekly
SAM21	See Note 1
GWC	See Note 1
CS 2000 CS LAN	Full backup - monthly, and prior to all migrations and patch operations and configuration changes
UAS	Daily
MS 2000 Series	Daily
APS	Daily
RTP Media Portal	Daily
CICM	Daily
USP	Full system backup - once a week Modified (differential) backup - once a day

Component backup frequency

Component	Backup Frequency
CORE NETWORK	
Passport devices	Full backup - monthly, and prior to all migrations and patch operations
GATEWAYS	
MG 9000	See Note 1
MG 4000	See Note 2
IW SPM	See Note 2
NETWORK MANAGEMENT	
CS 2000 Management Tools	Daily
MG 9000 Manager	Daily
Integrated EMS	Daily
Preside MDM	Full backup - monthly, and prior to all migrations and patch operations Incremental backup - weekly
Note 1: Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures. Note 2: Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up.	

Synchronized Backup Manager overview

Synchronized Backup Manager description

Throughout this document, the backup restore functionality delivered under this feature is referred to in three distinct ways:

- Synchronous Backup Restore Manager (SBRM) refers specifically to the IEMS launched synchronized backup/restore software. The SBRM controls/synchronizes the backup related activities across other components/devices which contain related backup software.
- Device Backup Restore Manager (DBRM) refers specifically to the component-/device-level backup software which is controlled by the SBRM.
- Backup Restore Manager is a generic term encompassing both SBRM and DBRM functionalities and in general simply refers to the software which is common to both.

The feature provides a centralized mechanism that allows the user to initiate a synchronous backup for the core components of the Carrier VoIP Call Server. Providing this capability reduces the possibility of error caused by manual backup procedures on the various component platforms spread across the Call Server solution.

In (I)SN08, the Backup Manager will provide synchronous centralized control of the backup functionality resident within the following Call Server components

- CS 2000 Management Tools (CSMT) server
- MG9000 Manager (MG9K) server
- Supernode Data Manager (SDM) / Core Billing Manager (CBM) server. The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. no SDM/CBM data is backed up via the Backup Restore Manager software.
- Integrated Element Management System (Integrated EMS) server

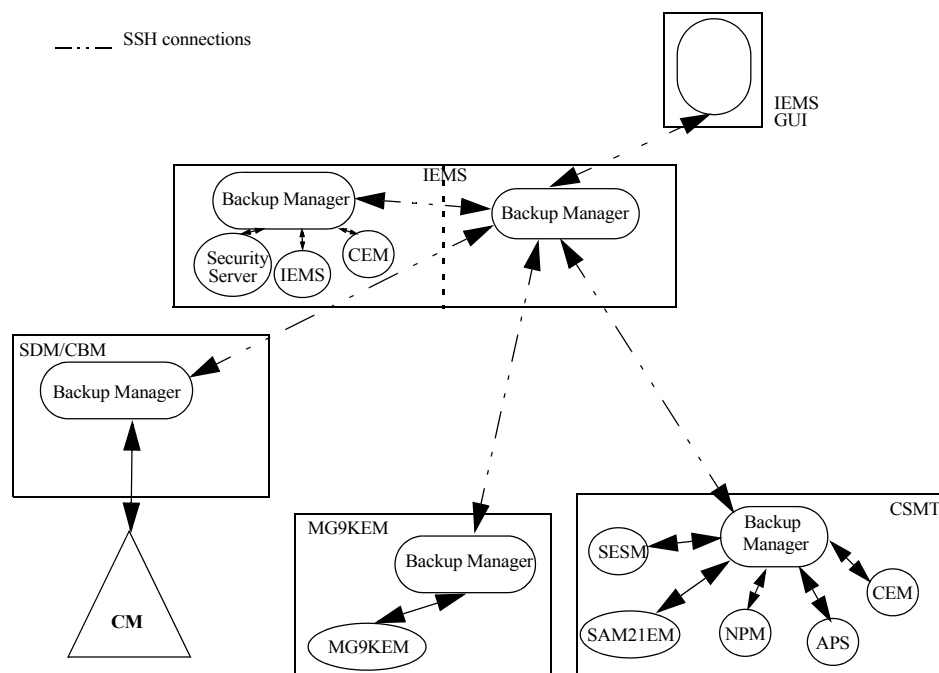
Note: The Integrated EMS may reside with the CSMT (and other applications) on the CSMT server.

From the IEMS GUI, the user launches the SBRM command line interface and initiates a backup for the core components of the Succession Call Server. The SBRM receives the user request, and subsequently initiates a backup command sequence (using CLI commands over SSH) to execute a synchronous backup of the

components. Once the backup is complete, the backup files are stored locally on each component.

The following figure shows a high-level functional overview of the SBRM.

High-level functional overview of the SBRM



Sequence of events to run the Synchronized Backup Manager

The component onto which the SBRM is being installed determines the sequence of events.

Installing and configuring SBRM on the SDM

To install and configure the Synchronized Backup Manager (SBRM) on the SDM, the following steps are required:

1. To install the Backup Restore Manager on the SDM, refer to procedure, [Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager on page 32](#).
2. To configure the bkmgrusr user ID and password on the SDM, refer to procedure, [Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM on page 73](#).

3. To configure SSH between the backup manager restore servers, refer to procedure, [Configuring SSH between the backup restore manager servers on page 81](#).
4. To configure core access for the SBRM through the SDM, refer to procedure, [Configuring core access for SBRM through the CS 2000 Core Manager on page 75](#).
5. To create the backup user ID on the core for SBRM, refer to procedure, [Creating the backup user ID on the core for SBRM on page 77](#).
6. To configure automated execution of backups, refer to procedure, [Configuring the automated synchronous backup restore manager service on page 89](#).
7. Configure the specific Backup Restore Manager installations, setting the appropriate properties for the SBRM which resides in the Integrated EMS and the individual component-level Backup Restore Managers which reside in the other platforms (for example, the CSMT and SDM).
8. Complete the common procedures for all components on page [28](#).

Installing and configuring SBRM on the CBM 850

To install and configure the Synchronized Backup Manager (SBRM) on the CBM 850, the following steps are required:

1. To install the Backup Restore Manager on the CBM 850, refer to procedure, [Installing optional software on a CBM 850 on page 38](#).

Note: No special configuration is required whilst performing this operation.
2. To configure SSH between the backup manager restore servers, refer to procedure, [Configuring SSH between the backup restore manager servers on page 81](#).
3. To configure core access for SBRM through the CBM 850, refer to procedure [Configuring core access for SBRM through the CBM 850 on page 79](#).
4. To create the backup user ID on the core for SBRM, refer to procedure, [Creating the backup user ID on the core for SBRM on page 77](#).
5. Complete the common procedure for all components in this section on page [28](#).

Common procedures for all components

The following procedures are required in order to configure the SBRM on all components.

- To configure SSH between the backup manager restore servers (if not already completed), refer to procedure, [Configuring SSH between the backup restore manager servers on page 81](#).

The following sections provide additional information regarding the SBRM:

- To configure automated execution of backups, refer to procedure, [Configuring the automated synchronous backup restore manager service on page 89](#).
- To control the automated execution of backups, refer to procedure, [Starting or stopping the automated synchronous backup restore manager service on page 95](#).

To configure the Integrated IEMS to support the SBRM, refer to the following procedures:

- To add the SBRM to the Integrated EMS using the Java Web Start Client, refer to procedure, “Adding a Synchronized Backup Restore Manager application (SBRM application)” in *Integrated EMS Configuration Management*, NN10330-511.
- To add the SBRM to the Integrated EMS using the web client, refer to procedure, “Adding an SBRM application” in *Integrated EMS Configuration Management*, NN10330-511.
- To launch the CLI for the SBRM using the Integrated EMS Java Web Start Client, refer to the procedure, “Launching CLI for SBRM application” in *Integrated EMS Basics*, NN10329-111. The SBRM cannot be launch using the Integrated EMS web client.

A network backup (that is, where several components are backed up at once) is invoked from the Integrated EMS Backup Manager. In rare instances, it may be necessary to run various portions of the backup process on individual components/servers themselves. This capability is implemented as a CLUI interface, as in the following section.

Execution of a backup at the component-level

ATTENTION

Execution of a backup at the component-level should be used only in rare circumstances. Care should be taken to keep the SBRM and the DBRM in sync.

The CLUI interface to perform a backup at the component-level can be invoked by logging into the appropriate component via a Telnet session. Refer to procedure, [Running the synchronous backup restore manager from a component level on page 99](#).

Hardware and software requirements

Backup Restore Manager functionality requires that the appropriate software is resident and configured in all platforms which require synchronized imaging. The Backup Restore Manager software itself is included in various platform software packages, including the SSPFS and SDM. SSPFS Backup Restore Manager functionality is used for integration of Call Server Management Tools (CSMT), the Media Gateway 9000 Element Manager (MG9KEM), the Integrated EMS, and the CBM. The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. No SDM/CBM data is backed up via the Backup Restore Manager software.

Requirements and restrictions

The following requirements and restrictions apply to Synchronized Backup Manager functionality in (I)SN08:

- All platforms requiring Backup Manager software functionality must be Java compatible and must provide a resident Java runtime system.
- Restore of generated synchronized backup images is not supported in the (I)SN08 SBRM software. Existing manual restore procedures must be followed in order to utilize the backup images produced by the Backup Restore Manager.
- The Backup Restore Manager system does not perform automatic spooling of backup data/image files to secure/redundant servers. Customers are required to manage their own secure server archiving capabilities. The Backup Restore Manager system will

publish data/image files in pre-determined/configurable directories on various servers:

— SSPSF Platform data/image file location:
/data/bkresmgr/backup.

— XACore/3PC data/image file location: Configurable

- Backup of program store and associated patches is not covered as part of the functionality associated with Synchronous Backup Restore Manager. If a customer needs to completely 'restore' a server/component, they will need to reinstall their applications and reapply the associated patches.
- The backup "abort" command may require manual cleanup/removal of some backup files. The user will be notified at "abort" command completion time if this is the case.
- The backup process itself can not be executed while certain constructive/destructive system audits are in progress (e.g. SESM's CS2K Data Integrity Audit). In general, if a backup is attempted while these audits are in progress, the backup attempt will be rejected. However, some constructive/destructive audits will be postponed when a backup request is received (e.g. MG9KEM Network Element Audit). The architecture of the system in question determines the appropriate behavior. In general, any system rejections of the backup request will result in an appropriate message being displayed to the Synchronous Backup Restore Manager client user.
- No system wide coordination between Synchronous Backup Restore Manager and other applications (eg. UpgradeManager, CS2K Audits, CM dump scheduling, etc.) is delivered in SN08. All application activity interdependencies must be manually managed by the user. For example, scheduled activities such as audits should be stopped during system backup. Also, any automated CM image dumps should be cancelled since the Synchronous Backup Restore Manager will be used to drive the dump within a synchronized system wide backup window.
- APS and NPM queries will be disallowed during backup. This is due to the applications being shut down during backup. Active clients will be informed of the application shutdown.
- Backup of the MG9KEM in isolation is not recommended due the CSMT platform data dependency. The MG9KEM database is hosted on the CSMT server.
- Synchronous Backup Restore Manager user authorization only controls the launch of the CLI. CLI Command specific authorization is not provided, therefore only users authorized to actually launch the Synchronous Backup Restore Manager CLI will be allowed to

perform query commands at the Synchronous Backup Restore Manager CLI.

- The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. No SDM/CBM data is backed up via the Backup Restore Manager software.

During the period when the backup is executing, user's of the various GUI and command line provisioning interfaces will be restricted from attempting actions which result in configuration and provisioning data changes. These restrictions include the following:

- Adding/deleting/updating GWCs at the Call Server Management Tools (CSMT) GUI or OSSGate interface.
- Adding/deleting/updating line service at the at the CSMT OSSGate interface.
- Manually invoking (or running via the scheduler) the various audits at the CSMT GUI.
- Adding/deleting/updating objects in the Integrated Element Management Server (Integrated EMS) topology via the Integrated EMS client.
- Adding/modifying collection jobs via the Integrated EMS client.
- Using the Runtime Administration interface at the Integrated EMS client to perform OSS configuration.
- Using the Security Administration interface at the Integrated client to add/delete Users/Groups/Operations.
- Using the Security Administration interface at the Integrated EMS client to change a user password.
- Adding/deleting/updating Trunks/Carriers via the CSMT.
- Node provisioning/deprovisioning via the SAM21Manager.
- ATM connection set provisioning/deprovisioning via the SAM21 Manager.

Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager

Purpose

Use this procedure to install and configure the Backup Restore Manager application on the CS 2000 Core Manager

Application

The Backup Restore Manager application functionality requires the appropriate software resident and configured on platforms that require synchronized imaging. Although no CS 2000 Core Manager data is backed up through the Backup Restore Manager, the Backup Restore Manager software must be installed on the CS 2000 Core Manager to allow control of the xa-core and 3PC (Compact) backup.

Procedures

Note: Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

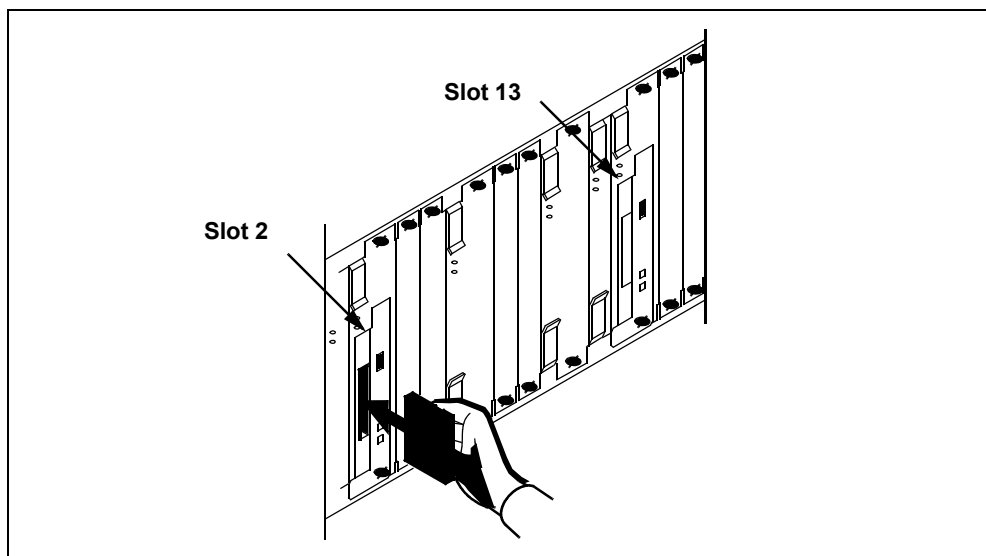
Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager

At the CS 2000 Core Manager

- 1 Insert the tape for the software load into one of the tape drives (slot 2 or slot 13) of the main chassis, as shown in the following figure.

Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

Tape drive in main chassis



At the maintenance interface

- 2 Determine the installation method.

If you choose to install OM Data Delivery by	Do
logging onto a local VT100 terminal connected to the CS 2000 Core Manager	log on to the CS 2000 Core Manager as the root user at the VT-100 terminal, and go to step 6

**If you choose to install OM
Data Delivery by****Do**

using telnet from a remote
UNIX workstation to the CS
2000 Core Manager

step [3](#)

- 3 Open a VT-100 compatible terminal window at the remote UNIX workstation.
- 4 Log onto the CS 2000 Core Manager from the terminal window prompt:
`telnet <ip_address>`
where
<ip_address> is the IP address of the CS 2000 Core Manager you want to install the Backup Restore Manager application on.
- 5 When prompted, enter the login ID and password for the root user.
- 6 Access the maintenance interface level:
`sdmmtc`
- 7 Access the software inventory manager (SWIM) level:
`swim`
The CS 2000 Core Manager lists the software applications currently installed.
- 8 List the contents of the tape you previously inserted:
`apply <n>`
where
`<n>`
is either 0 (slot 2) or 1 (slot 13).
- 9 Locate the Java Runtime Environment (JRE) 1.3 packages.
Note: If necessary, use the up (enter 12, u, or up) and down (enter 13, d, or down) commands to locate the JRE 1.3 packages.

- 10 Select and install the Java Runtime Environment Executables 1.3.0.0 package:
apply <n>
where
 <n>
 is the number next to the Java Runtime Environment Executables 1.3.0.0 package.
- 11 Confirm the apply command:
y
- 12 Select and install the Java Runtime Environment Libraries 1.3.0.0 package:
apply <n>
where
 <n>
 is the number next to the Java Runtime Environment Libraries 1.3.0.0 package.
- 13 Confirm the apply command:
y
- 14 Select and install the Java Runtime Environment Executables 1.3.0.15 package:
apply <n>
where
 <n>
 is the number next to the Java Runtime Environment Executables 1.3.0.15 package.
- 15 Confirm the apply command:
y
- 16 Select and install the Java Runtime Environment Libraries 1.3.0.15 package:
apply <n>
where
 <n>
 is the number next to the Java Runtime Environment Libraries 1.3.0.15 package.
- 17 Confirm the apply command:
y

- 18 Select and install Succession Provisioning Data Sync Manager (or Backup Restore Manager fileset, SDM_BKM.bkm).
apply <n>
where
 <n>
 is the number next to the Backup Restore Manager fileset, SDM_BKM.bkm (or Succession Prov Data Sync Manager)
- 19 Confirm the apply command:
y
- 20 As part of the Backup Restore Manager application installation, a script runs that enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). As the script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, "Creating the backup user ID on the core for SBRM" in *CS 2000 Core Manager Configuration Management*, NN10104-511, or in *ATM/IP Solution-level Security and Administration*, NN10402-600.
- 21 As the script continues to run, you are then prompted for the password of the user you entered (in step 20). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, "Creating the backup user ID on the core for SBRM" in *CS 2000 Core Manager Configuration Management*, NN10104-511, or in *ATM/IP Solution-level Security and Administration*, NN10402-600.
- 22 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.
- 23 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 24 If, at any time after the installation is complete, you wish to re-configure the access to the core for the SBRM, perform the following steps:

- a** Access the config level of the SDM maintenance interface:
`sdmmtc config`
 - b** From the list of filesets that displays, select the Succession Provisioning Data Sync Manager fileset (or Backup Restore Manager fileset, SDM_BKM.bkm) and then type **config**.
You will then be prompted again for the information that you supplied earlier in steps [20](#) through [23](#).

25 You have completed this procedure.

Installing optional software on a CBM 850

Purpose

This is a generic procedure that is used for installing optional software packages on the CBM 850. Consult [Filesets available for the CBM 850 on page 38](#) to determine the optional software packages (filesets) that you can install through this procedure.

Note: This procedure should be performed on a pre-cloned system. If the procedure is not performed on a pre-cloned system, you must clone the image of the active node to the inactive node of the cluster after the software package has been installed and configured, and after the active node has been made patch-current.

Filesets available for the CBM 850

The following table lists filesets (applications) included in the CBM0080 load. The table also shows which filesets are included with the CBM 850 at the time of installation (Base) and which filesets are optional and that you may install later.

Filesets available for the CBM 850 (Sheet 1 of 3)

Fileset	Description	Type
SDM_BASE.version_20.81 .0.0	Load Lineup Information	Base
CBM_SETUP	CBM installation and upgrade tool; only on CD	Base
NT_SIM.tools	Patching Tools	Base
SDM_ACE	SDM ACE distribution	optional
SDM_AFT.DMS500	SBA Automatic File Transfer	optional
SDM_BASE.base	Platform Base	Base
SDM_BASE.comm	Platform Maintenance Common	Base
SDM_BASE.gdd	Generic Data Delivery	Base
SDM_BASE.logs.client	Log Delivery Service Client	optional
SDM_BASE.logs	Log Delivery Service	Base
Note: Base = included with the CBM 850		

Filesets available for the CBM 850 (Sheet 2 of 3)

Fileset	Description	Type
SDM_BASE.mtce	Platform Maintenance	Base
SDM_BASE.omsl	OM Access Service	Base
SDM_BASE.tasl	Table Access Service	Base
SDM_BMI.bmi	Base Maintenance Interface	optional
SDM_DDMS_ossaps	OSS and Application Svcs	optional
SDM_DDMS_osscomms	OSS Comms Svcs	optional
SDM_BASE.util	Platform Utilities	Base
SDM_DEBUG.tools	SDM/CBM Debug Helper Tools	Base
SDM_DMA.dma	DMS Maintenance Application	optional
SDM_NTiwb.iaa	Integrated Accounting Application	optional
SDM_NTiaa.iaa	Integrated Accounting Application	optional
SDM_EM.lep	Integrated Accounting Application	optional
SDM_EM.aev	IAA Accounting Event Message Viewing	optional
SDM_EM.aep	IAA Accounting Event Message Processing	optional
SDM_FTP.proxy	FTP Proxy	optional
SDM_GR740PT.gr740pt	GR740 Pass Through	optional
SDM_LOGS.mdm	Passport Log Streamer	optional
SDM_OMDD.omdd	OM Delivery	optional
SDM_REACHTHRU.rttl1	Reach Through SPM	optional
SDM_SBA.DMS500	SDM Billing Application	optional
Note: Base = included with the CBM 850		

Filesets available for the CBM 850 (Sheet 3 of 3)

Fileset	Description	Type
SDM_SCFT.scft	Core File Transfer	optional
SDM_SWLD.swld	Bootpd and tftpd	optional
NTbkupmgr	Succession Provisioning Data Synch Manager	optional
NTdtsv	CEM DMS Data Server	optional
NTprxy	CEM Telnet Ftp Handler	optional
NTsaf	CEM Store and Forward	optional
Note: Base = included with the CBM 850		

Procedure for installing optional software on a CBM 850

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Installing optional software on a CBM 850

At your workstation

- 1 Open a connection to the active node of the CBM 850 using SSH and log in as the root user:

```
ssh -l root <ip_address>
```

where

<ip_address>
is the IP address of the active node of the CBM 850 cluster
- 2 Enter the password for the root user.
- 3 Use the following table to determine your next step.

If	Action
you are installing the DDMS application	1. Perform steps 1 and 2 only, of Procedure for installing DDMS on page 45 2. Go to step 5
you are installing the OMDD application	1. Perform step 1 only, of Procedure for installing the OM Data Delivery software package on page 51 2. Go to step 5
you are installing the log delivery service application	1. Perform Procedure for installing the Passport Log Streamer application on page 54 2. Go to step 8

If	Action
you are installing the SBA or AFT applications	1. Perform Procedure to install the SBA and AFT software packages on page 56 2. Go to step 8
you are installing GR740PT application server	1. Perform Procedure for installing GR740PT application server on page 57 2. Go to step 8
you are installing the FTP Proxy application	1. Create the logical volume, /cbmdata/00/esa, with size 25 Mbyte, using the logical volume creation procedure in the <i>CBM 850 Security and Administration</i> NTP, NN10358-611. 2. Go to step 4.
you are installing the Backup Restore Manager software	1. Perform Installing the Backup Restore Manager software on page 69 2. Go to step 8
you are installing any other optional software application	Go to step 4

- 4 Apply the software application package by performing the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 59](#). Since CD-ROM is being used to install the application, specify /cdrom/cdrom/applications/cbm/packages as the directory path of the source directory when you perform that procedure.

- 5 Use the following table to determine your next step.

If	Action
you are installing any other applications that require you to create logical volumes	Return to step 3 and follow the required action for the application you are installing.
you are not installing any other applications that require you to create logical volumes	Go to step 6

- 6 If you created any logical volumes in step [3](#), reboot the CBM 850:

init 6

Note: Be sure that you have created any required logical volumes for all of the applications you are installing before performing this step.

- 7 After the node reboot is complete, use the following table to determine your next step.

If	Action
you are installing the DDMS application	1. Perform the remaining steps of Procedure for installing DDMS on page 45 , starting with step 3 2. Go to step 8
you are installing the OMDD application	1. Perform the remaining steps of Procedure for installing the OM Data Delivery software package on page 51 , starting with step 2 2. Go to step 8
you are installing the FTP Proxy application	Go to step 8 .
you are installing any other optional software application	Go to step 8

- 8 Ensure that your CBMs are patch-current by performing the procedure, [Making the CBM 850 patch-current after optional software package installation on page 65](#).

- 9 Clone the image of the active node to the inactive node by performing the procedure, [Cloning the image of the active node to the inactive node of a CBM 850 cluster on page 66](#).
- 10 You have completed this procedure.

Procedure for installing DDMS

This procedure enables you to install the DDMS application.

Note 1: For a successful installation of DDMS, the Log Delivery Service application must be in service.

Note 2: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Installing DDMS on a CBM 850

At your workstation

- 1 Enter each of the following commands:

```
permit sdm01 <sdm01_pswd> 4 10000 english all
permit sdm02 <sdm02_pswd> 4 10000 english all
permit sdm03 <sdm03_pswd> 4 10000 english all
permit sdm04 <sdm04_pswd> 4 10000 english all
```

where

<sdm0n_pswd>

is the CM password for user SDM0n

Note 1: If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

Note 2: If Enhanced Password Control is in effect on the CM, DDMS software has the ability to manage automatic password changing on the CBM and the CM, before the passwords expire. You do not, therefore, have to manually change any of the SDM01-SDM04 passwords on the CBM or CM. When the DDMS software is returned to service, it reads the tables, ofcopt and ofceng, on the CM to determine whether Enhanced Password Control is in effect. If Enhanced Password Control is in effect, the DDMS software reads the password lifetime value and automatically changes the passwords one day before they expire. If you make manual changes to the password lifetime value, or if you turn on or off Enhanced Password Control, these changes should be synchronized with DDMS software by performing a bsy or rts of DDMS. If, however, you change any of the SDM01-SDM04 passwords manually, you need to apply the same password changes in the DDMS configuration file.

- 2 Create the required logical volumes for the DDMS application.

```
makelv /cbmdata/00/osscomms 16
```

```

chmod 755 /cbmdata/00/osscomms
chown maint:maint /cbmdata/00/osscomms
makelv /cbmdata/00/ossaps 112
chmod 755 /cbmdata/00/ossaps
chown maint:maint /cbmdata/00/ossaps
makelv /cbmdata/00/ossapslog 112
chmod 755 /cbmdata/00/ossapslog
chown maint:maint /cbmdata/00/ossapslog

```

- 3 Apply the two software application packages, OSS and Application Svcs and OSS Comms Svcs by performing the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 59](#). Specify /cdrom/cdrom/applications/cbm/packages as the source directory when you perform that procedure.
- 4 You should be prompted automatically to configure the OSS Comms Svcs package; the OSS and Application Svcs package does not require configuration. Use the following table to determine your next step.

If	Do
you are prompted automatically to configure the OSS Comms Svcs package	step 8
you are not prompted automatically to configure the OSS Comms Svcs package	step 5

- 5 Access the config level of the maintenance interface:
cbmmtc config
- 6 In the list of applications, locate the OSS Comms Svcs application and take note of its number (located next to the names of the applications). Select the application:
select <application number>
where
<application number>
is the number associated with the OSS Comms Svcs application, that you noted.
In response to the command, the OSS Comms Svcs application will be highlighted on the cbmmtc config screen.

- 7 Invoke the configuration of the OSS Comms Svcs application.

config

- 8 When prompted to enter the logroute tool, as shown in table [DDMS logroute tool banner](#), press Enter. The Logroute Main Menu appears, as shown in figure [Logroute tool main menu](#).

DDMS logroute tool banner

```
#####
# Adding DDMS logroute configuration
#####
Please add DDMS log routing:
      Device type      = file
      File              = /cbmdata/00/logs/ossaps/ossapslog
      Routing          = addrep
      log_type         = DDMS
Press <RETURN> when ready
```

Logroute tool main menu

```

                                Logroute Main Menu

                                1 - Device List
                                2 - Global Parameters
                                3 - CM Configuration File
                                4 - GDD Configuration
                                5 - Help
                                6 - Quit Logroute

Enter Option ==>
```

- 9 Set up a path and file to store DDMS customer logs as follows:

- a Select the Device List menu:
 - 1The Device List Menu screen is displayed.
- b Select 1 to display the Device List screen.

If the list	Do
includes device /cbmdata/00/logs/ossaps/ossapslog	step c
does not include device /cbmdata/00/logs/ossaps/ossapslog	step d

- c Press the Enter key.
- d Begin to add a new device:
 - 2
- e Select a file device:
 - 3

Response:

```
Enter file name ==> /data/logs/
```
- f Complete the path name by typing
ossaps/ossapslog
You have now set up the log routing for the DDMS.
- g When prompted, enter STD log format (from the range displayed).
- h When prompted, set the ECore option to ON.
- i Select addrep:
 - a
- j Enter the log identifier by typing, in uppercase
DDMS
- k When prompted to enter more log routing details, enter
N
- l Save the new device:
 - y

Response:

```
Save completed -- press return to continue
```

Press the Enter key to return to the Add Device screen.

m Return to the Device List Menu screen:

5

n Return to the main menu screen:

6

o Exit logroute:

6

p The CM User Setup screen is displayed as shown in the following example.

The required CM users, SDM01-SDM04, for DDMS will be added to the DDMS configuration file. The passwords for these users should be the same as those entered in step [1](#)

Note: The userIDs and passwords are not case sensitive and will be the same. You can change them after this installation is complete.

Example of DDMS CM user setup screen

CM User Setup
0. QUIT 1. Add user 2. Delete user (by ID) 3. Update passwd (by ID) 4. Display users (ID)
Enter choice:

10 Follow sub-steps [a](#) through [c](#) for each of the required userIDs:

a Add a new user:

1

b When prompted, enter the user name (for example, sdm01).

c When prompted enter the user password.

Note: Your first entry of a user name and password will cause an error message: "Error: file not valid." Ignore this message and continue to add the other user names and passwords.

d Exit the CM User Setup screen:

0

The DDMS Clients Configuration screen is displayed as shown in the following example.

Example of DDMS Clients Configuration screen

DDMS Clients Configuration
0. Quit 1. Add new clients 2. Remove existing clients 3. List existing clients Enter choice:

- 11** Follow sub-steps [a](#) through [c](#) to configure the DDMS clients.
- Note:** The DDMS clients are the CS 2000 Management Tools servers with the SESM load. If the CS 2000 Management Tools server is a cluster configuration, add the IP address of both units (active and inactive unit).
- a** Add a new client:
- 1**
- b** When prompted, enter the IP address for each of the CS 2000 Management Tools servers. Press the Enter key after each entry and type “done” once you have entered all the IP addresses.
- c** Exit the DDMS clients configuration screen:
- 0**
- 12** You have completed this procedure. Return to step [8](#) of procedure [Installing optional software on a CBM 850](#).

Procedure for installing the OM Data Delivery software package

The OM Data Delivery application collects and stores operational measurement (OM) data from the switch. The application stores the data in comma separated value (CSV) files that are sent to the client operations support system (OSS). This procedure contains the steps for installing and configuring the OM Data Delivery application on the CBM 850 cluster.

Prerequisites

Ensure that the OM Access Service and Table Access Service application filesets are installed and in service on your core manager before executing this procedure.

For the wireless market, the Nortel support group needs to increase the buffer size within the OM Access Service to 2.5 MB. This is done to accommodate the amount of data being transferred by the front end for a transfer period of every 30 minutes.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Installing and configuring the OM Data Delivery application on a Core and Billing Manager 850

At your workstation

- 1 Create the following logical volume (directory for a file system) required for the OMDD software package you are installing:
makelv /cbmdata/00/omdata 1008
- 2 Using the procedure, [Applying software packages on a CBM 850 using the CBMMTC interface on page 59](#) apply the SDM_OMDD.omdd software package located in the /cdrom/cdrom/applications/cbm/packages directory. Since CD-ROM is being used to install the application, specify /cdrom/cdrom/applications/cbm/packages as the directory path of the source directory when you perform that procedure.
- 3 Access the Config level of the CBM maintenance interface:
cbmmtc config
- 4 Configure OM Data Delivery:
config <n>
where

<n>

is the number next to OM Data Delivery under fileset description

- 5 The system indicates that the Tuple Number option is inactive and prompts you to determine whether you want to activate it.

Note: The Tuple Number option allows you to activate or disable a tuple number so that it can be included in a CSV file with other OM information.

If you	Do
want to activate the Tuple Number option	Type y Go to step 6
do not want to activate the Tuple Number option	Type n Go to step 6

- 6 The system prompts you to confirm whether the Multiservice Data Manager (MDM) and core manager are integrated.
To indicate that the MDM is connected to the core manager for collecting Passport 15000 performance measurement data, type **y**
- 7 Configure the core manager to communicate with the MDM as follows:
- a When prompted, enter the IP address of the first MDM you want to connect to.
 - b When prompted, enter the hostname of the first MDM.
 - c When prompted, enter the IP address of the second (alternate) MDM you want to connect to.
 - d When prompted, enter the hostname of the second MDM.
 - e When prompted, enter the port for 5-minute performance PM (performance measurement) data. The default port is 1646.
 - f When prompted, enter the port for 30-minute PM data. The default port is 1647.
- 8 You are prompted as to whether you want to use custom connection retry settings. In case of connection failure, OMDD will try connecting to the MDMs, alternatively. When prompted,

indicate whether you want to use custom connection retry settings.

If you	Do
want to use custom retry settings	Type y Go to step 9
do not want to use custom retry settings but want, instead, to use default settings	Type n Go to step 10

- 9** Respond to the prompts with your custom retry settings:
- Note:** The retry setting values shown here are examples. Retry setting values are in seconds (values higher than 300 seconds are not recommended as they may adversely affect recovery time).
- Enter the first connection retry interval: 2**
- Enter the number of retry attempts at that interval: 10**
- Enter the second connection retry interval: 10**
- Enter the number of retry attempts at that interval: 40**
- Enter the third connection retry interval: 60**
- 10** When prompted, confirm the configuration data you have entered by typing **y**
- Note:** If you type **n**, you will be prompted to re-enter all of the configuration data.
- 11** The system indicates that the configuration is complete.
Press the Enter key.
- 12** The system indicates that the changes will take place after the OM Data Delivery application is restarted.
Press the Enter key to restart the OM Data Delivery application.
- 13** Exit the maintenance interface:
quit all
- 14** You have completed this procedure. Return to step [8](#) of procedure [Installing optional software on a CBM 850](#).

Procedure for installing the Passport Log Streamer application

The following procedure contains the steps for installing and configuring the Passport Log Streamer application on the CBM 850 cluster.

For full operation, the log delivery application requires installation of the following application filesets:

- log delivery service (Base software)
- log delivery service client (optional software)
- Generic Data Delivery (Base software)
- Passport Log Streamer, if the core manager needs to communicate with the Multiservice Data Manager (MDM) for fault data. (optional software)

Prerequisites

Before performing this procedure, ensure that there are no disk faults on the core manager.

In order to ensure that the Passport Log Streamer is able to communicate with the configured MDMs and to collect logs, any restrictions for the configured MDM ports should be removed from all of the firewalls that exist between the MDM and the CBM 850.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Installing and configuring the Passport Log Streamer application on the Core and Billing Manager 850

At your workstation

- 1 Perform the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 59](#) to apply the SDM_LOGS.mdm_21.39.9.0.pkg software package located in the /cdrom/cdrom/applications/cbm/packages directory. Since CD-ROM is being used to install the application, specify /cdrom/cdrom/applications/cbm/packages as the directory path of the source directory when you perform that procedure.
- 2 Configure the Passport Log Streamer application as follows:
 - a When prompted, enter the IP address for the first MDM node.
 - b When prompted, enter the IP address for the second MDM node.

- c When prompted, enter the port number configured for the pserver application on the first MDM node.
 - d When prompted, enter the port number configured for the pserver application on the second MDM node.
 - e When prompted, indicate that you do not want to receive MDM logs by entering **n**.
 - f When prompted, indicate that you do not want to specify Passport 15000 log filters by entering **n**.
 - g When prompted, indicate that you do not want to specify Passport 8600 log filters by entering **n**.
 - h When prompted, confirm the configuration data you entered by entering **y**.
- 3 Place the log delivery service application and the Passport Log Streamer application into service. Begin by accessing the Application (Appl) level of the CBM maintenance interface:
appl
 - a Busy the application filesets:
bsy <fileset_number> <fileset_number>
where
fileset_number is the number next to each of the following application filesets:
 - Log delivery service
 - Passport Log Streamer
 - b Return the application filesets to service:
rts <fileset_number> <fileset_number>
where
fileset_number is the number next to each of the application filesets you busied in the previous step

Once the application filesets are in service, the system retrieves any current log records. To view or store the log records, see the procedure “Displaying or storing log records using log receiver” in the Fault Management document.

 - c Exit the CBM maintenance interface:
quit all
- 4 You have completed this procedure. Return to step [8](#) of procedure [Installing optional software on a CBM 850](#).

Procedure to install the SBA and AFT software packages

This procedure enables you to install the SuperNode Billing Application (SBA) and Automatic File Transfer (AFT) software packages on the CBM 850 cluster.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Installing the SBA and AFT software packages on a CBM 850

At your workstation

- 1 Using the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 59](#), apply the SBA and AFT software packages located in the /cdrom/cdrom/applications/cbm/packages directory.
- 2 Create the necessary logical volumes (directories for file systems) required for the SBA. For the procedure used to create logical volumes, see “Adding a logical volume through the command line” in the NTP NN10363-811, *CBM 850 Accounting*.
- 3 To configure the SBA for operation, refer to *Core and Billing Manager 850 Accounting*, NN10363-811 for the procedures to use.
- 4 To configure AFT for operation, refer to *Core and Billing Manager 850 Accounting*, NN10363-811 for the procedures to use.
- 5 You have completed this procedure. Return to step 8 of procedure [Installing optional software on a CBM 850](#)

Procedure for installing GR740PT application server

This procedure enables you to install the GR740PT application server.

Prerequisites

To ensure a successful GR740PT application server operation, the following must be configured:

- the settings for office parameters “eadas_dc_interface” and “eadas_nm_interface” in table OFCVAR, and the settings for the EADAS SOC (OAM00005 and OAM00006) are correct for your configuration.
- OAM00004 for EADAS/DC is ON and that office parameters “eadas_mpc_and_link” and “netminder_mpc_and_link” are appropriately datafilled in table OFCVAR when BX25 connectivity is required.

The following table lists the supported configurations for EADAS GR740PT application server.

CM EADAS TCP/IP configurations

Supported configurations	Setting for eadas_dc_interface	Setting for eadas_nm_interface	SOC OAM00005	SOC OAM00006
DC and NM over BX25	X25	N/A	ON	IDLE
DC and NM over TCP/IP	TCP_IP	N/A	ON	IDLE
DC and Netminder over BX25	X25	X25	IDLE	ON
DC over BX25 and Netminder over TCP/IP	X25	TCP_IP	IDLE	ON
DC over TCP/IP and Netminder over BX25	TCP_IP	X25	IDLE	ON
DC and Netminder over TCP/IP	TCP_IP	TCP_IP	IDLE	ON

The following table lists the channel assignments for EADAS. Note that DC EADAS channels 1, 2 and 3 support TR-740/746 compliant header

and message. NM EADAS channels 1, 2 and 3 support SR3942 and TR746 to Netminder.

EADAS channel assignments

Description	Service name	TCP port	MTS offset
DC EADAS lc 1	DC_EADAS_LOG_CHAN1	9550	234
DC EADAS lc 2	DC_EADAS_LOG_CHAN2	9551	235
DC EADAS lc 3	DC_EADAS_LOG_CHAN3	9552	236
NM EADAS lc 1	NM_EADAS_LOG_CHAN1	9553	237
NM EADAS lc 2	NM_EADAS_LOG_CHAN2	9554	238
NM EADAS lc 3	NM_EADAS_LOG_CHAN3	9555	239

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Installing GR740PT application server

At your workstation

- 1 Using the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 59](#), apply the GR740PT software package located in the /cdrom/cdrom/applications/cbm/packages directory.

Note: During configuration of GR740PT, use the following table to determine your response to the prompt, “Enter mode of security”.

If	Do
you are not configuring GR740PT in non-secure mode	select 1 . Non-secure
you are configuring GR740PT in local secure mode	select 2 . Local (SSH) security

- 2 You have completed this procedure. Return to step 8 of procedure [Installing optional software on a CBM 850](#)

Procedure for Applying software packages on a CBM 850 using the CBMMTC interface

This procedure enables you to install optional software packages on the nodes of a CBM 850 cluster.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Applying software packages on a CBM 850 using the CBMMTC interface

At your workstation

- 1 From the command line prompt, access the apply level of the cbm maintenance interface:

```
cbmmtc apply
```

The system displays the apply level screen of the cbm maintenance interface, which shows a list of the packages, if any exist, in the default source directory.

Note: Only 12 packages can be displayed at a time. You may need to scroll to the next screen by entering the Down command (command 13 on the left side of the window).

Example of cbm maintenance interface apply level screen display showing any available packages

```

xterm
  CBM      MATE  NET   APPL  SYS   HW   CLI: SN100
  *        -    *    *    *    *    Host: SN100_CBM
                                Active

Apply
0 Quit
2
3
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 16:12 >

Source: the directory /data/swd/sdm.
Filter: sdm Interactive Mode: OFF

# Package Description          Version          Status

No packages available in the directory /data/swd/sdm.
Use the Source command to list another directory.

```

If	Do
CD-ROM is being used to deliver the CBM software	step 2 , specifying: /cdrom/cdrom/applications/cbm/packages as the <source_directory_name>
you want to exit from the cbm maintenance interface	step 6

- 2 Insert the CD-ROM into the CD drive if the CD-ROM is not already present in the drive.
- 3 At the command line located at the bottom of the cbmmtc user interface screen, type:

source <source_directory_name>
where

<source_directory_name>
is the full pathname of the directory containing the package that you want to apply. Since CD-ROM is being used for the installation, specify
/cdrom/cdrom/applications/cbm/packages as the
source_directory_name

The system displays the apply level screen of the cbm maintenance interface, which shows a list of all packages in the source directory that you specified.

Example of cbm maintenance interface apply level screen display showing packages available in the source directory (CD-ROM)

```

xterm
  CBM      MATE    NET     APPL     SYS     HW     CLI: SN100
  *        -      *      *      *      *     Host: SN100_CBM
                                   Active

Apply
0 Quit
2
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh

Source: the directory /cdrom/cdrom/applications/cbm/packages.
Filter: sdm Interactive Mode: OFF

# Package Description          Version      Status
1 Platform Utilities          20.82.8.0   APPLIED
2 Table Access Service        20.82.8.0   APPLIED
3 Bootpd and tftpd            20.82.8.0   NOT APPLIED
4 SSH Core File Transfer       20.82.8.0   NOT APPLIED
5 SDM Billing Application       20.82.8.0   NOT APPLIED
6 Reach Through SPM           20.82.8.0   NOT APPLIED
7 Passport Log Streamer       20.82.8.0   NOT APPLIED
8 OSS Comms Svcs              20.82.8.0   NOT APPLIED
9 OSS and Application Svcs     20.82.8.0   NOT APPLIED
10 OM Access Service           20.82.8.0   APPLIED
11 OM Delivery                 20.82.8.0   NOT APPLIED

Packages on the source: 1 to 11 of 26

root
Time 15:50 >

```

- 4 In the list of packages, locate the packages to be applied and take note of their numbers (located next to the names of the packages). Select the packages that you have decided to apply:

select <package number> ... <package number>

where

<package number>

is the number associated with a package, that you noted.
Each package number is separated by preceding and succeeding spaces.

Example

To select the Reach Through SPM application, which is number 6, and OM Delivery, which is number 11 in the sample screen display shown above, enter

select 6 11

If the command is successful, the packages you selected will be highlighted on the cbmmtc apply screen, as shown below in the sample cbm maintenance screen.

Example of cbm maintenance interface apply level screen display showing packages you have selected for application

```

xterm
  CBM      MATE  NET   APPL  SYS   HW   CLI: SN100
  *        -    *    *    *    *   Host: SN100_CBM
                        Active
Apply
0 Quit
2
3
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 15:51 >

Source: the directory /cdrom/cdrom/applications/cbm/packages.
Filter: sdm Interactive Mode: OFF # Selected: 2
# Package Description          Version      Status
1 Platform Utilities          20.82.8.0   APPLIED
2 Table Access Service        20.82.8.0   APPLIED
3 Bootpd and tftpd            20.82.8.0   NOT APPLIED
4 SSH Core File Transfer       20.82.8.0   NOT APPLIED
5 SDM Billing Application       20.82.8.0   NOT APPLIED
6 Reach Through SPM           20.82.8.0   NOT APPLIED
7 Passport Log Streamer       20.82.8.0   NOT APPLIED
8 OSS Comms Svcs              20.82.8.0   NOT APPLIED
9 OSS and Application Svcs     20.82.8.0   NOT APPLIED
10 OM Access Service           20.82.8.0   APPLIED
11 OM Delivery                 20.82.8.0   NOT APPLIED
Packages on the source: 1 to 11 of 26

```

Note: If you want to de-select any packages that you selected, re-enter the select command for the packages you want to de-select. The highlighting on the packages that you de-select will be removed.

5 Apply the selected packages:

apply

Note: If a pre-requisite package for the package(s) you have selected has not already been applied on the system, SWIM will select (if you have not already selected the package in a previous step) and apply the pre-requisite package.

The system will prompt you once to ensure that you want to continue with the package application.

Example of cbm maintenance interface apply level screen display showing packages selected for application after the apply command has been issued

```

xterm
  CBM      MATE    NET     APPL     SYS     HW     CLI: SN100
  *        -      *      *      *      *      Host: SN100_CBM
                                Active

Apply
0 Quit
1
2
3
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up      The following new packages have been selected for install.
13 Down
14 Search  NTttt1120 'Reach Through SPH' 20.82.8.0
15 Filter  NTowd20 'OH Delivery' 20.82.8.0
16 View
17 Help    Do you wish to proceed?
18 Refresh Please confirm ("YES", "Y", "NO", or "N")

root
Time 15:52 >

```

If	Do
you want to continue the package application	step a
you do not want to continue the package application	step b

- a** Type yes in response to the prompt.

The status of each package application displays on the cbmmtc apply screen.

Example of cbm maintenance interface apply level screen display showing the status of the packages after they have been applied

```

xterm
CBM      MATE  NET  APPL  SYS  HW  CLI: SN100
ISTb     -    .  ISTb  .    .  Host: SN100_CBM
                        Active
Apply
0 Quit
2
3
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 15:55 >

Source: the directory /cdrom/cdrom/applications/cbm/packages.
Filter: sdm Interactive Mode: OFF
# Package Description          Version      Status
1 Platform Utilities          20.82.8.0    APPLIED
2 Table Access Service        20.82.8.0    APPLIED
3 Bootpd and tftpd            20.82.8.0    NOT APPLIED
4 SSH Core File Transfer       20.82.8.0    NOT APPLIED
5 SDM Billing Application       20.82.8.0    NOT APPLIED
6 Reach Through SPM           20.82.8.0    APPLIED
7 Passport Log Streamer       20.82.8.0    NOT APPLIED
8 OSS Comms Svcs              20.82.8.0    NOT APPLIED
9 OSS and Application Svcs     20.82.8.0    NOT APPLIED
10 OM Access Service          20.82.8.0    APPLIED
11 OM Delivery                 20.82.8.0    APPLIED
Packages on the source: 1 to 11 of 26

```

When the application is completed:

- The status of the packages shown on the cbmmtc apply screen (under the Status column) will indicate “Applied”.

Note: It is important that packages not be left on the system with a “Partial” status. In this event, or if the package application failed, contact your next level of support for assistance.

- The packages will appear in the list that displays when you enter the cbmmtc packages level.

If you want to view details about the CBM package application, perform the procedure [Viewing software transaction history and logs on the CBM 850 on page 71](#)

Go to step 6.

b Type no in response to the prompt.

6 Exit from the cbm maintenance interface:

quit all

7 You have completed this procedure. Return to step 8 of procedure [Installing optional software on a CBM 850](#).

Procedure for making the CBM 850 patch-current

This procedure enables you to make the CBM 850 cluster patch-current after the installation of optional software packages.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Making the CBM 850 patch-current after optional software package installation

At your workstation

- 1 Apply any patches for the optional software packages that you have installed:

```
patchctrl -d  
/cdrom/cdrom/applications/cbm/patches
```

Note: During installation, you may receive a prompt from the system to continue or abort the procedure because the inactive node is not available. You should enter Continue.

- 2 If you are informed by the system that there are interactive patches that could not be applied, enter the following command to apply each of these interactive patches:

```
patchctrl -f /swd/fixes/interactive/<patch_id>
```

where

<patch_id>

is the ID of the interactive patch that you are applying

- 3 If any special instructions display for manual patches that could not be applied, enter the following command to apply each of these manual patches:

```
patchctrl -f /swd/fixes/manual/<patch_id>
```

where

<patch_id>

is the ID of the manual patch that you are applying

- 4 You have completed this procedure. Return to step [9](#) of procedure [Installing optional software on a CBM 850](#).

Note: After you have completed this procedure, contact your patching prime to ensure you have now applied all required patches.

Procedure for cloning the image of the active node to the inactive node

This procedure enables you to clone the image of the active node onto the inactive node of a CBM 850 cluster.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Cloning the image of the active node to the inactive node of a CBM 850 cluster

At your workstation

- 1 Start the cloning process by typing
startb
and press the Enter key.

If the system	Do
prompts you for the Ethernet address	step 2
indicates it is using Ethernet address <EthernetAddress>	step 7

At the console connected to the inactive node

- 2 Log in to the inactive node through the console using the root user ID and password.
- 3 If the system is not already at the OK prompt, bring the system to the OK prompt:
init 0
- 4 At the OK prompt, display the Ethernet address of the inactive node:

OK **banner**

Example response:

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.
```

- 5 Take note of the Ethernet address that is displayed.

At your workstation (session connected to Active node)

- 6 Enter the Ethernet address of the inactive node you noted in step [5](#).
- 7 Use the following table to determine your next step.

If the system	Do
prompts you to enter the command "boot net - image"	step 8
does not prompt you to enter the command "boot net - image"	step 9

At the console connected to the inactive node

- 8 When prompted, boot the inactive node from the image of the active node by typing

OK **boot net - image**

and press the Enter key.

Note: There must be a space between the "-" and "image".

Example response:

SC Alert: Host System has Reset

Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All rights reserved. OpenBoot 4.8.0.build_04, 2048 MB memory installed, Serial #52964131. Ethernet address 0:3:ba:28:2b:23, Host ID: 83282b23.

Rebooting with command: boot net - image

.
.
.

SC Alert: Host System has Reset

At your workstation (session connected to the Active node)

- 9** Monitor the progress of the cloning from the active node. Cloning the inactive node takes approximately one hour to complete.

Example response:

```
Waiting for network response from unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become
normal.
Deleted snapshot 0.
Deleted snapshot 1.
Deleted snapshot 2.
Deleted snapshot 3.
d99: Soft Partition is cleared
```

- 10** You have completed this procedure. Return to step [10](#) of procedure [Installing optional software on a CBM 850](#).

Procedure for installing the Backup Restore Manager software

This procedure enables you to install the Backup Restore Manager software. The Backup Restore Manager application functionality requires the appropriate software resident and configured on platforms that require synchronized imaging. Although no Core and Billing Manager 850 data is backed up through the Backup Restore Manager, the Backup Restore Manager software must be installed on the CBM 850 to allow control of the xa-core and 3PC (Compact) backup.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Installing the Backup Restore Manager software

At the CLI prompt on the core

- 1 Enter the following command:

```
permit <backupuser> <backupuser_pswd> 4 10000  
english all
```

where

<backupuser>

is the user name for the core, that is up to 16 characters in length, that will be used by SBRM for login

<backupuser_pswd>

is the password for the <backupuser> user you are creating, which can be up to 16 characters in length

4

is the priority

10000

is the stack size

english

the language setting

all

is the privilege setting

Note 1: If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

Note 2: If Enhanced Password Control is in effect on the CM and after the user is permitted on the switch, log into the core manually with this user first. The core will prompt you to change the password at the first login after the login is permitted. Change the password and then perform step [1](#) again.

The SBRM does not have the ability to manage passwords. Therefore, you must re-run the configuration script in step [3](#).

At your workstation

- 2 Apply the software application package, NTbkupmgr by performing the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 59](#). Specify /cdrom/cdrom/applications/cbm/packages as the source directory when you perform that procedure.
- 3 **When the installation is complete, exit from CBMMTC. At the command line prompt, change directory to the directory containing appropriate configuration script:**
cd /opt/nortel/bkresmgr/cbm/scripts
- 4 **Run the configuration script:**
./bkmgr_config.sh
- 5 As the script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core in step [1](#).
- 6 As the script continues to run, you are then prompted for the user you entered (in step [5](#)). The script restricts the password to a maximum of 16 characters. This password is the one that was set up in step [1](#).
- 7 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.
- 8 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 9 You have completed this procedure. Return to step [8](#) of procedure [Installing optional software on a CBM 850](#).

Viewing software transaction history and logs on the CBM 850

Purpose

This procedure enables you to view additional details about the package transactions, either package configuration or package removal, that you have performed on a CBM 850.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Procedure

Viewing software transaction history and logs on the CBM 850

At your workstation

- 1 This procedure enables you to view logs that are local to each of the nodes in the CBM 850 cluster. Therefore, you must first choose the node in the cluster for which you want to view logs and then create a connection to that node.

If	Do
you are already connected to the CBM 850 for which you want to view logs	step 4
you are not already connected to a CBM 850 for which you want to view logs	step 2

- 2 Using SSH, open a connection to the node in the CBM 850 cluster for which you want to view logs and log in as the root user:

```
ssh -l root <ip_address>
```

where

<ip_address>
is the IP address of the CBM 850 node for which you want to view logs
- 3 Enter the password for the root user.

- 4 Determine the next step to perform.

If	Do
you have already accessed the cbmmtc user interface	step 6
you have not accessed the cbmmtc user interface	step 5

- 5 Type the following on the command line:

cbmmtc

- 6 Type the following on the command line located at the bottom of the cbmmtc user interface screen:

history

The system displays the information about the package transactions you have performed, including a log file and the results of the individual operations. Included also in this information is an indication as to the node on which the operations were performed. If the operations were performed on the active node, no special identifier, such as “active node”, is provided. If the operations were performed on the inactive node, however, the identifier, “inactive node” appears in the information displayed. For more details about a specific log displayed in the history command output, enter:

ViewLog <#>

where

<#>

is the number of the log in the log file.

- 7 Exit from the cbmmtc user interface:

quit all

- 8 You have completed this procedure.

Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM

Purpose

This procedure enables you to configure the bkmgrusr user ID and password in order for the Synchronous Backup Restore Manager (SBRM) to communicate with the Device Backup Restore Manager (DBRM) on the CS 2000 Core Manager.

Note: This procedure applies only to the CS 2000 Core Manager.

Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	<i>CS 2000 Core Manager Security and Administration</i> , NN10170-611
Displaying actions a user is authorized to perform	<i>CS 2000 Core Manager Security and Administration</i> , NN10170-611

Procedure

Configuring the bkmgrusr user ID and password for communication with SBRM

At your workstation

- 1 Log into the CS 2000 Core Manager on which the DBRM is installed as a user authorized to perform config-admin actions.
- 2 Create the user, "bkmgrusr":
`mkuser bkmgrusr`

- 3 Create the groups, “emsmtc”, “emsadm”, and “emsrw”:

```
mkgroup emsmtc
mkgroup emsadm
mkgroup emsrw
```
- 4 Add the bkmgrusr user to the primary group, “maint”, and to secondary groups, “emsmtc”, “emsadm”, “emsrw”:

```
chuser pgrp=maint groups=emsmtc,emsadm,emsrw
home=/home/bkmgrusr admin=true shell=/bin/ksh
bkmgrusr
```

Note: Although it may be unclear from the command syntax shown above, this command is entered on a single line. Therefore, when you enter this command, ensure that there is a space between **emsrw** and **home**, and that there is a space between **ksh** and **bkmgrusr**.
- 5 Confirm that the bkmgrusr user has been added to the required groups in step 4:

```
groups bkmgrusr
```

The system will display the groups that are associated with the bkmgrusr user.
- 6 Set the password for the bkmgrusr user:

```
passwd bkmgrusr
```

Note: The bkmgrusr user is disabled until this step is performed.
- 7 Log out of the CS 2000 Core Manager and then log back in as “bkmgrusr”.

When the system prompts you, change the password for the bkmgrusr user.
- 8 Change to the home directory and create the “.ssh” directory:

```
cd /home/bkmgrusr
mkdir .ssh
chmod 700 .ssh
```
- 9 You have completed this procedure.

Configuring core access for SBRM through the CS 2000 Core Manager

Purpose

This procedure enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). This procedure must be performed before the SBRM can automatically backup a core image.

Note 1: Perform the procedure, [Creating the backup user ID on the core for SBRM on page 77](#) before you perform this procedure for the first time.

Note 2: This procedure should be performed to whenever the password for the core user password expires or is changed. This ensures that the password you set in this procedure matches that set for the user on the core.

Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

Procedures

Configuring core access for SBRM through the CS 2000 Core Manager

At the CS 2000 Core Manager

- 1 Log into the core manager with the login ID and password for a user authorized to perform config-admin actions.

- 2 Use the following table to determine your next step.

If	Do
you wish to perform this procedure on the command line	step 3
you wish to perform this procedure through SDMMTC (SDM maintenance interface)	step 5

- 3 At the command line prompt, change directory to the directory containing appropriate configuration script:
- ```
cd /opt/nortel/bkresmgr/cbm/scripts
```
- 4 Run the configuration script:
- ```
./bkmgr_config.sh
```
- Go to step [7](#).
- 5 Access the config level of the SDM maintenance interface:
- ```
sdmmtc config
```
- 6 From the list of filesets that displays, select the Succession Provisioning Data Sync Manager fileset (Backup Restore Manager fileset, SDM\_BKM.bkm) and then type **config**.
- 7 As the configuration script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, [Creating the backup user ID on the core for SBRM on page 77](#)
- 8 As the script continues to run, you are then prompted for the user you entered (in step [7](#)). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, [Creating the backup user ID on the core for SBRM on page 77](#)
- 9 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.
- 10 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 11 You have completed this procedure.

---

## Creating the backup user ID on the core for SBRM

---

### Purpose

This procedure enables you to create the user ID on the core to enable the operation of the Synchronous Backup Restore Manager (SBRM). The types of operations that can be performed by this user are:

- set dump\_restore\_in\_progress field in ofcstd table
- start image dump
- ability to run itocci command set
- ability to perform diskut commands

**Note 1:** This procedure should be performed before you first perform the procedure, “Configuring core access for SBRM”.

**Note 2:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Procedure

#### Creating the backup user ID on the core for SBRM

##### *At the CLI prompt on the core*

- 1 Enter the following command:

```
permit <backupuser> <backupuser_pswd> 4 10000
english all
```

where

**<backupuser>**

is the user name for the core, that is up to 16 characters in length, that will be used by SBRM for login

**<backupuser\_pswd>**

is the password for the <backupuser> user you are creating, which can be up to 16 characters in length

**4**

is the priority

**10000**

is the stack size

**english**

the language setting

**all**  
is the privilege setting

**Note 1:** If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

**Note 2:** If Enhanced Password Control is in effect on the CM and after the user is permitted on the switch, log into the core manually with this user first. The core will prompt you to change the password at the first login after the login is permitted. Change the password and then perform the procedure, "Configuring core access for SBRM" using the <backupuser> user you have created and the changed password.

The SBRM does not have the ability to manage passwords. Therefore, you must re-run the configuration script in "Configuring core access for SBRM" to ensure that the password for the <backupuser> user

- 2 You have completed this procedure.

---

## Configuring core access for SBRM through the CBM 850

---

### Purpose

This procedure enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). This procedure must be performed before the SBRM can automatically backup a core image.

**Note 1:** Perform the procedure, [Creating the backup user ID on the core for SBRM on page 77](#) before you perform this procedure for the first time.

**Note 2:** This procedure should be performed whenever the password for the core user password expires or is changed. This ensures that the password you set in this procedure matches that set for the user on the core.

### Procedure

#### Configuring core access for SBRM

##### *At your workstation*

- 1 Log into the Core and Billing Manager 850 (CBM 850).
- 2 Change to the root user:  

```
su - root
```
- 3 When prompted, enter the root password.
- 4 Change directory to the directory containing appropriate configuration script:  

```
cd /opt/nortel/bkresmgr/cbm/scripts
```
- 5 Run the configuration script:  

```
./bkmgr_config.sh
```
- 6 As the script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, [Creating the backup user ID on the core for SBRM on page 77](#)
- 7 As the script continues to run, you are then prompted for the user you entered (in step 6). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, [Creating the backup user ID on the core for SBRM on page 77](#)

- 8** As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.
- 9** As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 10** You have completed this procedure.



---

## Configuring SSH between the backup restore manager servers

---

### Application

Use this procedure to configure the secure shell (SSH) between the Integrated Element Management system (EMS) server where the synchronous backup restore manager (SBRM) software is installed, and the SSPFS-based servers where the device backup restore manager (DBRM) software is installed.

**Note:** Throughout the remainder of this procedure, the Integrated EMS server will be referred to as the SBRM server and the SSPFS-based servers will be referred to as the DBRM servers.

SSH provides authentication and secure communications over insecure channels.

This procedure contains the steps to generate the SSH key pair on the SBRM server and transfer the key pair to each DBRM server and the SDM platform in the network. It also contains the steps to transfer an existing SSH key pair from the SBRM server to new or existing DBRM servers and the SDM platform in the network.

### Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password for the SBRM server
- you need the password for the bkmgrusr on the DBRM server to transfer the SSH key pair

**Note:** The bkmgrusr is created on the DBRM server when SSPFS is installed. To set or change the bkmgrusr password, refer to procedure [Changing a user password on an SSPFS-based server on page 417](#).

- you need the root password for the DBRM server when the DBRM server is a two-server configuration, to synchronize the SSH data between the two servers

## Action

Perform the following steps to complete this procedure.

### *At your workstation*

- 1 Log in to the SBRM server by typing  
`> telnet <server>`  
and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the Integrated EMS  
server where the SBRM software is installed  
**Note:** In a two-server configuration, log in to the Active side  
using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  
`$ su - root`  
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to where the backup restore manager  
configuration script is located by typing  
`# cd /opt/bkresmgr/admin/bin`  
and pressing the Enter key.
- 6 Run the backup restore manager configuration script by typing  
`# ./configure`  
and pressing the Enter key.

### *Example response:*

Backup Restore Manager Configuration

```
1 - Backup Restore Manager SSH Setup
2 - Automated Synchronous Backup Restore
 Manager Service
```

```
X - exit
```

```
select - [X, 1-2]
```

- 7 Enter the number next to the “Backup Restore Manager SSH setup” option in the menu.

*Example response:*

SSH Setup for Synchronous Backup Restore Manager

- 1 - Generate SSH key and transfer to Device Backup Restore Manager servers
- 2 - Transfer existing SSH key to Device Backup Restore Manager servers

X - exit

select - [X, 1-2]

- 8 Use the following table to determine your next step.

| If you are                                                       | Do                      |
|------------------------------------------------------------------|-------------------------|
| configuring SSH for the first time, or changing the SSH key pair | step <a href="#">9</a>  |
| transferring the SSH key pair to a new or existing DBRM server   | step <a href="#">22</a> |

- 9** Enter the number next to the “Generate SSH key and transfer to Device Backup Restore Manager servers” option in the menu.

*Example response:*

Generate SSH key for Synchronous Backup Restore Manager and transfer to Device Backup Restore Manager servers.

WARNING: Running this script will generate a new SSH key for the bkmgrusr.

This new SSH key must be transferred to all existing and new Device Backup Restore Manager servers.

Do you want to continue? [y/n]:

- 10** When prompted, confirm you want to continue by typing  
**y**  
and pressing the Enter key.

*Example response:*

Generating SSH key for bkmgrusr.  
Sun Microsystems Inc. SunOS 5.9                      Generic  
May 2002  
Generating public/private rsa key pair.  
Enter file in which to save the key  
(/export/home/bkmgrusr/.ssh/id\_rsa):

- 11** When prompted, press the Enter key to accept the default location and filename “/export/home/bkmgrusr/.ssh/id\_rsa” for the key.

**Note 1:** If the default location and filename is not provided, enter “/export/home/bkmgrusr/.ssh/id\_rsa”.

**Note 2:** If the location and filename “/export/home/bkmgrusr/.ssh/id\_rsa” already exists and you wish to overwrite, enter **y**. Otherwise, enter **n**.

*Example response:*

```
Your identification has been saved in
/export/home/bkmgrusr/.ssh/id_rsa.
```

```
Your public key has been saved in
/export/home/bkmgrusr/.ssh/id_rsa.pub.
```

```
The key fingerprint is:
```

```
33:99:17:f0:ac:2a:3a:86:a9:d9:76:65:e6:70:4b:6
:8 bkmgrusr@comp5iems
```

```
Synchronizing files IF clustered node
```

```
Transfer existing SSH key to Device Backup
Restore Manager servers
```

```
WARNING: You must have the password for the
bkmgrusr on the Device Backup Restore Manager
server to transfer the SSH key.
```

```
Do you want to transfer the SSH key? [y/n]:
```

- 12** When prompted, confirm you want to transfer the SSH key pair by typing

**y**

and pressing the Enter key.

*Example response:*

```
Setting up to transfer SSH key to DBRM server.
```

```
Enter hostname or IP address of DBRM server to
transfer the SSH key to:
```

- 13** When prompted, enter the hostname or IP address of a DBRM server in your network.

*Example response:*

```
Platform type of DBRM server to transfer SSH key
to:
```

- 1 - SSPFS
- 2 - SDM

```
Enter platform type of DBRM server to transfer
SSH key to [1-2]:
```

- 14** When prompted, enter the number next to the platform type of the DBRM server.

**Note:** The SSPFS platform type is for servers hosting the CS 2000 Management Tools, MG 9000 Manager and Core and Billing Manager (CBM). The SDM platform type is an AIX platform containing core management software.

*Example response:*

```
Sun Microsystems Inc. SunOS 5.9 Generic
May 2002
```

```
The authenticity of host 'comp5iems
(45.123.456.98)' can't be established.
```

```
RSA key fingerprint is
ff:eb:a8:87:14:d0:82:28:5c:43:70:5a:ab:af:e6:f
d
```

```
Are you sure you want to continue connecting
(yes/no)?:
```

- 15** When prompted, confirm you want to continue connecting by typing

**yes**

and pressing the Enter key.

```
Warning: Permanently added 'comp5iems
(45.123.456.98)' (RSA) to the list of known
hosts.
```

```
Password:
```

- 16** When prompted, enter the password for the bkmgrusr on the DBRM server.

*Example response:*

Transfer of SSH key to <server> complete.

Is DBRM <server> a High Availability (HA) server? [y/n]:

- 17** When prompted, enter **y** if the DBRM server is a two-server configuration (HA), otherwise, enter **n**.

| If you entered | Do                      |
|----------------|-------------------------|
| y (yes)        | step <a href="#">18</a> |
| n (no)         | step <a href="#">21</a> |

- 18**

**ATTENTION**

You need the password for the root user on the DBRM server to complete the steps that follow.

*Example response:*

WARNING: On HA DBRM servers, SSH setup is not complete unless one of the following steps is performed.

- a) The HA DBRM server <servername> is cloned.
- b) The SSH data on HA DBRM <servername> is manually synched.

WARNING: Choosing this option requires the root password for <servername>

Do you want to manually synchronize the SSH data on DBRM <servername> now [y/n]

- 19** When prompted, enter **y** if you want to manually synchronize the SSH data, otherwise, enter **n**.

| If you entered | Do                      |
|----------------|-------------------------|
| y (yes)        | step <a href="#">20</a> |
| n (no)         | step <a href="#">21</a> |

- 20** When prompted, enter the root password for the DBRM server

*Example response:*

```
Synchronization of SSH data on DBRM <servername>
complete.
```

- 21** When prompted, indicate that you want to transfer the SSH key pair to the DBRM installation on the SBRM server in your network.

**Note:** The SBRM always makes a SSH connection to the DBRM residing on the local server so that the local IEMS application is notified of the synchronized backup by way of SBRM to DBRM messaging.

- 22** Enter the number next to the “Transfer existing SSH key to Device Backup Restore Manager servers” option in the menu.

*Example response:*

```
Transfer existing SSH key to Device Backup
Restore Manager servers
```

```
WARNING: You must have the password for the
bkmgrusr on the Device Backup Restore Manager
server to transfer the SSH key.
```

```
Do you want to transfer the SSH key? [y/n]:
```

- 23** Exit the “Backup Restore Manager SSH setup” level by typing

```
select - x
```

and pressing the Enter key.

- 24** Exit the “Backup Restore Manager Configuration” level by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.



## Configuring the automated synchronous backup restore manager service

---

### Application

Use this procedure to configure the synchronous backup restore manager (SBRM) service on the SSPFS-based server where the SBRM software is installed, for automated execution of backups. Configuring the SBRM service involves specifying the day of the week and the time of day you want the backup to take place.

### Prerequisites

You need the root user ID and password for the SSPFS-based server where the SBRM software is installed.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the SBRM server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the Integrated EMS server where the SBRM software is installed  
**Note:** In a two-server configuration, log in to the Active side using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to where the backup restore manager configuration script is located by typing  

```
cd /opt/bkresmgr/admin/bin
```

and pressing the Enter key.

- 6** Run the backup restore manager configuration script by typing  
**# ./configure**  
and pressing the Enter key.

*Example response:*

Backup Restore Manager Configuration

- 1 - Backup Restore Manager SSH Setup
- 2 - Automated Synchronous Backup Restore Manager Service

X - exit

select - [X, 1-2]

- 7** Enter the number next to the “Automated Synchronous Backup Restore Manager Service” option in the menu.

*Example response:*

Automated Synchronous Backup Restore Manager Service

- 1 - Configure Automated Synchronous Backup Restore Manager Service
- 2 - Start the Automated Synchronous Backup Restore Manager Service
- 3 - Stop the Automated Synchronous Backup Restore Manager Service
- 4 - View the Automated Synchronous Backup Restore Manager Service Configuration

X - exit

select - [X, 1-4]

**8** View the configuration settings as follows:

- a** Enter the number next to the “View the Automated Synchronous Backup Restore Manager Service Configuration” option in the menu.

*Example response:*

The Automated Synchronous Backup Restore Manager Service is not running

Automated Synchronous Backup Restore Manager Service Configuration Settings

|                |          |
|----------------|----------|
| Backup Enabled | : N      |
| Backup Day     | : SUNDAY |
| Backup Hour    | : 24     |

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

| If you                                                               | Do                      |
|----------------------------------------------------------------------|-------------------------|
| want to change the configuration settings of the SBRM service        | step <a href="#">9</a>  |
| do not want to change the configuration settings of the SBRM service | step <a href="#">11</a> |

**9** Change the configuration settings as follows:

- a** Enter the number next to the “Configure Automated Synchronous Backup Restore Manager Service” option in the menu.

*Example response:*

Automated Synchronous Backup Restore Manager  
Service Configuration

Configuring the Automated Synchronous Backup  
Restore Manager Service does not START the  
service. Return to the previos menu and  
select 'Start the Automated Synchronous  
Backup Restore Manager Service' to start the  
service.

Day of the week to run the Synchronous Backup  
Restore Manager:

This is day of the week the Synchronous Backup  
Restore Manager will execute a full backup.

- 1 - MONDAY
- 2 - TUESDAY
- 3 - WEDNESDAY
- 4 - THURSDAY
- 5 - FRIDAY
- 6 - SATURDAY
- 7 - SUNDAY

Enter day of week to run the Synchronous  
Backup Restore Manager (default: SUNDAY):

- b** When prompted, enter the number next to the day of the week on which you want the backup to execute, or press the Enter key to accept the default value.

*Example response:*

Hour to run the Synchronous Backup Restore Manager based on 24 hour clock:

Example 1 is 1 AM, 12 is noon, and 24 is midnight.

This is the hour on the <DAY> the Synchronous Backup Restore Manager will execute a full backup.

Enter hour to run the Synchronous Backup Restore Manager (default: 24)

- c** When prompted, enter the time of day at which you want the backup to execute, or press the Enter key to accept the default.

*Example response:*

Automated Synchronous Backup Restore Manager Service Configuration complete.

Configuring the Automated Synchronous Backup Restore Manager Service does not START the service. Return to the previous menu and select 'Start the Automated Synchronous Backup Restore Manager Service' to start the service.

- 10** Use the following table to determine your next step.

| If you                                              | Do                                                                 |
|-----------------------------------------------------|--------------------------------------------------------------------|
| want to start the automated SBRM service now        | perform procedure Enabling or disabling the automated SBRM service |
| do not want to start the automated SBRM service now | step <a href="#">11</a>                                            |

- 11** Exit the “Automated Synchronous Backup Restore Manager Service” level by typing

`select - x`

and pressing the Enter key.
- 12** Exit the “Backup Restore Manager Configuration” level by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

---

## Starting or stopping the automated synchronous backup restore manager service

---

### Application

Use this procedure to start or stop the synchronous backup restore manager (SBRM) service on the SPFS-based server where the SBRM software is installed.

### Prerequisites

You need the root user ID and password for the SPFS-based server where the SBRM software is installed.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the SBRM server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the IEMS server where the SBRM software is installed  
**Note:** In a two-server configuration, log in to the Active side using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to where the backup restore manager configuration script is located by typing  

```
cd /opt/bkresmgr/admin/bin
```

and pressing the Enter key.

- 6** Run the backup restore manager configuration script by typing  
**# ./configure**  
and pressing the Enter key.

*Example response:*

Backup Restore Manager Configuration

- 1 - Backup Restore Manager SSH Setup
- 2 - Automated Synchronous Backup Restore Manager Service

X - exit

select - [X, 1-2]

- 7** Enter the number next to the “Automated Synchronous Backup Restore Manager Service” option in the menu.

*Example response:*

Automated Synchronous Backup Restore Manager Service

- 1 - Configure Automated Synchronous Backup Restore Manager Service
- 2 - Start the Automated Synchronous Backup Restore Manager Service
- 3 - Stop the Automated Synchronous Backup Restore Manager Service
- 4 - View the Automated Synchronous Backup Restore Manager Service Configuration

X - exit

select - [X, 1-4]

- 8** Use the following table to determine your next step.

| If you want to                   | Do                      |
|----------------------------------|-------------------------|
| start the automated SBRM service | step <a href="#">9</a>  |
| stop the automated SBRM service  | step <a href="#">10</a> |



**9** Start the SBRM service as follows:

- a** Enter the number next to the “Start the Automated Synchronous Backup Restore Manager Service” option in the menu.

*Example response:*

```
Start the Automated Synchronous Backup
Restore Manager Service
```

```
WARNING: Running this script will start the
Automated Synchronous Backup Restore Manager
Service
```

```
Starting the service does not initiate a
backup until the day and time configured.
```

```
Do you want to continue? - [y/n]:
```

- b** When prompted, confirm you want to start the SBRM service by typing

**y**

and pressing the Enter key.

*Example response:*

```
Registering with SERVMAN.
```

```
Starting the Automated Synchronous Backup
Restore Manager Service.
```

```
Starting AUTO_BACKUP_MANAGER through
servstart AUTO_BACKUP_MANAGER Started
```

- c** Proceed to step [11](#).

**10** Stop the SBRM service as follows:

- a** Enter the number next to the “Stop the Automated Synchronous Backup Restore Manager Service” option in the menu.

*Example response:*

```
Stop the Automated Synchronous Backup Restore
Manager Service
```

```
WARNING: Running this script will stop the
Automated Synchronous Backup Restore Manager
Service
```

```
Stopping the service does not abort a backup
in progress.
```

```
Do you want to continue? - [y/n]:
```

- b** When prompted, confirm you want to stop the SBRM service by typing

**y**

and pressing the Enter key.

*Example response:*

```
Stopping the Automated Synchronous Backup
Restore Manager Service.
```

```
Stopping group using servstop
AUTO_BACKUP_MANAGER Stopped
```

```
Deregistering with SERVMAN
```

**11** Exit the “Automated Synchronous Backup Restore Manager Service” level by typing

```
select - x
```

and pressing the Enter key.

**12** Exit the “Backup Restore Manager Configuration” level by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

## Running the synchronous backup restore manager from a component level

---

### Application

Use this procedure to run various portions of the synchronous backup restore manager (SBRM) process from the backup manager CLUI on an SSPFS-based server where the Device Backup Restore Manager (DBRM) software resides, rather than from the CLUI on the Integrated Element Management System (IEMS) server where the Synchronous Backup Restore Manager (SBRM) software resides.

**Note:** All backups will be stored in a common file location. For example, “/data/bkresmgr/backup”.

### Prerequisites

You need the root user ID and password for the SSPFS-based server on which you are running the various portions of the SBRM process.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the SSPFS-based server by typing

> **telnet** <server>

and pressing the Enter key.

where

**server**

is the IP address or host name of the SSPFS-based server on which you are running the various portions of the SBRM process

**Note:** In a two-server configuration, log in to the Active side using its physical IP address.

- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  
\$ **su** -  
and pressing the Enter key.
- 4 When prompted, enter the root password.

- 5 Change directory to where the backup restore manager script is located by typing

```
cd /opt/nortel/bkresmgr/cbm
```

and pressing the Enter key.

- 6 Start the backup restore manager by typing

```
./bkmgr
```

and pressing the Enter key.

- 7 Invoke the desired step of the backup process by typing

```
bkmgr> <command>
```

where

**command**

is any one of the following commands:

- precheck
- stopprov
- dumpdata
- verify
- startprov
- activatenew

Refer to [Additional information on page 100](#) for further information on commands.

You have completed this procedure.

## Additional information

The following commands are available through telnet:

- **commands:** Lists all the commands that are available in the SBRM CLUI.
- **help [command]:** Displays information on the command, or all commands if no command is specified.
- **exit or quit:** Exits the SBRM CLUI.
- **query status:** Displays the status of the backup at a high level. For example, "Backup in progress" or "Backup failed".
- **query history:** Displays information about most recent backup. For example, "Last backup executed <date> <time> successful".
- **query inventory:** Displays the components available for backup.

- **precheck:** Performs a basic sanity check to ensure the system is in a state to perform a backup. For example, disk space check and subtending application health if applicable.
- **stopprov:** Stops the provisioning process.
- **dumpdata:** Backs up the critical data.
- **startprov:** Starts the provisioning process (if stopped)
- **verify:** Checks the validity of the backed up data. For example, validates the database data.
- **activatenew:** Marks the new backup data as the current backup.

The following commands are not available through telnet:

- **backup full:** Performs a complete backup. If a failure is encountered, the process stops, and manual intervention is required to recover from the failure.
- **backup auto:** Performs a complete backup. If a failure is encountered, the backup process will restore provisioning if it was stopped by the backup process.
- **backup abort:** Aborts the backup after completion of the current step, and restarts provisioning if it was stopped by the backup process.

---

## How to backup an XA-Core office image from disk to tape

---

### Application

Use this procedure to copy the office image files of an eXtended Architecture Core (XA-Core). Use this procedure to copy the office image files from a disk to a digital audio tape (DAT) cartridge in an XA-Core shelf.

### Interval

Perform this procedure each week or as indicated in the routine maintenance schedule for your office.

### Common procedures

There are no common procedures.

### Action

This procedure contains a summary flowchart and a list of steps. Use the flowchart to review the procedure. Follow the steps to perform this procedure.

#### How to backup an XA-Core office image from disk to tape

##### *At the MAP*

- 1 To access the MAP CI level display, type:  
**>QUIT ALL**  
and press the Enter key.  
Example of a MAP response  
CI:
- 2 To access the image table of contents (ITOC) user interface, type:  
**>ITOC CI**  
and press the Enter key.  
Example of a MAP response  
ITOC User Interface is now active.  
ITOC CI:
- 3 To list the boot file for the XA-Core in ITOC, type:  
**>LISTBOOTFILE XA**  
and press the Enter key.

### Example of a MAP response

Image table Of Contents for XA :

```

 A Registered Generic Device File
 L Date Time Name
 R MM/DD/YYYY HH:MM:SS

-- - - - -
0 * 05/17/1999 19:26:29 F02LIMAGE
IMG0517CY_CM

```

**Note:** The example of a MAP response identifies the autoload registered (ALR) image file by an asterisk (\*) in the ALR column. Each image file has an index number at the beginning of the tuple line. The ALR image in the example of a MAP response has an index number of 0. The XA-Core selects the ALR image file first to boot the switch. If the ALR image file does not boot the switch then the XA-Core selects the next image file. The next image file is by sequence of the index number from the top of the table.

- 4 To list the boot file for the message switch (MS) in ITOC, type

>**LISTBOOTFILE MS**

and press the Enter key.

### Example of a MAP response

Image Table of Contents for MS :

```

 A Registered Generic Device File
 L Date Time Name
 R MM/DD/YYYY HH:MM:SS

-- - - - -
0 * 05/17/1999 19:26:29 F02LIMAGE
IMG0517CY_MS

```

- 5 Determine if the XA-Core and MS have image files that are autoload registered (ALR). The examples of a MAP response in steps <3> and <4> identify the ALR image files by an asterisk (\*) in the ALR column.

**If the image files are**

ALR

not ALR

**Do**

step [6](#)

step [24](#)

- 6 Record the names of the office image files for XA-Core and MS that are ALR. Also record the volume name that has these office image files. The ALR image file is the file that you copy to the XA-Core tape.

**Note 1:** In the example of a MAP response in step 3, the name of the office image file for XA-Core is IMG0517CY\_CM. Image file IMG0517CY\_CM is ALR. Image file IMG0517CY\_CM is in volume F02LIMAGE.

**Note 2:** In the example of a MAP response in step 4, the name of the office image file for the MS is IMG0517CY\_MS. Image file IMG0517CY\_MS is ALR. Image file IMG0517CY\_MS is in volume F02LIMAGE.

- 7 To quit the ITOCCI user interface, type:

**>QUIT**

and press the Enter key.

Example of MAP response

CI:

### **At the shelf**

8



#### **WARNING**

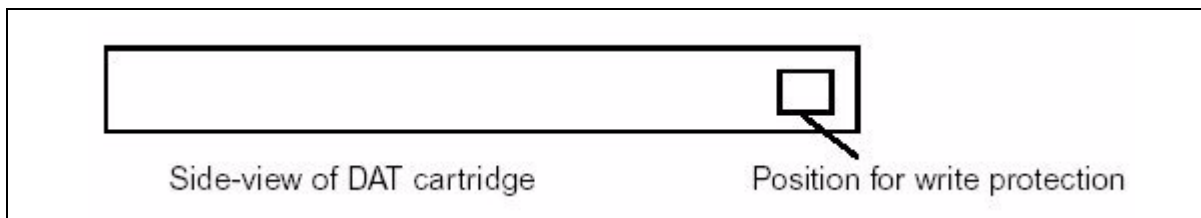
**Static electricity damage**

Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP) when you handle the tape and packlet. The use of the wrist strap protects the packlets against damage caused by electrostatic discharge (ESD).

- Determine from office records or office personnel if the DAT tape drive is clean. Refer to the XA-Core procedure "How to clean the XA-Core tape drive" in the *XA-Core Maintenance Manual*, 297-8991-510.
- 9 Get a tape cartridge that has the approval of Nortel. Determine the tape planned for a backup of an office image. Determine the tape to use from the office records or from office personnel.
  - 10 Make sure the tape write protection is at the position that permits recording (closed). The tape write protection is an entrance on one side of the tape that has a sliding door. The sliding door is open for write protection and closed to allow a write to the tape.



## Write protection of DAT cartridge



- 11 Insert the DAT tape cartridge into the XA-Core tape drive and close the drive door. The XA-Core tape drive is in the input/output processor (IOP) card of the XA-Core shelf.

### *At the MAP*

12



#### **CAUTION**

**File of tape lost when formatted**

If the tape had files, the formatting of the tape loses the files. Make sure the tape has no files that your office needs.

To access the MAP disk utility, type:

**>DISKUT**

and press the enter key.

Example of a MAP response:

Disk utility is now active.

DISKUT:

- 13 To insert the tape in the MAP disk utility, type  
**>INSERTTAPE snnpTAPE WRITELABEL label\_name**  
and press the enter key.  
where  
**s**  
is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device  
**nn**  
is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**

is the upper (U) or lower (L) packlet position of the IOP that has the tape device

**label\_name**

is the alphanumeric name of the tape label that records the data. The name can be up to 32 characters long. If blank spaces are in the label name then enclose the label name with quotation marks.

Example of MAP input:

```
>INSERTTAPE F02UTAPE WRITELABEL IMAGE_1
```

Example of a MAP response

```
***** WARNING *****
```

```
Writing the label IMAGE_1 to tape volume
F02UTAPE on node CM will destroy all files
stored on this tape volume.
```

```
Do you want to continue?
```

```
Please confirm ("YES", "Y", "NO", or "N")
```

**14** To confirm the command, type:

```
>YES
```

and press the enter key.

Example of a MAP response:

```
The INSERT operation may take up to 5 minutes to
tension the tape.
```

```
A tape is now available to user on unit 0, node
CM.
```

```
Name IMAGE_1 has been written to the tape label.
```

**15** To list the files in the volume that contains the office image, type:

```
>LISTFL vol_name
```

and press the enter key.

where

**vol\_name**

is the name of the disk volume that contains the office image files

Example of MAP input

```
>LISTFL F02LIMAGE
```

**Example of a MAP response**

File information for volume F02LIMAGE:

{NOTE: 1 BLOCK = 512 BYTES }

```

FILE NAME O R I O O V FILE MAX
NUM OF FILE LAST
 R E T P L L CODE REC
RECORDS SIZE MODIFY
 G C O E D D LEN
IN IN DATE
 C N FILE
BLOCKS

IMG0517CY_MS I F Y 0 1020
7542 15360 990517
IMG0517CY_CM I F Y 0 1020
165180 329728 990517

```

**Note:** A volume can have more files listed by command LISTVOLS than by command LISTFL in the MAP disk utility. The difference in the number of files between the commands is because of directory files not displayed by command LISTFL.

- 16** Begin the disk to tape backup process. To create a backup copy of the XA-Core image file, type:

**>BACKUP FILE file\_name snnpTAPE**

and press the Enter key.

where

**s**

is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn**

is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**

is the upper (U) or lower (L) packlet position of the IOP that has the tape device

Example of MAP input:

```
>BACKUP FILE IMG0517CY_CM F02UTAPE
```

Example of a MAP response

FTFS file IMG0517CY\_CM on disk volume F02LIMAGE on node CM backed up as file IMG0517CY\_CM on tape device F02UTAPE on node CM.

| If the command was | Do                      |
|--------------------|-------------------------|
| successful         | step <a href="#">17</a> |
| not successful     | step <a href="#">24</a> |

- 17 To create a backup copy of the MS image file, type:

```
>BACKUP FILE file_name snnp TAPE
```

and press the enter key.

where

**file\_name**

is the name of the MS image file that requires backup to tape

**s**

is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn**

is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**

is the upper (U) or lower (L) packlet position of the IOP that has the tape device

Example of MAP input

```
>BACKUP FILE IMG0517CY_MS F02UTAPE
```

Example of a MAP response

FTFS file IMG0517CY\_MS on disk volume F02LIMAGE on node CM backup up as file IMG0517CY\_MS on tape device F02UTAPE on node CM.

| If the command was | Do                      |
|--------------------|-------------------------|
| successful         | step <a href="#">18</a> |
| not successful     | step <a href="#">24</a> |

- 18** To check the backup copies of the image files on the tape, type

**>LISTFL snnpTAPE**

and press the enter key.

where

**s**

is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn**

is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**

is the upper (U) or lower (L) packlet position of the IOP that has the tape device

Example of MAP input

**>LISTFL F02UTAPE**

Example of a MAP response

File information for tape volume F02UTAPE, node CM:

{Note: 1 BLOCK = 512 BYTES}

```

CREATE ORG FILE V FILE NUM OF REC FILE NAME
DATE TYPE CODE L SIZE IN RECORDS LEN
D BLOCKS IN FILE

```

```
990520 IMAG 0 329070 165180 1020 IMG0517CY_CM
990520 IMAG 0 15026 7542 1020 IMG0517CY_MS
```

- 19** To eject the tape from the MAP disk utility after the backup procedure completes, type

**>EJECTTAPE snnpTAPE**

and press the enter key.

where

**s**

is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn**

is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**

is the upper (U) or lower (L) packlet position of the IOP that has the tape device

Example of MAP input

**>EJECTTAPE F02TAPE**

Example of a MAP response

The EJECT operation may take up to 5 minutes to position the tape to the beginning.

Rewind of tape F02UTAPE, unit 0, on node CM is completed.

This tape device is not available to the user now.

**20** To exit the MAP disk utility and return to the MAP CI level, type

**>QUIT**

and press the Enter key.

Example of a MAP response

CI:

### ***At the shelf***

**21**



#### **WARNING**

**Static electricity damage**

Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP) when you handle the tape and packlet. The use of the wrist strap protects the packlets against damage caused by electrostatic discharge (ESD).

Remove the tape cartridge from the tape drive. Set the tape write protection to the position that does not permit recording (open). The tape write protection is an entrance on one side of the tape that has a sliding door. The sliding door is open for write protection and closed to allow a write to the tape.

### Write protection of DAT cartridge



- 22** Store the tape cartridge per office procedure.
- 23** Go to step [25](#).
- 24** For additional help, contact the next level of support.
- 25** You have completed this procedure.

---

## Perform a manual backup of the Policy Controller database

---

### Purpose of this procedure

Use this procedure to perform a backup of the active Policy Controller unit Policy Controller application database. Use this procedure to make regular backup copies of the database or as a precautionary activity before starting any type of upgrade to the Policy Controller application. This procedure may be used as a standalone task or as part of a higher level upgrade activity.

### Limitations and Restrictions

#### ATTENTION

If you perform provisioning changes during this procedure, it can lead to database corruption and possible system outages. To ensure that you create an accurate and complete copy of the active unit database, verify that all provisioning changes are stopped before continuing this procedure.

### Prerequisites

#### ATTENTION

The Policy Controller database and the CS 2000 database must always be in sync. CS 2000 core images, CS 2000 GWC Manager Oracle database backups, and the Policy Controller application backups must always be maintained in sync for emergency recovery. To ensure they are in sync, perform images and backups at the same time.

### Action

#### *At the Policy Controller command line interface*

- 1 Log onto the active Policy Controller unit and change to the root user.
- 2 Change directory to the database directory by typing  
**# cd /opt/apps/database/solid/dbfiles**  
and pressing the Enter key.



- 3 Put a copy of the database for the active unit in the backup directory by typing

```
cp solid.db /opt/apps/database/solid/backup
```

and pressing the Enter key.

**Note:** If other backup copies of the database exist with the same filename, you have the option of deleting those files or putting the backup copy into the backup directory under a new file name.

**Example**

```
cp solid.db
/opt/apps/database/solid/backup/solid.db.backup1
```

- 4 For security purposes, ensure that a backup copy of the database file is transferred to a secure location.

Use the unix **scp** command to make a secure copy of the backup database file to a secure, remote server on your network. This server should be continuously available for cases where a restoration of the Policy Controller application database become necessary, such as during an upgrade rollback. A root password for the remote server may be required.

- 5 You have completed this procedure.

## Call Agent backup

The Call Agent uses two software loads. The first software load includes the platform software such as the operating system and system utilities. The second software load provides the call processing application.

This procedure describes how to make a backup of the call processing application. Images to be backed up are created either manually with the DUMP command, or automatically scheduled with entries in table IMAGEDEV and IMGSCHEDEV.

### At the MAP

- 1 List the available images to determine which image to backup. The image with the asterisk in the ALR column identifies the image that is set to Auto Load Record and is the image to backup.

```

CI:
>ITOC CI
ITOC User Interface is now active.
ITOC CI:
>LBF CM
Image Table Of Contents:
 A Registered Generic Device File
 L Date Time Name
 R MM/DD/YYYY HH:MM:SS

 0 01/22/2003 10:29:53 SD00IMAGE1 SN04_JAN07_CM
 1 01/22/2003 12:07:26 SD00IMAGE0 SN04_JAN22_CM
 2 01/22/2003 13:00:50 SD00IMAGE0 BOTHELL_010903
 3 * 01/30/2003 14:31:47 SD00IMAGE0 IMG_TO_BACKUP

```

### At the Call Agent Manager

- 2 Log in to the inactive Call Agent and change directory to the location of the image.

The location of the image is identified by the value in the Generic Device column as follows:

**/3PC**

is prefixed in all cases

**sd0x/**

is taken from the first four characters in the Generic Device name

**imagex/**

is taken from the remaining characters in the Generic Device name

```
[mtc@hostname mtc]$ cd /3PC/sd00/image0
[mtc@hostname image0]$ ls -l IMG_TO_BACKUP
-rw-r--r-- 1 root root 225820860 Feb 27 11:37 IMG_TO_
[mtc@hostname image0]$
```

**3****ATTENTION**

Do not modify files at this level. Any modification to files must be completed through the MAP.

Open a file transfer protocol (FTP) session to the CS 2000 Core Manager and transfer the file.

```
[mtc@hostname image0]$ ftp <core_manager_ip>
Connected to <core_manager_ip>
220 <core_manager_ip> SFTPD Server (Version 19.0.0.0 Nov 14
Name (<core_manager_ip>:mtc): root
Password: <root_passwd>
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> cd /swd/3pc
250 CWD command successful.
ftp> put IMG_TO_BACKUP
local: IMG_TO_BACKUP remote: IMG_TO_BACKUP
227 Entering Passive Mode (10,40,44,6,195,224)
150 Opening data connection for IMG_TO_BACKUP (binary mode)
226 Transfer complete.
225820860 bytes sent in 332 secs (6.7e+02 Kbytes/sec)
ftp> bye
221 Goodbye.
```

**At the SDM**

- 4** Insert a DAT cassette.

**At the CS 2000 Core Manager**

- 5 Verify that the size of the transferred file is the same as in [step 2](#) and copy the file to tape.

```
cd /swd/3pc
ls -l
total 19816
-rw-r--r-- 1 swld swld 1527 Feb 27 12:40 000167C42C
-rw-r--r-- 1 swld swld 1527 Feb 26 17:58 000F07C430
-rw-rw-rw- 1 ftpuser maint 225820860 Feb 21 09:56 IMG_TO_B
tar cvf /dev/rmt0 IMG_TO_BACKUP
```

**Note:** Use the `rvf` argument to append to the tape. After the backup completes, optionally verify the integrity of the backup by using `tar tvf /dev/rmt0` to view the contents of the tape.

- 6 Use the `rm` command to erase the oldest image so the volume does not fill up.
- 7 This procedure is complete.

---

## Backing up files to DVD-RW

---

### Application

Use this procedure to copy office images or all the files from a disk volume to a digital video disk read write optical disk (DVD-RW).

**Note:** Rewritable DVDs (DVD+RW) will not work. Use a blank DVD-RW (write once).



#### CAUTION

##### Maximum one volume per DVD-RW

Copy no more than one volume onto a DVD-RW. To copy multiple volumes, use a separate DVD-RW for each volume.

### Interval

Perform this procedure when required by your office.

### Common procedures

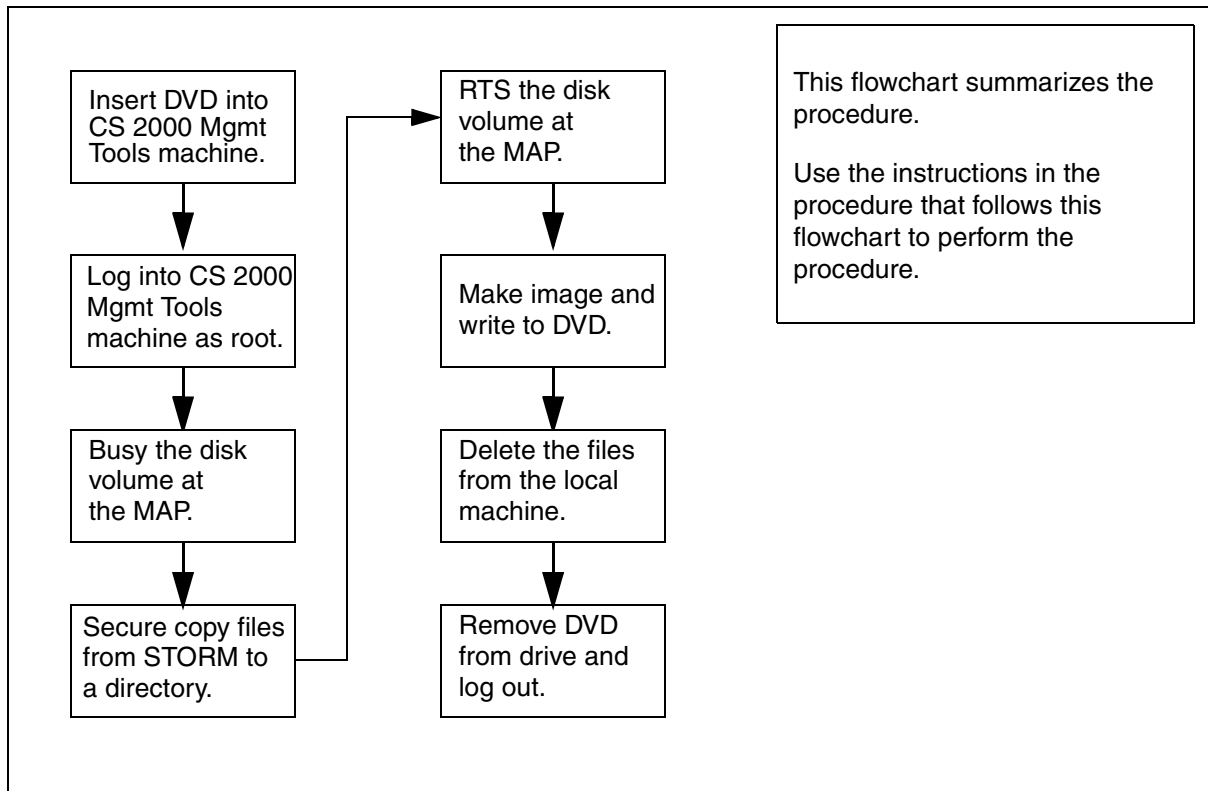
The UNIX commands `mkisofs` and `cdwr` are used. For information about these commands, type **man mkisofs** or **man cdwr** at a terminal prompt.

The IP addresses of the STORM units are determined in [step 1](#). The root password for STORM is needed. The root password for the CS 2000 Management Tools server is needed.

### Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

## Summary of backing up files to DVD-RW



### At the Call Agent Manager

- 1 Quit the maintenance application and then use the mount command to determine the IP addresses of the STORM units.

```
> quit all
[mtc@ip_address mtc]$ mount
```

Determine which STORM unit provides sd00 and which provides sd01. This information is needed in [step 12](#).

```
[mtc@10.40.44.67 mtc]$ mount
/dev/ram0 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0622)
10.40.44.238:/nfsserv/3pc/mtc/tape0 on /TAPE type nfs (rw,rsiz=4096...
10.40.44.239:/nfsserv/3pc/mtc/tape1 on /TAPE1 type nfs (rw,rsiz=409...
10.40.44.238:/nfsserv/3pc/cs/sd00 on /3PC/sd00 type nfs (rw,rsiz=409...
10.40.44.239:/nfsserv/3pc/cs/sd01 on /3PC/sd01 type nfs (rw,rsiz=409...
10.40.44.238:/nfsserv/3pc/mtc/log0 on /var/log_mate type nfs (rw,rsi...
10.40.44.239:/nfsserv/3pc/mtc/log1 on /var/log type nfs (rw,rsiz=409...
```

**At the CS 2000 Management Tools server****2****CAUTION****Maximum one volume**

Copy only *one* volume onto a DVD-RW. To copy multiple volumes, use a separate DVD-RW for each volume.

Determine the volume to backup. Determine the volume from office records or from office personnel. Record the volume name.

- 3** Get a DVD-RW that has the approval of Nortel.
- 4** Insert the DVD-RW (write once DVD) into the DVD tray. If the CS 2000 Management Tools server is a pair of Sun Microsystems Netra 240 machines, put the DVD-RW into the machine with a lit USER LED on the faceplate.

**At a CS 2000 Management Tools server terminal**

- 5** Log in as a maintenance level user such as the maint user. Root permissions are used later in this procedure to write the DVD.
- 6** Change directory to `/data` and create a temporary directory to store the files:

```
$ cd /data
```

```
$ mkdir tmp
```

**Note:** Do not change directory into tmp now. The tmp directory will hold the data to backup.

- 7** Determine the environment shell:

```
$ env | grep SHELL
```

```
SHELL=/bin/ksh
```

- 8** Set a filesize creation limit for this instance of the shell. Choose the **one** that is applicable to your shell. `/bin/ksh` is the default shell:

for `/bin/ksh`:

```
$ ulimit -f 2929688
```

for `/bin/bash`:

```
$ ulimit -f 1464844
```

for `/bin/csh`:

```
$ limit filesize 1500 megabytes
```

### At the MAP

- 9 Determine the approximate size of the image or volume:

| Data to backup   | How to determine size                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |                  |        |        |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------|--------|--------|------|------|--|------------------|-----|---------|------|--------|--|-------------|-----|----|----|------|--|-----|--|------|--------|--|------------------|-----|-------|-----|----|--------|------------------|-------|--------|--------|--------|--------|------------------|-------|--------|------|-------|--------|
| image            | <p>Listfile the volume that the image is in:</p> <p>&gt; DISKUT; LF &lt;vol_name&gt;</p> <div><p>&gt; LF SD00ADUMP0</p><p>File information for volume SD00ADUMP0:</p><p>{NOTE: 1 BLOCK = 512 BYTES }</p><table><tr><td>FILE NAME</td><td>O R I O O V FILE</td><td>MAX</td><td>NUM OF</td><td>FILE</td><td>LAST</td></tr><tr><td></td><td>R E T P L L CODE</td><td>REC</td><td>RECORDS</td><td>SIZE</td><td>MODIFY</td></tr><tr><td></td><td>G C O E D D</td><td>LEN</td><td>IN</td><td>IN</td><td>DATE</td></tr><tr><td></td><td>C N</td><td></td><td>FILE</td><td>BLOCKS</td><td></td></tr><tr><td>S040210135002HIS</td><td>O V</td><td>0 255</td><td>276</td><td>27</td><td>040210</td></tr><tr><td>S040210135002_CM</td><td>I F Y</td><td>0 1020</td><td>220288</td><td>438855</td><td>040210</td></tr><tr><td>S040210135002_MS</td><td>I F Y</td><td>0 1020</td><td>7803</td><td>15546</td><td>040210</td></tr></table></div> <p>The approximate size of the image in megabytes is NUM OF RECORDS IN FILE / 1000:</p> <p>220288 / 1000 = 220 MB</p> | FILE NAME | O R I O O V FILE | MAX    | NUM OF | FILE | LAST |  | R E T P L L CODE | REC | RECORDS | SIZE | MODIFY |  | G C O E D D | LEN | IN | IN | DATE |  | C N |  | FILE | BLOCKS |  | S040210135002HIS | O V | 0 255 | 276 | 27 | 040210 | S040210135002_CM | I F Y | 0 1020 | 220288 | 438855 | 040210 | S040210135002_MS | I F Y | 0 1020 | 7803 | 15546 | 040210 |
| FILE NAME        | O R I O O V FILE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | MAX       | NUM OF           | FILE   | LAST   |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
|                  | R E T P L L CODE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | REC       | RECORDS          | SIZE   | MODIFY |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
|                  | G C O E D D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | LEN       | IN               | IN     | DATE   |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
|                  | C N                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           | FILE             | BLOCKS |        |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
| S040210135002HIS | O V                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 0 255     | 276              | 27     | 040210 |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
| S040210135002_CM | I F Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0 1020    | 220288           | 438855 | 040210 |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
| S040210135002_MS | I F Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0 1020    | 7803             | 15546  | 040210 |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
| volume           | <p>Listvols the volume with the megabyte option:</p> <p>&gt; DISKUT; LV SD00TEMP MB</p> <p>Subtract FREE MBYTES from TOTAL MBYTES to determine the approximate size of the volume:</p> <p>400 - 340 = 60 MB</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |           |                  |        |        |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |

- 10 If backing up an entire volume, enter the DISKADM level and busy the volume:

```
> QUIT ALL
> DISKADM <sd0x>; BSY <volname>
> QUIT
sd0x
is SD00 or SD01
```



**volname**

is the name of the volume such as TEMP or ADUMPO

*The BSY command fails if applications have open files on any volume for the device. A busied disk may affect data recording or retrieval for applications. Consider [step 13](#) to RTS the volume as soon as possible or convenient after copying the files.*

*If applications are active and writing to the volume, determine if the application can ROTATE the disk writing activity to a backup volume. If unsure, contact your next level of support.*

**At a CS 2000 Management Tools server terminal**

- 11** Ensure that enough disk space is available for the data to record. Twice the space determined in [step 9](#) is needed:

```
$ df -k /data
```

*The free space on the device that /data is mounted is printed. The value for “avail” is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes. Ensure that there is free space for two times the size of the data to record.*

```
$ df -k /data
```

| Filesystem      | kbytes  | used  | avail   | capacity | Mounted on |
|-----------------|---------|-------|---------|----------|------------|
| /dev/md/dsk/d20 | 3082223 | 14412 | 2876454 | 5%       | /data      |

2876454 / 1000 = 2876 MB free

- 12** Secure copy the files from the STORM unit to the /data/tmp directory created in [step 6](#). Enter the root password for the STORM unit when prompted:

```
$ scp -r "root@<stormip>:</path_to_files>" /data/tmp
```

**Note:** There is a space before the /data/tmp argument.

**stormip**

is the IP Address of the STORM unit such as 10.40.44.238. Use the value determined in [step 1](#).

**/path\_to\_file**

is the absolute path to the files on the STORM unit to copy such as /nfsserv/3pc/cs/sd00/temp/\*

**Example**

Copy an office image named S040210135002\_CM from SD00ADUMP0:

```
$ scp -r
```

```
"root@<stormip>:/nfsserv/3pc/cs/sd00/adump0/S040210135002_CM" /data/tmp
```

**Note:** The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a "yes." The root password for the STORM unit is needed.

*The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.*

**At the MAP**

- 13 If the volume was busied in [step 10](#), enter the DISKADM level and RTS the copied volumes:

```
> DISKADM <sd0x>; RTS <volname>
> QUIT
```

**At a CS 2000 Management Tools server terminal**

- 14 If only image files are transferred, and the files do not end in \_CM or \_MS, rename the files to include the file attributes IMG and 1020:

```
$ mv <image_filename> <image_filename>.IMG1020
```

**Example**

```
$ mv raleigh_04wk06 raleigh_04wk06.IMG1020
```

**Note:** If the name of the image already ends in \_CM or \_MS, skip this step.

- 15 Change directory out of /data/tmp and make an ISO9660 image named dvdimage.iso with Rock Ridge extensions from the files in tmp:

```
$ cd /data
```

```
$ mkisofs -R -o /data/dvdimage.iso -r /data/tmp
```

*Status is printed to the terminal:*

## Create dvdimage.iso with mkisofs command

```
$ mkisofs -R -o /data/dvdimage.iso -r /data/tmp
4.56% done, estimate finish Tue Feb 10 14:52:00 2004
9.11% done, estimate finish Tue Feb 10 14:52:00 2004
13.67% done, estimate finish Tue Feb 10 14:52:00 2004
...
95.67% done, estimate finish Tue Feb 10 14:52:05 2004
Total extents actually written = 109764
Total translation table size: 0
Total rockridge attributes bytes: 421
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 8000
109764 extents written (214 Mb)
$
```

- 16 Become the root user:

```
$ su - root
```

Provide the root password at the prompt.

- 17 Optionally verify the ISO9660 image:

```
lofiadm -a /data/dvdimage.iso /dev/lofi/1
mount -F hsfs /dev/lofi/1 /mnt
ls -as1 /mnt
```

*The contents of the ISO 9660 image are displayed. These files will be written to the DVD-RW. Ensure the display looks similar to the following image.*

**Note 1:** If the `lofiadm` command reports the error “`lofiadm: could not map file /data/dvdimage.iso to /dev/lofi/1: Device busy,`” then the first loopback file driver is already in use. Reenter the command and substitute `/dev/lofi/2` for `/dev/lofi/1`. Continue incrementing the number until the command succeeds and then use the successful value in the mount command.

**Note 2:** If the `mount` command reports the error “`mount: /dev/lofi/1 is already mounted, /mnt is busy, or allowable number of mount points exceeded,`” unmount the `/mnt` directory with the **`umount /mnt`** command and reenter the mount command.



*If the error response "Media in the device is not writable" is returned, verify that the CDROM tray is closed.*

*Approximately two minutes pass before progress is printed to the screen. After the first 1% is written, each additional percent requires about two seconds.*

## CDRW command progress

```
cdrw -d cdrom0 -i /data/dvdimage.iso
Initializing device...done.
Preparing to write DVD
Writing track 1 ... 99 %
```

*Approximately nine minutes pass before the command completes.*

```
done.
done.
Finalizing (Can take up to 4 minutes)...done.
$
```

*The CDROM tray on the CS 2000 Management Tools server ejects. **Close the CDROM tray and continue this procedure to verify the contents of the DVD-RW.***

- 21** Check that ISO9660 image recorded correctly:

```
ls -asl /cdrom/cdrom
```

*The contents of the DVD-ROM are printed.*

- 22** Unmount the DVD-RW, eject it, and exit from root privilege:

```
eject cdrom
```

If the ISO 9660 image was verified with the lofiadm command, remove the loopback file driver device:

```
umount /mnt
```

```
lofiadm -d /dev/lofi/1
```

**Note:** If /dev/lofi/2 was used above, substitute /dev/lofi/2 in this command.

Exit from root privilege:

```
exit
```

```
$
```

*The dollar sign command prompt returns.*

- 23** Remove the local copies of the files:

```
$ rm /data/tmp/*
$ rm /data/dvdimage.iso
```

***At the CS 2000 Management Tools server***

- 24** Remove the DVD-RW from the tray and close the tray. Label the DVD-RW.
- 25** Store the DVD-RW per office procedure.
- 26** This procedure is complete.

---

## Perform a manual backup of the Session Server database

---

### Purpose of this procedure

Use this procedure to perform a backup of the active Session Server unit SIP Gateway application database. Use this procedure to make regular backup copies of the database or as a precautionary activity before starting any type of upgrade to the SIP Gateway application. This procedure may be used as a standalone task or as part of a higher level upgrade activity.

### Limitations and Restrictions

#### ATTENTION

SIP Gateway application provisioning activities must be suspended during the time of the database backup in order to ensure that an accurate and complete copy of the active unit database is created. However, call processing is not affected.

### Prerequisites

#### ATTENTION

The SIP Gateway application database must be in sync with the CS 2000 to ensure an accurate copy of the active unit database is created. Verify this condition using procedure [Verify synchronization status of Session Server units on page 129](#).

### Action

#### *At the Session Server CLI or Integrated EMS client*

- 1 Log onto the active Session Server unit and change to the root user.
- 2 Change directory to the database directory by typing  
**# cd /opt/apps/database/solid/dbfiles**  
and pressing the Enter key.
- 3 Put a copy of the database for the active unit in the backup directory by typing  
**# cp solid.db /opt/apps/database/solid/backup**

and pressing the Enter key.

**Note:** If other backup copies of the database exist with the same filename, you have the option of deleting those files or putting the backup copy into the backup directory under a new file name.

**Example**

```
cp solid.db
/opt/apps/database/solid/backup/solid.db.backup1
```

- 4 For security purposes, ensure that a backup copy of the database file is transferred to a secure location.  
  
Use the unix **scp** command to make a secure copy of the backup database file to a secure, remote server on your network. This server should be continuously available for cases where a restoration of the SIP Gateway application database become necessary, such as during an upgrade rollback. A root password for the remote server may be required.
- 5 You have completed this procedure.



## Verify synchronization status of Session Server units

### Purpose of this procedure

Use this procedure to determine the synchronization status of the Session Server units. This procedure may be used as a standalone task or as part of a higher level activity.

### Limitations and restrictions

There are no restrictions for performing this procedure.

### Prerequisites

There are no prerequisites for performing this procedure.

### Action

#### *At the Session Server GUI or Integrated EMS client*

- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

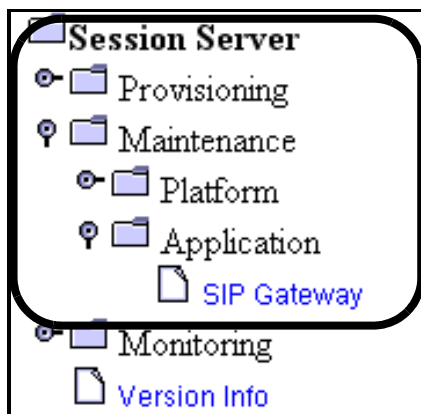
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

[Succession Communication Server 2000 NCGL Platform Manager](#)

[Succession Communication Server 2000 Session Server Manager](#)

- 2 At the Session Server folder, click the **Maintenance folder**, then click the **Application** folder.



- 3 Click on the **SIP Gateway** folder to open it.

- 4 At the bottom of the SIP Gateway Maintenance panel, locate and click the **QueryInfo** button.

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |
| <div>Refresh</div> <div><b>QueryInfo</b></div>         |                                         |

- 5 The synchronization status of the units is displayed at the bottom of the query results panel.

If the units are not in sync, execute procedure *View Session Server alarms*, found in the Session Server Fault Management NTP, NN10332-911, and check for alarm conditions.

|                                                 |
|-------------------------------------------------|
| Last Performed Operation: Query Number of Calls |
| Result: Passed                                  |
| Number Of Active Calls: 0                       |
| <b>SIP Gateway is: In Sync</b>                  |
| SIP Gateway Cold SwAct                          |

- 6 The procedure is complete.

---

## Saving the Ethernet Routing Switch 8600 boot configuration file

---

The Ethernet Routing Switch 8600 boot configuration can be saved to a file using the Boot Monitor Command Line Interface (CLI). You must have access to the Boot Monitor CLI through a direct connection to the switch or a Telnet connection. For more information on accessing the Boot Monitor CLI, refer to “Managing the Ethernet Routing Switch 8000 Series Switch Using the Command Line Interface Release 3.2,” 313194-\*.

**Note:** You must be directly connected to the switch to initiate a Boot Monitor session. You can connect using a Telnet connection only if the Boot Monitor CLI is already active.

### Save the boot configuration

#### *At the Boot Monitor CLI*

- 1 Issue the save command by typing

```
monitor# save <save_type> [file <value>]
[verbose] [standby <value>] [backup <value>]
```

where

**save\_type**

specifies what to save. Possible values for this parameter are config, bootconfig, log, and trace.

**file <value>**

is a filename in one of the following formats:

- [a.b.c.d]: <file>
- /pcmcia/<file>
- /flash/<file>

**verbose**

saves default and current configuration. if you omit this parameter, only parameters you have changed are saved.

**standby <value>**

saves the specified file name to the standby CPU (currently not supported)

**backup <value>**

saves the specified file name and identifies the file as a backup file

**Example**

```
save config file ralph.cfg backup 2
```

**Note:** To save a file to the standby CPU, you must enable TFTP on the standby CPU. To enable TFTP, enter flags tftpd true in the Boot Monitor CLI or config bootconfig flags tftpd true in the Run-Time CLI.

- 2** You have completed this procedure.

---

## Backing up UAS configuration files

---

All configuration data supporting the operation of the UAS is stored in configuration files. The configuration files include:

- uas.conf - containing configuration parameters that support the function of the UAS, including CG6000C card settings, Call Agent definition, APS hostname definition, network element settings, and conferencing service state definition
- ugw.conf - containing trunk configuration information for PRI Solutions
- snmpd.cnf - containing parameters that support the SNMP function, including management station address, SNMP user names, community names, and trap version
- hosts - containing parameters that support the function of the APS, including APS hostname and IP address
- atmhard.con - containing ATM bearer interface settings that link a local port ATM address to a particular ATM interface port
- atmconn.con - containing ATM bearer connections settings that provide the UAS with a remote gateway's name and ATM address
- mainsa.conf - containing Main Subagent program settings specifying the kinds of error and log messages to be sent to the management station
- atmSvcProfile.con - containing data on Switched Virtual Channel (SVC) traffic parameters associated with AAL2 SVCs
- atmhardloop.con - containing information associated with the loopback of SVCs

At the time of installation, the UAS is configured to automatically back up configuration files each day at 2:00 am. If an APS node is configured in the network, all UAS nodes in the network can be backed up to the APS node. If an APS node is not configured in the network, the configuration files for UAS nodes in the network can be backed up, instead, to a remote UNIX server. This procedure enables you to set up automatic backup to a remote server.

## Backing up UAS configuration files

### *At the Windows desktop interface*

- 1 This step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server.

- a Open a command interface by performing the following steps:

- i select **Start -> Run**

- ii type **cmd** in the window that displays

- iii press Enter

- b Open a telnet session to the remote UNIX server and log in as the Root user. Then enter:

```
cd /;mkdir /opt;chmod 777 opt
```

```
cd /opt;
```

```
mkdir uas;chmod 777 uas
```

```
cd uas;
```

```
mkdir uas_conf_backup;chmod 777
```

```
uas_conf_backup
```

```
cd /
```

```
cd /opt/uas/uas_conf_backup
```

- c Configure NFS to share the “/opt/uas” filesystem and start the NFS server:

```
echo "share -F nfs /opt/uas" >>
/etc/dfs/dfstab
```

**Note:** The commands from this point forward are specific for a Sun Solaris system.

```
/etc/init.d/nfs.server start
```

- d Create a user login called “Administrator” that does not require a password:

```
/usr/sbin/useradd -d
```

```
/export/home/Administrator -g 1 -s /bin/ksh
```

```
-m -u 1002 Administrator 2> /dev/null
```

```
passwd -d Administrator 2> /dev/null
```

- 2 At the local system console, enter the IP address of the remote server in the “Backup Storage IP” field of the Local Configuration Interface GUI screen, using the procedure “Modifying

configuration parameters through the Local Configuration Interface GUI” in the document, NN10095-511, entitled “UAS Configuration Management.”

- 3** You have completed this procedure.

---

## Configuring automated INI file backups

---

This procedure enables you to configure automated INI file backups.

**Note:** This procedure pertains to both the Media Server 2010 and the Media Server 2020.

### ***At the Windows desktop interface***

- 1 Open a telnet connection to the CS 2000 Management Tool.
- 2 Log in with the appropriate user name.  
**Note:** The user name must be a member of the “succssn” and “emsadm” groups.
- 3 Invoke the MS 2000 Series CLUI by entering the following on the command line:  
**`/opt/nortel/NTsesm/bin/ms2000.sh`**
- 4 When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- ```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 5 Press 5 to configure automated INI file backups.

The current automated INI backup settings display:

```
Current Automated INI Backup Settings
```

```
=====
```

```
Automated INI Backup Time      = 02:00
```

```
Automated INI Backup Enabled = true
```

```
Would you like to change the Automated INI Backup
Settings? (y/n)
```


- 6** Follow the prompts to change the automated INI backup settings or press Enter to return to the Media Server 2000 series CLUI main menu.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- 1) Display list of MS 2000 series nodes
- 2) Node Maintenance and Configuration
- 3) Backup INI file for all nodes
- 4) Copy a file to the SDM/CBM
- 5) Configure Automated INI file backup
- x) EXIT CLUI

Enter selection (1 - 5, x)

- 7** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 8** Enter exit to close the telnet session.
- 9** You have completed this procedure.

Changing the SNMP community string password for a Media Server 2010 node

This procedure enables you to change the SNMP community string password for a Media Server 2010 node.

Note: After making configuration changes, execute a soft reset of the Media Server to burn the new configuration to flash memory. Refer to the *Performing a soft reset on a Media Server 2000 series node* section of this document.



CAUTION

For proper operation with the IEMS, the SNMP community string must match the community string used when adding the Media Server 2010 node to the IEMS topology.

At the Windows desktop interface

- 1 Open a telnet connection to the CS 2000 Management Tool.
- 2 Log in with the appropriate user name.
Note: The user name must be a member of the “succssn” and “emsadm” groups.
- 3 Invoke the MS 2000 Series CLUI by entering the following on the command line:

```
/opt/nortel/NTsesm/bin/ms2000.sh
```

- 4 When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- ```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 5** Enter 2 to access Node Maintenance and Configuration menu.
- 6** When prompted, enter the IP address of the Media Server node.  
The *Main Menu* displays.

```
*** Main Menu for MS2010 at 172.17.40.230 ***
```

- 1) Maintenance Menu
- 2) Configuration Menu
- x) EXIT

Enter selection (1 - 2, x)

- 7** Enter 2 to access the Configuration Menu.

The *Main Configuration Menu* displays.

```
Main Configuration Menu for MS2010 at 172.17.40.230
```

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security
- x) EXIT

Enter selection (1 - 4, x)

- 8** Press 4 to access the SNMP configuration and security menu.

The *SNMP Configuration and Password Management Menu* displays.

```
*** SNMP Configuration and Password Menu for MS2010
at 172.17.40.230 ***
```

- 1) Setup Trusted SNMP Managers
- 2) Configuring SNMP Trap Destinations
- 3) Change SNMP Community String password
- 4) Change File Upload and Download user and password
- ?) Help
- x) EXIT

Enter selection (1 - 4, ?, x)

- 9** Press 3 to change the SNMP community string password.

The following message displays:

```
** SNMP Community String Password Management **
```

Would you like to change the SNMP Community password for this node? (y/n)

>

- 10** Press y to change the SNMP community password, or enter 'n' to return to the SNMP Configuration and Password Management menu.

The following message displays.

\*\*\* WARNING \*\*\*

This password will be written to the MS2010 and is the only password that can be used for either reading from or writing to the node via SNMP. If there are other managers that must communicate to this MS2010 node then you will need to go to that manager and reconfigure the community strings it uses to communicate with this MS2010 node. The password you are entering here will be used for both the read and write SNMP community strings.

Press <enter> to continue

- 11** Press Enter. The following message displays.

Enter the SNMP password for the CLUI to use when communicating with the 172.17.40.230 MS2010 node. The password must be alpha numeric and can be up to 255 characters long. Return to exit.

>

- 12** Enter the new SNMP community password. The following message displays.

Re-enter the Password

>

- 13** Enter the new SNMP community password again. The following message displays.

Save the SNMP password change? (y/n)

>

- 14** Enter y to save the new community password. The *SNMP Configuration and Password Management Menu* displays.

\*\*\* SNMP Configuration and Password Menu for MS2010 at 172.17.40.230 \*\*\*

1) Setup Trusted SNMP Managers

- 2) Configuring SNMP Trap Destinations
- 3) Change SNMP Community String password
- 4) Change File Upload and Download user and password
- ? ) Help
- x) EXIT

Enter selection (1 - 4, ?, x)

- 15** Follow the prompts to return to the *Media Server 2000 Series CLUI Main Menu*.
- 16** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 17** Enter exit to close the telnet session.  
  
**Note:** After making configuration changes, execute a soft reset of the Media Server to burn the new configuration to flash memory. Refer to the *Performing a soft reset on a Media Server 2000 series node* section of this document.
- 18** You have completed this procedure.

## Changing the SNMP community string password for a Media Server 2020 node

This procedure enables you to change the SNMP community string password for a Media Server 2020 node.

**Note:** After making configuration changes, execute a soft reset of the Media Server to burn the new configuration to flash memory. Refer to the *Performing a soft reset on a Media Server 2000 series node* section of this document.



### CAUTION

For proper operation with the IEMS, the SNMP community string must match the community string used when adding the Media Server 2020 node to the IEMS topology.

### At the Windows desktop interface

- 1 Open a telnet connection to the CS 2000 Management Tool.
- 2 Log in with the appropriate user name.  
**Note:** The user name must be a member of the “succssn” and “emsadm” groups.
- 3 Invoke the MS 2000 Series CLUI by entering the following on the command line:

```
/opt/nortel/NTsesm/bin/ms2000.sh
```

- 4 When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- ```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 5** Enter 2 to access Node Maintenance and Configuration menu.
- 6** When prompted, enter the IP address of the Media Server node.
The *Main Menu* displays.

```
*** Main Menu for MS2020 at 172.17.40.221 ***
```

- 1) Maintenance Menu
- 2) Configuration Menu
- x) EXIT

Enter selection (1 - 2, x)

- 7** Enter 2 to access the Configuration Menu.
The *AAL2 Main Configuration Menu* displays.

```
*** AAL2 Main Configuration Menu for MS2020 at  
172.17.40.221 ***
```

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security
- 5) Configure ATM loopback table
- 6) Display SVC Connection table
- 7) Configure ATM port table
- 8) Configure Remote Gateway table
- 9) Configure AAL2 PVC table
- 10) Configure SVC Profile table
- x) EXIT

Enter selection (1 - 10, x)

- 8** Press 4 to access the SNMP configuration and security menu.
The *SNMP Configuration and Password Management Menu* displays.

```
*** SNMP Configuration and Password Menu for MS2020  
at 172.17.40.221 ***
```

- 1) Setup Trusted SNMP Managers
- 2) Configuring SNMP Trap Destinations
- 3) Change SNMP Community String password
- 4) Change File Upload and Download user and password

?) Help

x) EXIT

Enter selection (1 - 4, ?, x)

9 Press 3 to change the SNMP community string password.

The following message displays:

```
** SNMP Community String Password Management **
```

```
Would you like to change the SNMP Community password  
for this node? (y/n)
```

>

10 Press y to change the SNMP community password, or enter 'n' to return to the SNMP Configuration and Password Management menu.

The following message displays.

```
*** WARNING ***
```

```
This password will be written to the MS2020 and  
is the only password that can be used for either  
reading from or writing to the node via SNMP. If  
there are other managers that must communicate  
to this MS2020 node then you will need to go to  
that manager and reconfigure the community  
strings it uses to communicate with this MS2020  
node. The password you are entering here will be  
used for both the read and write SNMP community  
strings.
```

```
Press <enter> to continue
```

11 Press Enter. The following message displays.

```
Enter the SNMP password for the CLUI to use when  
communicating with the 172.17.40.221 MS2020  
node. The password must be alpha numeric and can  
be up to 255 characters long. Return to exit.
```

>

12 Enter the new SNMP community password. The following message displays.

```
Re-enter the Password
```

>

- 13** Enter the new SNMP community password again. The following message displays.

Save the SNMP password change? (y/n)

>

- 14** Enter y to save the new community password. The *SNMP Configuration and Password Management Menu* displays.

*** SNMP Configuration and Password Menu for MS2020
at 172.17.40.221 ***

- 1) Setup Trusted SNMP Managers
- 2) Configuring SNMP Trap Destinations
- 3) Change SNMP Community String password
- 4) Change File Upload and Download user and password
- ?) Help
- x) EXIT

Enter selection (1 - 4, ?, x)

- 15** Follow the prompts to return to the *Media Server 2000 Series CLUI Main Menu*.
- 16** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 17** Enter exit to close the telnet session.

Note: After making configuration changes, execute a soft reset of the Media Server to burn the new configuration to flash memory. Refer to the *Performing a soft reset on a Media Server 2000 series node* section of this document.

- 18** You have completed this procedure.

Backing up INI files for all nodes

This procedure enables you to back up the INI files for all nodes.

Note: This procedure pertains to both the Media Server 2010 and the Media Server 2020. The example screens in this procedure show a Media Server 2010.

At the Windows desktop interface

- 1 Open a telnet connection to the CS 2000 Management Tool.
- 2 Log in with the appropriate user name.

Note: The user name must be a member of the “succssn” and “emsadm” groups.

- 3 Invoke the MS 2000 Series CLUI by entering the following on the command line:

```
/opt/nortel/NTsesm/bin/ms2000.sh
```

- 4 When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- ```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 5 Press 3 to back up the INI files for all nodes.

The following is an example message display:

### **Example**

```
Backup of .ini for node 172.17.40.230 completed and
copied to SDM
```

```
Press <enter> to continue
```

- 6 Press Enter.

The *Media Server 2000 Series CLUI Main Menu* displays.

\*\*\* Media Server 2000 Series CLUI Main Menu \*\*\*

- 1) Display list of MS 2000 series nodes
- 2) Node Maintenance and Configuration
- 3) Backup INI file for all nodes
- 4) Copy a file to the SDM/CBM
- 5) Configure Automated INI file backup
- x) EXIT CLUI

Enter selection (1 - 5, x)

- 7** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 8** Enter exit to close the telnet session.
- 9** You have completed this procedure.

---

## Displaying Media Server 2010 node current configuration

---

This procedure enables you to display the current configuration of the Media Server 2010 node.

### ***At the Windows desktop interface***

- 1** Open a telnet connection to the CS 2000 Management Tool.
- 2** Log in with the appropriate user name.  
**Note:** The user name must be a member of the “succssn” and “emsadm” groups.
- 3** Invoke the MS 2000 Series CLUI by entering the following on the command line:

**`/opt/nortel/NTsesm/bin/ms2000.sh`**

- 4** When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

\*\*\* Media Server 2000 Series CLUI Main Menu \*\*\*

- 1) Display list of MS 2000 series nodes
- 2) Node Maintenance and Configuration
- 3) Backup INI file for all nodes
- 4) Copy a file to the SDM/CBM
- 5) Configure Automated INI file backup
- x) EXIT CLUI

Enter selection (1 - 5, x)

- 5** Enter 2 to access Node Maintenance and Configuration menu.
- 6** When prompted, enter the IP address of the Media Server node.

The *Main Menu* displays.

\*\*\* Main Menu for MS2010 at 172.17.40.230 \*\*\*

- 1) Maintenance Menu
- 2) Configuration Menu
- x) EXIT

Enter selection (1 - 2, x)

- 7** Enter 2 to access the Configuration Menu.

The *Main Configuration Menu* displays.

\*Main Configuration Menu for MS2010 at 172.17.40.230\*

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security
- x) EXIT

Enter selection (1 - 4, x)

**8** Press 1 to display the current configuration for this node.

The current configuration datafill displays:

**Example**

\*Current configuration for MS2010 at 172.17.40.230\*

|                                  |                             |
|----------------------------------|-----------------------------|
| IP Address                       | : 172.17.40.230             |
| Subnet Address                   | : 255.255.248.0             |
| Default Gateway                  | : 172.17.40.1               |
| MG Control Protocol              | : controlPtotocol-MEGACO(2) |
| Software Version                 | : 4.40.9.14                 |
| Lock State                       | : unlocked(2)               |
| Megaco Call Agent IP Address     | : 172.17.40.36              |
| Is Megaco Call Agent Used        | : yes(1)                    |
| Number of Conference Ports       | : 60                        |
| Number of TestTrunk Ports        | : 2                         |
| Number of Lawful Intercept Ports | : 8                         |
| Number of Announcement Ports     | : 50                        |
| APS IP Address                   | : 47.142.89.70              |
| Primary Language                 | : isoLangEnglish(2)         |
| Secondary Language               | : isoLangEnglish(2)         |
| Syslog Server IP                 | : 47.142.89.221             |

Press <enter> to continue

**9** Press enter. The *Main Configuration Menu* displays.

\*Main Configuration Menu for MS2010 at 172.17.40.230\*

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security

x) EXIT

Enter selection (1 - 4, x)

- 10** Follow the prompts to return to the *Media Server 2000 Series CLUI Main Menu*.
- 11** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 12** Enter exit to close the telnet session.
- 13** You have completed this procedure.

---

## Displaying Media Server 2020 node current configuration

---

This procedure enables you to display the current configuration of the Media Server 2020 node.

### ***At the Windows desktop interface***

- 1 Open a telnet connection to the CS 2000 Management Tool.
- 2 Log in with the appropriate user name.  
**Note:** The user name must be a member of the “succssn” and “emsadm” groups.
- 3 Invoke the MS 2000 Series CLUI by entering the following on the command line:  
**`/opt/nortel/NTsesm/bin/ms2000.sh`**
- 4 When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- ```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 5 Enter 2 to access Node Maintenance and Configuration menu.
- 6 When prompted, enter the IP address of the Media Server node.

The *Main Menu* displays.

```
*** Main Menu for MS2020 at 172.17.40.221 ***
```

- ```
1) Maintenance Menu
2) Configuration Menu
x) EXIT
```

```
Enter selection (1 - 2, x)
```

- 7 Enter 2 to access the Configuration Menu.

The *AAL2 Main Configuration Menu* displays.

```
*** AAL2 Main Configuration Menu for MS2020 at
 172.17.40.221 ***
```

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security
- 5) Configure ATM loopback table
- 6) Display SVC Connection table
- 7) Configure ATM port table
- 8) Configure Remote Gateway table
- 9) Configure AAL2 PVC table
- 10) Configure SVC Profile table
- x) EXIT

Enter selection (1 - 10, x)

**8** Press 1 to display the current configuration for this node.

The current configuration datafill displays:

**Example**

```
Current configuration for MS2020 at 172.17.40.221
IP Address : 172.17.40.221
Subnet Address : 255.255.248.0
Default Gateway : 172.17.40.1
MG Control Protocol : controlPtotocol-MEGACO(2)
Software Version : 4.40.0.1
Lock State : unlocked(2)
Megaco Call Agent IP Address : 172.17.40.68
Is Megaco Call Agent Used : yes(1)
Number of Conference Ports : 30
Number of TestTrunk Ports : 30
Number of Lawful Intercept Ports : 30
Number of Announcement Ports : 30
APS IP Address : 47.142.89.70
Primary Language : isoLangEnglish(2)
Secondary Language : isoLangEnglish(2)
Syslog Server IP : 47.142.89.27
```



```
ATM Default Application Type : aal2-i-366-2(2)
Transmission mode : sonet(1)
Press <enter> to continue
```

**9** Press enter. The *AAL2 Main Configuration Menu* displays.

```
*** AAL2 Main Configuration Menu for MS2020 at
 172.17.40.221 ***
```

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security
- 5) Configure ATM loopback table
- 6) Display SVC Connection table
- 7) Configure ATM port table
- 8) Configure Remote Gateway table
- 9) Configure AAL2 PVC table
- 10) Configure SVC Profile table
- x) EXIT

Enter selection (1 - 10, x)

- 10** Follow the prompts to return to the *Media Server 2000 Series CLUI Main Menu*.
- 11** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 12** Enter exit to close the telnet session.
- 13** You have completed this procedure.

---

## Backing up the APS-specific Oracle database and application files

---

To ensure successful recovery from a system problem that causes database file corruption, it is recommended that you periodically back up the database files that support operation of the APS. These files include:

- Oracle database
- Root database files
- non-Root database files

The Succession Server Platform Foundation Software (SSPFS) base software provides two utilities that enable you to back up these files: “bkfullora” and “bkfullsys”.

The “bkfullora” utility backs up the Oracle database. This utility runs automatically each day at 1:00 am and backs up the database to a 4mm DAT tape. The utility can also be run manually to back up the database to a disk file.

The “bkfullsys” utility backs up the UNIX file system, including all of the “Root” and “non-Root” database files. This utility can only be run manually.

Instructions for performing the “bkfullora” and “bkfullsys” backup procedures are found in *ATM/IP Configuration Management*, NN10261-600.

In addition to these two utilities, two additional APS-specific utilities enable you to back up selected files, when only files required for APS operation must be restored. The “ips\_export\_db.sh” utility backs up the APS Oracle database. The “backup\_appl\_data.sh” utility backs up only the non-Root application files, “/audio\_files,” “PROV\_data,” “/user\_audio\_files,” and Root application file, “/etc/inet/hosts.” Both of these utilities can only be run manually.

This procedure enables you to perform a complete manual backup of the APS-specific Oracle database files and application files. It is recommended that this procedure be performed once per week.

## Backing up the APS-specific Oracle database and application files

### *In a telnet connection to the APS server*

- 1 Open an xterm window, and log in using the “maint” login and password.
- 2 Become the “root” user by entering:  
**su - root**
- 3 Enter the following command to start the backup:  
**ips\_export\_db.sh -diskonly**  
*The system displays a log of the backup activity.*
- 4 To ensure that the backup was successful, list the content of the tape on the terminal screen by entering the following commands:  
**cd /audio\_files/aps\_db\_backup**  
**ls -l**  
*A listing of the backed-up files displays. Look in this list for “dmp” files.*  
**more README**  
*A timestamp displays, which should show the time and date of this backup.*  
**Note:** At this point, you have completed the disk-only portion of the backup. Continue with the next step to complete the backup of the application files. The application files are backed up on tape.
- 5 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) DAT tape into the 4mm DAT drive on the APS server, and then rewind the tape by entering the following command:  
**mt -f /dev/rmt/0c rewind**
- 6 Enter the following command to start a backup of the application file systems on a single tape:  
**/usr/ntdb/uas/scripts/backup\_appl\_data.sh**  
*The system displays a log of the backup activity.*
- 7 Rewind the backup tape by performing the following command:  
**mt -f /dev/rmt/0c rewind**
- 8 To ensure that the backup was successful, list the content of the tape on the terminal screen by entering the following command:  
**tar tvf /dev/rmt/0c | more**

- 9** Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen), to prevent the data on the tape from being accidentally over-written. Store the tape for use later. Insert another write-enabled DAT tape into the drive to be used for the automatic Oracle system back up that runs daily at 1:00 a.m.
- 10** You have completed this procedure.

---

## Administration: OAMP Workstation Backup

---

You can perform two types of backup on your OAMP workstation, manual and automatic. Manual backups are performed from the desktop by manually initializing the backup process. Automatic backups are performed according to the settings defined in the tape drive application.

**Note:** Nortel Networks recommends that you use the automatic backups to ensure that the data that is stored on the tapes is up-to-date.

The OAMP workstation is equipped with a tape drive, software to support tape backup, and five blank data tapes. These tapes will allow approximately one month's worth of backups to be kept on-site.

**Note:** Nortel Networks recommends that you label the tapes to indicate the OAMP workstation associated with the backups to ensure that any recovery operations are performed from the correct tape.

### Backup schedule

You should create a schedule for your automatic backups to ensure up-to-date storage of the system configuration of your OAMP workstation.

**Note:** Nortel Networks recommends that you perform a full system backup once a week and modified (differential) backups once a day.

### Manual backup

Nortel Networks recommends that you perform a manual backup of your OAMP workstation after initial installation.

To perform a manual backup of the system configuration for your OAMP workstation, refer to the documentation provided with your Colorado or Veritas software.

### Automatic backup configuration

There are two types of automatic backup, full system backup and modified (differential) system backup.

The full system backup saves all of the files contained in the hard disk on your OAMP workstation.

The modified (differential) system backup saves only the files on the hard disk that have been modified since the last full system backup.

**Note:** When you are using automatic backup, you must leave your OAMP workstation turned on with Windows running and ensure that there is a tape in the tape drive.

During the initial installation of your system, the tape drive application was configured to perform an automatic full system backup once a week, every Saturday at 1:00am. However, you can modify the settings in the tape drive application to suit your needs.

**Note 1:** If you do not change the default setting for automatic full system backup, you will need to swap out the tape every Friday.

**Note 2:** In order for automatic backups to work, the tape drive scheduler icon must be active in the notification box in the taskbar with the automated daily backups option enabled, your OAMP workstation must remain on with Windows active, and a tape must be in the tape drive.

### **Verify the current modified system backup settings**

There is a tape drive configuration file associated with the modified system backup. To verify that the current settings in the configuration file matches the system requirements, refer to the tape drive documentation provided with the OAMP workstation.

### **View the current automatic backup schedule**

To view the current settings for automatic backup in the tape drive application, refer to the tape drive documentation provided with the OAMP workstation.

---

## Backing up a Multiservice Switch or Media Gateway device

---

This section describes using Service Data Backup and Restore to perform a basic back up of service data.

Backup copies only the configuration data of the Multiservice Switch 7400/15000 or Media Gateway 7400/15000. The service data views that make up the configuration data are found on the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 disk in a set of files in individual directories under the directory /provisioning. Backup also copies the special files that are found under the directory /provisioning/netsentry.

Service Data Backup and Restore provide three types of backup.

- A *full* backup copies all service data on the selected device or devices.
- An *incremental* backup copies only service data changed or created since the last backup. Like the full backup, you can perform an incremental backup on either one or multiple devices.
- A *selective* backup copies specific service data that you select. You can perform a selective backup on either one or multiple devices.

The following information applies to using the Service Data Backup and Restore tool to backup Multiservice Switch 7400/15000 or Media Gateway 7400/15000 nodes:

- [Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the backup list](#)
- [Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the backup list](#)
- [Viewing the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 backup repository](#)
- [Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 in the backup list](#)
- [Changing the Default User Authentication](#)
- [Performing a full backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Performing an incremental backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Performing a selective backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)

## Using the command line interface to perform backups

You can use the command line to perform full, incremental, or selective backups. You can perform multiple backups on multiple devices in a single command. You have the option of obtaining the backup information from a file.

Before you perform a backup, you need to start up the Backup Controller and Providers.

To display online help for this command, use the -h option on the command line.

### Procedure steps

Enter the following command as one continuous command:

```
/opt/MagellanNMS/bin/nsbck
[-full <devtype> <devname> <devaddr> <id> <pw>]
[-incr <devtype> <devname> <devaddr> <id> <pw>]
[-view <viewname> <devtype> <devname> <devaddr>
<id> <pw>] [-cdir <backup_dir_path> [-f
<backup_info_file>] [-chost <controller_address>]
[-nolog] | [-log [<logfile>]]
[-nc <#_concurrent_connections>]
```

where:

-full

indicates a full backup.

-incr

indicates an incremental backup.

-view

indicates a selective backup.

devtype

is the name of the device type, such as PASSPORT.

devname

is the name of the device.



devaddr

is the IP address of the device and has the format n.n.n.n.

id

is the userID for a Passport and the READ community string for a Passport 4400/4460.

pw

is the user password for a Passport and the WRITE community string for a Passport 4400/4460.

viewname

is the name of the view file for a selective backup.

-cdir

is the backup directory used for this backup operation.

-f

indicates that the backup information is obtained from a file.

backup\_info\_file

is the name of the file containing backup information. Each line in the file has the same format as the -full, incr, or -view options.

-chost

indicates the remote Controller to be used in place of the Controller running on the local host.

controller\_address

is the address of the Controller and has the format host[:port]

-nolog

indicates that output messages are to be discarded.

-log

indicates that output messages go to stdout/stderr or to a log file. The default is stdout/stderr.

logfile

is the name of the file to which output messages go. If not specified, the messages go to the file mbrbackup.log in the current directory (where the tool runs).

-nc

indicates the number of concurrent backups to be performed. By default, SNMP Devices Backup tries to back up 5 different devices concurrently. This parameter is useful when you are backing up a large number of devices.

#\_concurrent\_connections

is the number of concurrent backups.

## Backup file naming convention

The service data backup files have the following naming convention:

```
./<devtype>/<devname>/<timestamp>.<dataset>/ \
<datafiles...>
```

**Note:** The period (.) represents the SNMP Devices Backup and Restore root directory.

where:

devtype

is the device type (PP4400, or PP4460).

devname

is the device name.

timestamp

has the format `yyyymmddhhmmss`

dataset

is the dataset name.

<datafiles...>

are the names of one or more files that are backed up.

## **Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the backup list**

Use this procedure to add devices to the list of devices that you wish to backup.

### ***Procedure steps***

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 Select Add to launch the Add Devices Dialog.
- 4 From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.
- 5 From the drop down list, in the right pane, select a backup mode (Incremental or Full).
- 6 If a specific userid and password is required for the device, enter the values in the user ID and Password fields and uncheck the Use default checkbox.
- 7 If you wish to use the default userid and password, click the Use default checkbox.
- 8 Click OK.

The devices display in the Device List.

## **Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the backup list**

Use this procedure to remove devices from the list of devices that you wish to backup.

### ***Procedure steps***

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 In the Device List, select the devices you wish to remove.
- 4 Click Remove.

- 5 In the confirmation dialog, select Yes to confirm or No to cancel the removal.

## **Viewing the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 backup repository**

If the backup server is running locally, use the following procedure to view all the backup files in the backup repository.

### ***Procedure steps***

- 1 Telnet into the remote workstation with the appropriate userid and password.
- 2 Navigate to the repository directory.
- 3 Use Unix directory commands to view the contents of the backup repository.

## **Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 in the backup list**

A specific userid and password can be defined when you add the node to the node list or you can set it later using the following procedure.

### ***Procedure steps***

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 Select a node in the Device List section.
- 4 In the Device Details section, in the Authentication tab, enter a userid and password.
- 5 Clear the Use default checkbox.

## **Changing the Default User Authentication**

Use the following procedure to define a default userid and password which is used for all node access unless overridden by a specific userid and password for the node.

### ***Procedure steps***

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.

- 2 Select Options ->Set default authentication.
- 3 Enter the userid and password in the appropriate fields.
- 4 Click OK.  
The new userid and password are used on the next node access.

## Performing a full backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 Select Add to launch the Add Devices dialog.
- 4 From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.
- 5 Select a device in the Device list:
- 6 Click in the Mode title and select Full from the drop-down list.
- 7 Click Backup.

The progress of the backup is displayed in the Messages area. If the backup is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure.

**Note:** To cancel a backup in progress click Cancel.

## Performing an incremental backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to backup only backup files that are not already in the repository.

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 Select Add to launch the Add Devices dialog.

- 4 From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.
- 5 Select a node in the nodes list.
- 6 In the Mode title, select Incremental from the drop-down list.
- 7 If you wish to specify a backup of views later than a specific date, enter the date in the date field. (for example July 3, 2003)
- 8 Click Backup.

The progress of the backup is displayed in the Status area. If the backup is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure.

**Note:** To cancel a backup in progress click Cancel.

## Performing a selective backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to backup only a single specified file to the repository.

### **Procedure steps**

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 Select Add to launch the Add Devices dialog.
- 4 From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.
- 5 Select a device in the Devices list.
- 6 In the Mode title, select Selective from the drop-down list.  
The Configuration column in the table is enabled.
- 7 Click in the Configuration cell to display a pull-down list that displays all the available views on the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.  
**Note:** This step may take a few seconds to complete because the application must access the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 and list all the views names.
- 8 Click Backup.

The progress of the backup is displayed in the Status area. If the backup is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure.

**Note:** To cancel a backup in progress click Cancel.

---

## Performing a backup of oracle data on an SSPFS-based server

---

### Application

Use this procedure to perform a backup of oracle data on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240) running the (I)SN06.2 or greater release of the SSPFS.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)

**Note:** If the server is hosting the Integrated EMS, it is highly recommended to purge the Integrated EMS event and performance data prior to executing the data backup. This reduces the size of the oracle space used by the Integrated EMS, and therefore, reduces the backup time, and can avoid a backup failure. The purge capability is only available in (I)SN07 onward.

- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core and Billing Manager (CBM)

**Note:** If the server is hosting the Core and Billing Manager (CBM), an oracle data backup is not required.

#### ATTENTION

It is recommended that provisioning activities be put on hold during the time of the data backup.



## Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater
- for a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- for a Sun Netra 240, you need one or more blank DVD-R or DVD-RW to store the data

**Note 1:** The backup utility limits the storage to 2 GB on aDVD-R and DVD-RW.

**Note 2:** If you are using a newDVD-RW, or want to use a used DVD-RW andneed to erase the contents, refer to procedure “Preparing a DVD-RW for use” in the *ATM/IP Security and Administration*, NN10402-600.

### ATTENTION

The database must be in sync with the Communication Server 2000 and the MG 9000 Manager (if present). Therefore, ensure you have an image of both before you proceed. Performing a restore from the Oracle database alone can cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

## Action

### ATTENTION

In a two-sever configuration, execute this procedure on the active server.

### **At the server**

- 1 Insert the blank tape or DVD into the drive. In a two-server configuration, insert the blank DVD into the drive of the active server.

**At your workstation**

- 2** Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**

is the IP address or hostname of the SSPFS-based server on which you want to perform the backup

Enter the physical IP address of the active server in a two-server configuration.

- 3** When prompted, enter your user ID and password.

- 4** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 5** When prompted, enter the root password.

- 6** If the server is hosting the Integrated EMS, and you want to purge the event and performance data, do step [7](#), otherwise proceed to step [8](#).

- 7** Purge the Integrated EMS event and performance data as follows:

**Note:** Purging the Integrated EMS event and performance data prior to executing the data backup, reduces the size of the oracle space used by the Integrated EMS, and therefore, reduces the backup time, and can avoid backup failure. The purge capability is only available in (I)SN07 onward.

**a**

**ATTENTION**

This step stops the Integrated EMS server, therefore, ensure it is acceptable at this time to stop the Integrated EMS server.

Stop the Integrated EMS server by typing

```
servstop IEMS
```

and pressing the Enter key.

- b** Run the script to purge the data by typing  
`# /opt/nortel/iems/current/bin/purgeTempData.sh`  
and pressing the Enter key.
- c** Start the Integrated EMS server by typing  
`# servstart IEMS`  
and pressing the Enter key.

**8** Use the following table to determine your next step.

| If you are using | Do                      |
|------------------|-------------------------|
| a tape           | step <a href="#">9</a>  |
| a DVD            | step <a href="#">10</a> |

- 9** Rewind the tape by typing  
`# mt -f /dev/rmt/0 rewind`  
and pressing the Enter key.

- 10** Backup the data by typing  
`$ /opt/nortel/sspfs/bks/bkdata`  
and pressing the Enter key.

*Example response:*

Backup Completes Successfully

| If you are using | Do                      |
|------------------|-------------------------|
| a tape           | step <a href="#">11</a> |
| a DVD            | step <a href="#">12</a> |

**11** Verify the backup to tape was successful as follows:**a** List the content of the tape by typing

```
tar tvf /dev/rmt/0
```

and pressing the Enter key.

*Example response:*

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:16 2005
opt/oracle.dmp.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:16 2005
opt/critdata.cpio
```

**b** Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

You have completed this procedure.

**Note:** To restore the data from this tape, refer to procedure “Restoring the oracle data on an SSPFS-based server” in the *ATM/IP Security and Administration*, NN10402-600.

**12** Verify the backup to DVD was successful as follows:**a** Reinsert the backup DVD into the drive.**b** List the content of the DVD by typing

```
tar tvf /cdrom/*bkdata*/*.tar
```

and pressing the Enter key.

*Example response:*

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:17 2005
opt/oracle.dmp.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:17 2005
opt/critdata.cpio
```

**Note:** When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

**13** Eject the DVD from the drive as follows:

- a** Ensure you are at the root directory level by typing

```
cd /
```

and pressing the Enter key.

- b** Eject the DVD by typing

```
eject cdrom
```

and pressing the Enter key.

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

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

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

Then press the eject button located on the front of the DVD drive.

- c** Remove the DVD from the drive, label it, and store it in a safe place.

You have completed this procedure.

**Note:** To restore the data from this DVD, refer to procedure “Restoring the oracle data on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.

---

## Performing a backup of file systems on an SSPFS-based server

---

### Application

Use this procedure to perform a backup of the file systems on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240) running the (I)SN06.2 or greater release of the SSPFS.

The server can be hosting one or more of the following components:

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

### Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater
- you must perform a data backup prior to performing this procedure (refer to procedure [Performing a backup of oracle data on an SSPFS-based server on page 168](#), if required)

**Note:** The data backup is not required prior to this procedure for the Core and Billing Manager (CBM) product family.

- for a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- for Sun Netra 240, you need one or more blank DVD-R or DVD-RW to store the data

**Note 1:** The backup utility limits the storage to 2 GB on a DVD-R and DVD-RW.

**Note 2:** If you are using a new DVD-RW, or want to use a used DVD-RW and need to erase the contents, refer to procedure “Preparing a DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

## Action

### ATTENTION

In a two-server configuration, execute this procedure on the active server.

#### *At the server*

- 1 Insert the blank tape or DVD into the drive. In a two-server configuration, insert the blank DVD into the Active server.

#### *At your workstation*

- 2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

#### **server**

is the IP address or host name of the SSPFS-based server on which you are performing the backup

Enter the physical IP address of the Active server in a two-server configuration.

- 3 When prompted, enter your user ID and password.

- 4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 5 When prompted, enter the root password.

| If you are using | Do                     |
|------------------|------------------------|
| a tape           | step <a href="#">6</a> |
| a DVD            | step <a href="#">7</a> |

- 6 Rewind the tape by typing

```
mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

- 7 Backup the file systems by typing
- ```
# /opt/nortel/sspfs/bks/bkfullsys
```
- and pressing the Enter key.

Example response:

Backup Completed Successfully

Note: If you are using DVD, the system will prompt you to insert another blank DVD if more than one is needed.

If you are using	Do
a tape	step 8
a DVD	step 9

- 8 Verify the backup to tape was successful as follows:

- a List the content of the tape by typing
- ```
gtar -tvMf /dev/rmt/0
```
- and pressing the Enter key.
- b Eject and remove the tape from the drive, label it, write-protect it, and store it in a safe place.
- You have completed this procedure.

- 9 Verify the backup to DVD was successful as follows:

- a Reinsert the backup DVD into the drive.
- b List the content of the DVD by typing
- ```
# gtar -tvMf /cdrom/*bkfullsys*/*.tar
```
- and pressing the Enter key.

Note: When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

10 Eject the DVD from the drive as follows:

- a** Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- b** Eject the DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

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

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

Then, press the eject button located on the front of the DVD drive.

- c** Remove the DVD from the drive, label it, and store it in a safe place.

You have completed this procedure.

Backing up the central security server

Use this procedure to backup the central security server. When the Security Services component is installed, the generic backup and restore script (brr_security.sh) is registered with servman (bkmgr).

The NDS database and all files under the following directories are backed up using this procedure.

- /opt/nortel/config/3rd_party/netscape
- /opt/nortel/config/3rd_party/security/s1is
- /opt/nortel/config/applications/security
- /opt/nortel/data/3rd_party/netscape
- /opt/nortel/data/3rd_party/security/s1is
- /opt/nortel/data/applications/security

Prerequisites

You must have root user privileges to perform this procedure.

Action

In a telnet connection to the security server

- 1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the server where Integrated EMS resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Enter the following command:

```
/opt/bkresmgr/cbm/bkmgr
```

- 6 Enter the following command to start the backup:
backup full
- 7 The Security Services configuration settings and data are backed up to the following file:
/data/bkresmgr/<date><time>backupSS1.1<host_name>.tar
- 8 You have completed this procedure.

Backing up an SSPFS-based security client

Use the following procedure to obtain a list of the files that will be backed up from the client machine. To enable backup and restore of the security client, the files to be backed up are registered with servman during installation. The files backed up depend on the packages installed.

Prerequisites

You must have root user privileges to perform this procedure.

Action

In a telnet connection to the security server

- 1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the server where Integrated EMS resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Enter the following command:

```
cat etc/critdata.conf
```

The system returns a list of all non-oracle data files that will be backed up from the client machine.
- 6 Use the Synchronous Backup Restore Manager (SBRM) to backup the central security client data. When SBRM is run, all of the SSPFS data, including the security client data and oracle data, is backed up. For details, see the procedure for “Starting or stopping the automated synchronous backup restore manager service” in *ATM/IP Solution-level Security and Administration*, NN10402-600.
- 7 You have completed this procedure.

Create a backup of the GWC load file

Purpose of this procedure

This procedure is used to log onto the CS 2000 Core Manager or Core and Billing Manager (CBM) and manually make a copy of one or more existing GWC load images stored on the CS 2000 Core Manager or CBM.

When to use this procedure

Use this procedure prior to saving an image of a GWC load if you wish to save a backup of the original GWC load stored on the CS 2000 Core Manager or CBM.

Note: If a backup is not created, then the process of taking a GWC load image overwrites the existing image stored on the CS 2000 Core Manager or CBM.

Prerequisites

There are no prerequisites to this procedure.

Action

At the CS 2000 Core Manager or CBM console

- 1 Log in to the CS 2000 Core Manager or CBM as the root user.

```
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

- 2 Change directory to the GWC software directory by typing
cd /swd/gwc
and pressing the Enter key.
- 3 Type **ls** and press the Enter key to list the contents of the directory.
- 4 Locate the load file name that corresponds to the load you wish to back up.

Note: There are likely to be multiple load file names. Ensure that you select the correct load filename. If you are saving the load file of a specific GWC card or node, refer to procedure “View the operational status of a GWC” in *Gateway Controller Configuration Management*, NN10205-511, to locate the load filename associated with a specific GWC card.

5

**CAUTION**

Be sure to use the command **cp** in this step.

Failure to use the **cp** command can cause problems with the general upgrade process.

Make a copy of the existing GWC software load file by typing
cp <load_filename>.imag <load_filename>.imag.bak
and pressing the Enter key.

where

<load_filename>

is the GWC load filename that you want to copy

Note: You can use any name for the backup file name. You can also include the date in this filename, for example:
<load_filename>.imag.031201

6

Change the permissions for the image file by typing

chmod 755 <load_filename>.imag.bak

and pressing the Enter key.

where

<load_filename>

is the GWC load filename

7

This procedure is complete.

Note: To return to the procedure that sent you here, refer to “Overall GWC upgrade procedure” (automated or manual) in *Upgrading the Gateway Controller*, NN10196-461.

Administration: Manual Backup

If you change the external IP address of an RTC system node in your system (or perform any other data provision changes on your system), you should immediately perform a backup operation and delete any data snapshots that were made before you changed the IP address. This will ensure proper communication with your OAMP workstations. Refer to the Modifying RTC System Node Provisioning Data section of this document for more information on changing the external IP addresses.

Performing a Backup Operation

At the OAMP workstation

- 1 Click **Administration>backup**.
- 2 Enter a description of the data snapshot in the **Snapshot Description** box. You can enter up to 32 characters.
- 3 Click the corresponding checkboxes to activate the following options, as appropriate:
 - Transfer snapshot to alternate boot server
Note: Nortel Networks recommends that you enable this option, if you don't select this option a warning dialog box will appear. Click **Yes** to continue.
 - Set as active snapshot on alternate boot server
Note: Nortel Networks recommends that you enable this option if you don't select this option a warning dialog box will appear. Click **Yes** to continue.
 - Delete oldest snapshot on alternate boot server if maximum reached (16)
 - Delete oldest snapshot on rtc if maximum reached (5)
- 4 Click **Create** to create the data snapshot. This can take several minutes, depending on system activity.
- 5 Click **Close** to close the Backup Active RTC window and return to the Administration window.
- 6 If you **selected transfer snapshot to alt boot server** on alt boot server, go to step [12](#).
- 7 Click **Administration>File Manager**. The File Manager window appears.

- 8 Select the active RTC system node from the **Destination** list in the right window pane.
- 9 Select the new data snapshot from the **Snapshot** box in the Destination portion of the window. Make note of the timestamp of the data snapshot.
- 10 Copy the snapshot to your alternate boot server by clicking <--. An hourglass appears while the data snapshot is copied. The boxes in the **Source** portion (left window) of the window will be updated with the information for the copied data snapshot when the copy operation is complete.

Note: These files are large and can take several minutes to copy from an RTC system node to your alternate boot server.
- 11 When the file is transferred, click **Close**.
- 12 Update the Alternate Boot Data Snapshot using the ABS Settings ABS window:
 - a Open the Alternate Boot Server (ABS) Configuration Manager window by clicking **ABS Settings** on the Administration>alternate-boot-server window.
 - b Select an alternate snapshot by clicking the arrow button.
 - c Click **Modify** to save your changes and close the window.
- 13 Your backup is complete.

Creating system image backup tapes (S-tapes) manually

Purpose

Use this procedure to create a system backup image manually.

Prerequisites

You must be a user authorized to perform config-manage actions.

Application

Create a system image backup tape (S-tape) manually.

Note: If you want to schedule automatic system image backups, refer to SDM Security and Administration document.

The system image includes the following:

- boot (startup) files
- AIX operating system
- system configuration data
- core manager software

Prerequisites

ATTENTION

This procedure must be performed a trained AIX system administrator authorized to perform config-manage actions.

ATTENTION

All volume groups on the core manager must be fully mirrored (Mirrored) before performing this procedure. If not, an error message is displayed.

ATTENTION

If your system includes the SuperNode Billing Application (SBA), you must use tape drive DAT0 to perform this procedure.

ATTENTION

The files under the /data file system are temporary files only, and are excluded from system image backup.

Perform a system image backup after the following events:

- initial installation and commissioning of the core manager
- changes to the configuration of disks or logical volumes
- installation of a new version of core manager platform software
- installation of new hardware
- changes or upgrades to existing hardware

A system image backup takes a minimum of 10 minutes to complete, depending on the size of your file systems.

Recommended tapes

To complete this procedure, use one of the digital audio tape (DAT) drive tapes approved by Nortel.

The brands approved by Nortel are: Hewlett Packard (HP), Maxell, Verbatim, Imation.

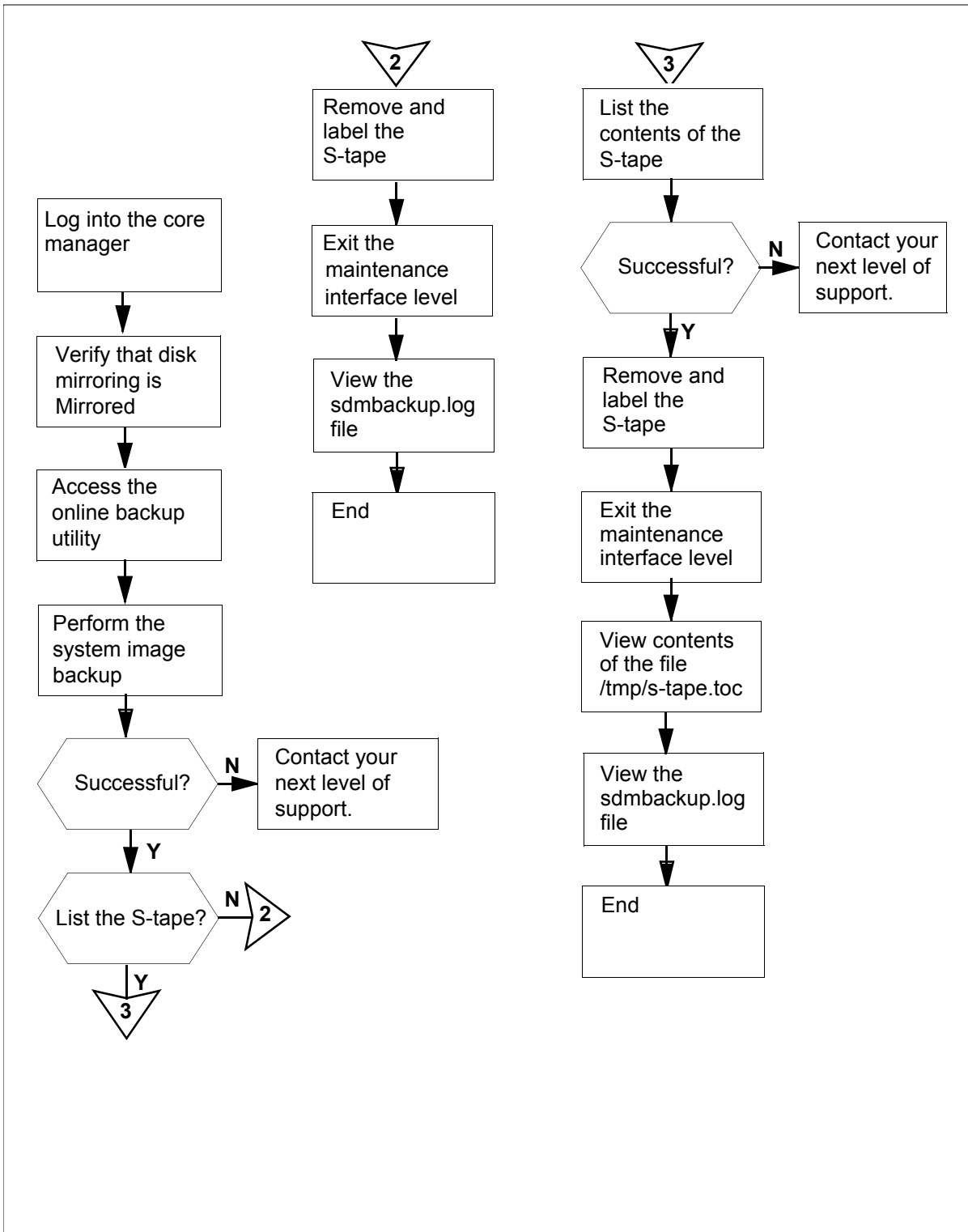
The tape lengths approved by Nortel are:

- 90-meter (90M)
- 125-meter (125M)
- 120-meter (120M)

The 125M tape is approved for UMFIOs only, assuming that your system is equipped with DDS3-capable devices to read the content of the tape.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the procedure.

Summary of creating system image backup tapes (S-tapes)

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Creating system image backup tapes (S-tapes)

At the local VT100 console

1 Log into the core manager as a user authorized to perform config-manage actions.

2 Access the maintenance interface:

sdmmtc

3



CAUTION

System mirroring must be **MIRRORED**

You cannot perform this procedure until disk mirroring of all volume groups is Mirrored. If necessary, contact the personnel responsible for your next level of support. When disk mirroring is Mirrored, continue this procedure.

Access the storage menu level:

storage

Example response:

Volume Group	Status	
Free (MB)		
rootvg	Mirrored	608

Logical Volume	Location	Size (MB)	
%full/threshold 1 /	rootvg	20	
25/ 80			
2 /usr	rootvg	192	85/ 90
3 /var	rootvg	64	11/ 80
4 /tmp	rootvg	24	6/ 90
5 /home	rootvg	300	4/ 70

```
6 /sdm          rootvg          300          44/ 90
Logical volumes showing: 1 to 6 of 6
```

If the disks	Do
are "Mirrored"	step 4
are not "Mirrored"	contact next level of support

- 4 Access the administration (Admin) menu level of the RMI:
admin

- 5 Access the System Image Backup and Restore Menu:
backup

Example response:

```
Currently there is a backup running on
bnode73.Please execute yours later.
Exiting . . .
```

Note: If another operator attempts to use the Backup and Restore utility when it is in use, an error message is displayed.

- 6 From the System Image Backup and Restore Menu, select
Create a System Image on Tape (S-tape):

2

After you select option 2, you are prompted to select the tape drive.

Example response:

Select the tape drive you wish to use:

```
Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main Chassis-Slot
2
Enter 2 for tape drive DAT1 in Main Chassis-Slot
13
( 0, 1 or 2 ) ==>
```

Note: Use tape drive DAT0 (option 1) if your system also includes SBA.

- 7 Select the tape drive to use:

<n>

where

<n>

is the option (1 or 2) for the tape drive you wish to use

Note: If your system includes SBA, and you wish to use tape drive DAT1 (option 2), the following message is displayed:

Example response:

You have selected DAT 1. This is the default DAT drive for the Billing application, and may currently be in use for the emergency storage of billing records.

If you continue to use DAT 1, make sure that the correct tape is in the drive, and that billing records will not be lost during the backup restore operation.

Do you wish to continue with DAT 1? (y | n)

If you	Do
wish to continue using DAT1	enter y press the Enter key
do not wish to use DAT1	enter n press the Enter key

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

After you select the tape drive, you are prompted to insert a tape in the drive you have selected.

Example response:

Please insert a 4mm DAT tape into the tape drive DAT0.

Caution:

This action will overwrite the content on the inserted tape. Do you want to proceed? (y | n)
==>

At the core manager**8****CAUTION****System image backup tape**

Creating a system image overwrites the contents of the inserted tape. Ensure that you are using the correct tape before starting the system image backup. If your system includes SBA and you are using DAT1, ensure that the tape drive does not contain an SBA tape.

Ensure that the appropriate core manager tape drive contains a 4-mm digital audio tape (DAT) either 90 m or 120 m long. This tape will be designated as the system image backup tape (S-tape).

Note: For the complete list of approved tapes, refer to the [Recommended tapes on page 186](#).

At the local console

9 When you are certain you are using the correct tape, enter:

y

10 Read the system message to determine if there is enough room on the temporary directory for the system image backup to proceed.

Note: If there is not enough room on the temporary directory, an error message appears.

Example response:

Rewinding the tape...

```
The /tmp directory is not big enough.  
Trying to expand /tmp by 6600KB...
```

```
Failed to expand the /tmp directory because  
there isn't enough free disk space left on the  
rootvg.
```

```
Please erase some files under /tmp directory to  
create at least 6600KB for the full system image  
backup.
```


Enter any key and return to exit ==>

If there is	Do
enough disk space	step 14
not enough disk space	step 11

- 11** Erase enough files from the temporary directory to create the required amount of disk space specified in the error message:

rm -rf /tmp/<filenames>

Note: If you have trouble erasing files from the temporary directory to free up disk space, contact the personnel responsible for your next level of support.

- 12** Execute the system image backup again.

The system image backup begins.

Example response:

Rewinding the tape...

Starting the system image backup on bnode73.

The backup takes a minimum of 10 minutes, depending on the size of your file systems.

When the backup is complete, you will be asked to remove the tape from the tape drive.

System image backup is in progress ...

Note: This backup process takes approximately 10 minutes to complete, depending on the amount of data stored on the disk.

- 13** Read the system message.

If the backup	Do
is successfully completed	step 14
fails	contact your next level of support

- 14** The system informs you if the backup is successful. When the backup is complete, the system prompts you to remove the tape and label it as an S-tape.

Example response:

```
The tape backup started on Wed Oct 16 08:21:15
EDT 1997
completed successfully on Wed Oct 16 08:37:37
EDT 1997.
The log for this session has been added to
"/var/adm/sdmbbackup.log".
```

Please remove the backup tape from the tape drive.
Label the tape as shown below and store it in a safe place.

```
System Image Tape (S-tape)
The Machine Node Id: bnode73
Date: Wed Oct 16 08:37:37 EDT 1997
```

```
Eject the S-tape from the tape drive? ( y | n )
==>
```

15 Determine if you wish to eject the S-tape. Enter

- **y** to eject the tape, or
- **n** if you do not wish to eject the tape, and wish to list its contents.

If you	Do
you wish to list the S-tape	step 28
protect and label the tape	step 16

If you eject the tape, the screen displays "Tape ejected." below the information displayed in step [14](#). You are then prompted to return to the System Image Backup and Restore Main Menu.

Response:

Tape ejected.

```
Would you like to return to the previous
menu? ( y | n)
```

16 Place the write-protected tab of the S-tape in the open position, to prevent accidental erasure.

17 When you are ready for the system to return to the System Image Backup and Restore Main Menu, enter

y

18 Determine if the backup is successful.

The system informs you if the system image backup is successful, as shown in the response in step 14. You may also wish to view the /var/adm/sdmbbackup.log file or list the files on the S-tape.

If	Do
you wish to view the /var/adm/sdmbbackup.log file	step 19
you wish to list the S-tape	step 28
the backup is successful	step 36
the backup fails	contact your next level of support

19 Exit the System Image Backup and Restore Main Menu:

0

20 Exit the RMI:

quit all

21 Access the sdmbbackup.log file:

cd /var/adm

22 Scroll through the file:

more sdmbbackup.log

This screen informs you that the system image backup was completed successfully.

Example response:

```
bosboot:  Boot image is 5881 512 byte blocks.
0+1 records in.
1+0 records out.
```

```
Backing up the system...
```

```
.....
.....
```

```
0512 038 mksysb: Backup Completed Successfully.
```

```
The S-tape backup started on Wed Oct 16 09:24:07
EDT 1997
completed successfully on Wed Oct 16 09:36:03
EDT 1997
```

- 23 Determine if you wish to list the S-tape.

If you	Do
wish to list the S-tape	step 24
do not wish to list the S-tape	step 40

- 24 Return to the login directory:

cd

- 25 Access the RMI:

sdmmtc

- 26 Access the administration (Admin) menu level of the RMI:

admin

- 27 Access the System Image Backup and Restore Menu:

backup

- 28 From the System Image Backup and Restore Menu, select List Contents of the System Image Tape (S-tape):

3

- 29 After you select option 3, you are prompted to select the tape drive.

Example response:

Select a tape drive you wish to use:

```
Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
( 0, 1 or 2 ) ==>
```

Note: Use tape drive DAT0 (option 1) if your system also includes SBA.

- 30 Select the tape drive:

<n>

where

<n>

is the number (1 or 2) for the tape drive you wish to use

Example response:

You have selected DAT 1. This is the default DAT drive for the Billing application, and may currently be in use for the emergency storage of billing records.

If you continue to use DAT 1, make sure that the correct tape is in the drive, and that billing records will not be lost during the backup restore operation.

Do you wish to continue with DAT 1? (y | n)

If you do not wish to use DAT1, the system prompts you to return to the System Image Backup and Restore Menu.

If you wish to	Enter
continue using DAT1	y
not continue	n

Note: If your system includes SBA, and you still wish to use DAT1 (option 2), the following message is displayed:

- 31** After you select the tape drive, you are prompted to insert the S-tape into the tape drive that you selected in step [30](#).

Example response:

Please insert your System Image Backup tape (S-tape) into the tape drive DAT0 and allow at least 5 minutes to complete the listing.

A log file will be saved in /tmp/s-tape.toc

Are you ready to proceed? (y | n)

At the core manager

- 32** Insert the S-tape into the tape drive.

Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

At the local VT100 terminal

- 33** When you are ready to continue this procedure, enter:

y

- 34** The contents of the S-tape are displayed. When the listing is complete, the system prompts you to return to the System Image Backup and Restore Menu.

Example response:

Would you like to return to the previous menu?
(y | n)

35 Return to the System Image Backup and Restore Menu:

y

At the core manager

36 If you have not already done so, remove the S-tape from the tape drive by pressing the eject button on the tape drive.

37 Label the tape according to your office practices, and store it in a safe location.

38 If you ejected an SBA tape, reinsert the tape.

At the local VT100 terminal

39 Exit the System Image Backup and Restore Menu,:

0

Note: If you wish to exit the RMI, enter QUIT ALL.

40 You have completed this procedure.

Configuring SBA backup volumes on the core

Purpose

Use this procedure to configure backup volumes on IOP, 3PC, DDU, or SLM disks on the core for a billing stream. The maximum number of volumes that can be configured for a billing stream is either 69 or the maximum supported by the underlying hardware, whichever is less per stream.

The following table lists the disk drive backup volumes that you can configure for the BRISC and XA-core platforms.

Platform	Backup volume(s)
BRISC	DDU or SLM
XA-core (for releases prior to SDM16 or CS2E03)	DDU or IOP
XA-core (for SDM16 or CS2E0 and higher)	IOP

Prerequisites

Prior to starting this procedure, you must be aware of the following:

- you must configure additional backup storage to prevent a temporary problem that forces the SBA into long-term backup mode
- the billing stream is aware that the replaced volumes exist, and recovers files from both the swapped-out and swapped-in sets of volumes as part of the recovery process
- the billing stream loses track of swapped-out volumes when a switch of activity (SwAct) or a restart is performed on the DMS or Communication Server 2000 prior to the completion of the recovery of the files
- there is a risk of losing some billing records when you reconfigure or swap-out backup volumes of a stream that is in backup mode during the transition process
- you must allow recovery to complete prior to a switch outage when you choose to swap out an active backup volume during an emergency situation. If not, the billing stream does not recognize the swapped-out volumes.

If you are using or migrating to a XAC16 system, your backup volumes must be on IOP volumes. If your current backup volumes

are on SLM or DDU volumes and you are running a previous release, you must migrate to IOP volumes before upgrading to this release.

ATTENTION**Ensure the size for backup volumes is sufficient.**

Refer to “Disk space requirements” (Calculation of core disk space requirements) in procedure “Preparing for SBA installation and configuration” in *North American ATM/IP Solution-level Accounting*, NN10412-800 or *International ATM/IP Solution-level Accounting*, NN10400-800 . The absolute minimum size for backup volumes is 30MB.

ATTENTION

Backup volumes must be configured evenly across the available disks of the same disk type in your system.

Procedures

Use the following procedures to configure SBA backup volumes on the core.

Note: Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Calculate disk space to contain backup volumes

At your system

- 1 Write down the dms_disk_space value from the procedure “Preparing for SBA installation and configuration” in *North American ATM/IP Solution-level Accounting*, NN10412-800 or *International ATM/IP Solution-level Accounting*, NN10400-800 (answer 28), which shows the amount of disk space required for the backup volumes.
- 2 Determine the amount of disk space of each disk type in your system to be used for storing the backup volumes. Divide the value you recorded in [step 1](#) by the maximum volume size

supported for the appropriate disk types for your system, obtained from the table below. Record these values.

Disk type	Maximum disks per core	Maximum volumes per device	Maximum volumes configurable for SBA	Maximum volume size
IOP	2	32	64	2GB
3PC	2	32	64	2GB
DDU	10	32	69	64MB
SLM	2	32	64	

- 3** Ensure that the backup volumes can fit on the disks in your system. Compare the values that you recorded in [step 2](#) with the maximum number of volumes supported for the disk types in your system, obtained from the table in [step 2](#). Determine the next step to perform:

If the number of volumes obtained in step 2	Do
is less than or equal to the maximum number allowed	step 4
is greater than the maximum number allowed	contact the next level of support

- 4** Determine the next steps to perform.

To configure disk type	Use this procedure
DDU	Configuring DDU disk drive backup volumes on page 202
IOP	Configuring IOP disk drive backup volumes on page 206
SLM	Configuring SLM disk drive backup volumes on page 209
3PC	Configuring 3PC disk drive backup volumes on page 213

Configuring DDU disk drive backup volumes

At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

<stream_name>

is the name of the billing stream

- 2 Obtain information about the existing backup volumes for the billing stream:

```
conf view <stream_name>
```

where

<stream_name>

is the name of the billing stream

Note: SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

- 3 Quit out of the MAPCI level:

```
quit all
```

- 4 Display and record the size of a volume and its number of free blocks:

```
dskut;sv <volume name>
```

where

<volume name>

is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5 Repeat step [step 5](#) for each volume name that you recorded in [step 2](#).

- 6 Create an eight-character, alphanumeric name for each of the new backup volumes that you determined in the procedure, [Calculate disk space to contain backup volumes on page 200](#) and record each of these names for future reference.

Note 1: DDU volume names can be up to eight alphanumeric characters in length, with the first four characters reserved for the disk prefix.

Note 2: Logical volumes must be configured evenly across the disks.

- 7 Access the IOD level:
`mapci;mtc;iod`
 - 8 Locate the DDUs:
`listdev ddu`
 - 9 Record the DDU numbers and their respective IOC, CARD, and PORT locations for future reference.
 - 10 Begin to busy a DDU:
`ioc <ioc>`
where
`<ioc>`
is the IOC controlling the respective DDU
 - 11 Display the DDU card:
`card <ddu_card>`
where
`<ddu_card>`
is the DDU card number
 - 12 Complete the busy process:
`bsy`
 - 13 Confirm the DDU card number that you selected in [step 11](#) indicates a status of ManB.
 - 14 Display the free space for this DDU:
`dskalloc <ddu #>`
where
`<ddu #>`
is the DDU card number
- Note:** Record the free space amount from the `dskalloc` command that is displayed, for future reference.
- 15 Determine DDU disk space availability.

If you have	Do
located a DDU with sufficient disk space for the new backup volumes	step 19

If you have	Do
not located a DDU with sufficient disk space for the new backup volumes	step 16

- 16 Return the DDU to service:
`rts`
- 17 Return to the IOC level:
`quit`
- 18 Repeat [step 10](#) through [17](#) until you locate a DDU with sufficient space for the new backup volumes.
- 19 Create a new logical volume:
`add <volume> <blocksize>`
where:

<volume>
is the backup volume name

<blocksize>
is the size of the volume. Calculate this by multiplying the maximum volume size allowed for the DDU disk, which is shown in the table in [step 2](#) of the procedure [Calculate disk space to contain backup volumes on page 200](#), by 1024.

Example
add AMA8 51200

This example prompts the system to create the logical volume D000AMA8, consisting of 51200 1024-byte blocks (50 Mbyte) of available disk space.

Note: If you receive an error message while updating the last DDU volume with 64 Mbyte, this volume must be configured with a size less than 32767 blocks.
- 20 Verify the names of the volume identifiers:
`display`
- 21 Add an allocation volume to the root directory:
`diradd <backup_volume>`
where:

<backup_volume>
is the backup volume name

- 22 Update the volume identifiers:
`update`
- 23 Repeat [step 19](#) through [22](#) until each new logical volume has been created.
- 24 Exit the disk administration level:
`quit`
- 25 Return the DDU to service:
`mapci;mtc;iod;ddu <#>;rts`
where:
`<#>`
is the DDU disk drive number (0 or 1) that you busied in [step 12](#)
- 26 Return to the MAPCI level:
`quit`
- 27 Configure the billing stream of the logical volumes you created in [step 19](#) through [23](#) once you receive confirmation that the files are successfully created. Perform procedure “Configuring SBA backup volumes on a billing stream” in *North American ATM/IP Solution-level Accounting*, NN10412-800 or *International ATM/IP Solution-level Accounting*, NN10400-800.
- 28 Exit back to the command prompt:
`quit all`
Note: You must alert all operating company personnel who work on the core, and provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must understand that any restarts or activity switch (SwAct) that occurs before the billing stream returns to normal mode can cause a loss of billing records.
It is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.
- 29 You have completed this procedure.

Configuring IOP disk drive backup volumes

At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

<stream_name>

is the name of the billing stream

- 2 Obtain information about the existing backup volumes for the billing stream:

```
conf view <stream_name>
```

where

<stream_name>

is the name of the billing stream

Note: SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

- 3 Quit out of the MAPCI level:

```
quit all
```

- 4 Display and record the size of a volume and its number of free blocks:

```
diskut;lv <volume name>
```

where

<volume name>

is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5 Repeat [step 4](#) for each volume name that you recorded in [step 2](#).

- 6 Create an alphanumeric name, consisting of a maximum of twelve characters, for each of the new backup volumes that you determined in the procedure [Calculate disk space to contain backup volumes on page 200](#). Record each of these names for future reference.

Note 1: IOP volume names on the IOP disks can be up to twelve alphanumeric characters in length, with the first four characters reserved for the disk prefix.

Note 2: Logical volumes must be configured evenly across the disks.

- 7 Access the disk administration level:

diskadm <disk prefix>

where

<disk prefix>

is one of the prefixes assigned to the two disks; for example, F02L or F17D.

- 8 Determine the free disk space:

dd

- 9 Note the following example, which is a response to the command performed in [step 8](#), choosing the F02L disk name.

Disk drive information for F02L

```
Date last formatted       : 2000/01/01 01:00:50.145 THU.
Date last modified       : 2001/09/26 11:22:38.587 WED.
Total space for volumes  : 4095 Mbytes
Total free space         : 1014 Mbytes
Size of largest free segment : 1014 Mbytes
Total number of volumes  : 14
```

1 Block = 512 bytes

- 10 Determine the size of the largest free segment.

If the size of the largest free segment is	Do
greater than or equal to the maximum allowable volume size for the IOP disk type	step 11
less than the maximum allowable volume size for the IOP disk type	contact your next level of support before proceeding with this procedure

- 11 Create a new logical volume:

cv <volume> <size> ftfs

where

<volume>

is the backup volume name

<size>

is the size of the volume. Compare the size recorded in [step 1](#) of the procedure [Calculate disk space to contain backup volumes on page 200](#), with the allowable size for the IOP disk type (obtained from the table under [step 2](#) of the same procedure. The lesser of the two values must be entered as this size.

Example

cv AMA8 50 ffs

This entry prompts the system to create the logical volume F17LAMA8, consisting of 50 Mbyte (102400 512-byte blocks) of available disk space.

- 12** Exit the disk administration level at the prompt:

quit

- 13** Repeat [step 7](#) through [12](#) until all new logical volumes have been created.

- 14** Exit to the command prompt:

quit all

- 15** Configure the billing stream of the logical volumes you created in [step 11](#) through [14](#) once you receive confirmation that the files are successfully created. Perform the procedure “Configuring SBA backup volumes on a billing stream” in *North American ATM/IP Solution-level Accounting*, NN10412-800 or *International ATM/IP Solution-level Accounting*, NN10400-800.

- 16** Exit back to the command prompt:

quit all

Note: You must alert all operating company personnel who are associated with the DMS switch. Provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware of that any RESTARTs or SwActs that occur before the billing stream returns to normal mode can cause a loss of billing records.

Also, it is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

- 17** You have completed this procedure.

Configuring SLM disk drive backup volumes

At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

<stream_name>

is the name of the billing stream

- 2 Obtain the names of the existing backup volumes for the billing stream:

```
conf view <stream_name>
```

where

<stream_name>

is the name of the billing stream

Note: SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

- 3 Quit out of the MAPCI level:

```
quit all
```

- 4 Display and record the size of a volume and its number of free blocks:

```
diskut;lv <volume name>
```

where

<volume name>

is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5 Repeat [step 4](#) for each volume name that you recorded in [step 2](#).

- 6 Create an eight-character, alphanumeric name for each of the new backup volumes that you determined in the procedure [Calculate disk space to contain backup volumes on page 200](#). Record each of these names for future reference.

Note 1: SLM volume names on the SLM disks can be up to eight alphanumeric characters in length for the core manager, with the first four characters reserved for the disk prefix.

Note 2: Logical volumes must be configured evenly across the disks.

- 7 Busy SLM 0:
`mapci;mtc;iod;slm 0;bsy`
- 8 Access the disk administration level:
`diskadm <disk prefix>`
where
<disk prefix>
 is one of the prefixes assigned to the two disks; for example, S00D or S01D
- 9 Determine the free disk space:
`dd`
- 10 Note the following example, which is a response to the command you performed in [step 9](#), choosing the S00D disk name.

```

Disk drive information for S00D
Drive name:  S00D
Vendor Information           :  SEAGATE  ST31051N  9470
Date last formatted         :  2000/01/01  05:38:44.718
THU.
Date last modified          :  1998/04/23  17:46:59.754
THU.
Total space for volumes     :  1000 Mbytes
Total Free space            :  174 Mbytes
Size of largest free segment :  174 Mbytes

```

1 Block = 512 bytes

If the size of the largest free segment is	Do
greater than or equal to the maximum allowable volume size for the SLM disk type	step 11
less than the maximum allowable volume size for the SLM disk type	contact your next level of support

- 11 Create a new logical volume:
`cv <volume> <volume_size> std`
Where

<volume>

is the backup volume name

<volume_size>

is the size of the volume. Compare the size recorded in [step 1](#) of the procedure [Calculate disk space to contain backup volumes on page 200](#) with the allowable size for the IOP disk type (obtained from the table under [step 2](#) of the same procedure. The lesser of the two values must be entered as this size.

Example

cv AMA8 50 std

This entry prompts the system to create the logical volume S00DAMA8, consisting of 50 Mbyte (102400 512-byte blocks) of available disk space.

- 12 Exit the disk administration level at the prompt:

quit

- 13 RTS the SLM 0 disk drives that you busied in [step 7](#) to an InSv state:

mapci;mtc;iod;slm 0;rts

- 14 Exit to the command prompt:

quit all

- 15 Repeat [step 7](#) to [14](#) until all volumes have been created.

- 16 Configure the billing stream of the logical volumes you created in [step 11](#) through [14](#) once you receive confirmation that the files are successfully created, by performing the procedure "Configuring SBA backup volumes on a billing stream" in *North American ATM/IP Solution-level Accounting*, NN10412-800 or *International ATM/IP Solution-level Accounting*, NN10400-800

- 17 Exit back to the command prompt:

quit all

Note: You must alert all operating company personnel who are associated with the DMS switch. Provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware of that any RESTARTs or SwActs that occur before the billing stream returns to normal mode can cause a loss of billing records.

Also, it is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

18 You have completed this procedure.

Configuring 3PC disk drive backup volumes

At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

<stream_name>

is the name of the billing stream

- 2 Obtain information about the existing backup volumes for the billing stream:

```
conf view <stream_name>
```

where

<stream_name>

is the name of the billing stream

Note: SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

- 3 Quit out of the MAPCI level:

```
quit all
```

- 4 Display and record the size of a volume and its number of free blocks:

```
diskut;lv <volume name>
```

where

<volume name>

is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5 Repeat [step 4](#) for each volume name that you recorded in [step 2](#).

- 6 Create a twelve-character, alphanumeric name for each of the new backup volumes that you determined in the procedure [Calculate disk space to contain backup volumes on page 200](#). Record each of these names for future reference.

Note 1: 3PC volume names on the 3PC disks can be up to twelve alphanumeric characters in length, with the first four characters reserved for the disk prefix.

Note 2: Logical volumes must be configured evenly across the disks.

- 7 Access the disk administration level:

diskadm <disk prefix>

where

<disk prefix>

is one of the prefixes assigned to the two disks; for example, FD00 or FD01

- 8 Determine the free disk space:

dd

- 9 Note the following example, which is a response to the command performed in [step 8](#), choosing the FD00 disk name.

Disk drive information for FD00

```
Date last formatted      : 2000/01/01 01:00:50.145 THU.
Date last modified      : 2001/09/26 11:22:38.587 WED.
Total space for volumes : 4095 Mbytes
Total free space        : 1014 Mbytes
Size of largest free segment : 1014 Mbytes
Total number of volumes : 14
```

1 Block = 512 bytes

- 10 Determine the size of the largest free segment.

If the size of the largest free segment is	Do
greater than or equal to the maximum allowable volume size for the IOP disk type	step 11
less than the maximum allowable volume size for the IOP disk type	contact your next level of support before proceeding with this procedure

- 11 Create a new logical volume:

cv <volume> <size> ftfs

where

<volume>

is the backup volume name

<size>

is the size of the volume. Compare the size recorded in step 1 of the procedure [Calculate disk space to contain backup volumes on page 200](#) with the allowable size for the IOP disk type (obtained from the table under [step 2](#) of the same procedure. The lesser of the two values must be entered as this size.

Example

cv AMA8 50 ffs

This entry prompts the system to create the logical volume FD00AMA8, consisting of 50 Mbyte (102400 512-byte blocks) of available disk space.

- 12 Exit the disk administration level at the prompt:

quit

- 13 Repeat [step 7](#) through [12](#) until all new logical volumes have been created.

- 14 Exit to the command prompt:

quit all

- 15 Configure the billing stream of the logical volumes you created in [step 11](#) through [14](#) once you receive confirmation that the files are successfully created, by performing the procedure “Configuring SBA backup volumes on a billing stream” in *North American ATM/IP Solution-level Accounting*, NN10412-800 or *International ATM/IP Solution-level Accounting*, NN10400-800

- 16 Exit back to the command prompt:

quit all

Note: You must alert all operating company personnel who are associated with the DMS switch. Provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware of that any RESTARTs or SwActs that occur before the billing stream returns to normal mode can cause a loss of billing records.

Also, it is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

- 17 You have completed this procedure.

Administration: Creating Disaster Recovery Floppy Disks

The disaster recovery operation is used when it is necessary to restore the programs and data stored on your OAM&P workstation. The disaster recovery operation depends on the use of disaster recovery floppy disks. You can use the tape drive application to create the two disaster recovery floppy disks required to perform the disaster recovery operation.

To create the disaster recovery floppy disks, perform the following steps:

At the OAM&P workstation

- 1 Label two formatted floppy disks as Disaster Recovery Disk 1 and Disaster Recovery Disk 2.
- 2 Insert Disaster Recovery Disk 1 into the A: drive in your OAM&P workstation and follow the directions.

Note 1: The disaster recovery floppy disk creation process does not format the disks for you, but it does erase all of the data on the disks. Ensure that you have copied important data from the disks before proceeding.

Note 2: For more information on creating disaster recovery disks, refer to the tape drive documentation provided with the OAM&P workstation.

Administration: Creating Disaster Recovery Floppy Disks (continued)

Restore operations

Restore operations are performed when it is necessary to apply previously backed-up data to the current component. The following table lists the procedures used to restore Succession components.

Component restoration procedures

Component	Procedure (s)	Page
NETWORK INTELLIGENCE		
CS 2000	Bootling the XA-Core from a Reset Terminal	221
Call Agent	Restoring a Call Agent Restoring files from a DVD-RW	227 230
SAM21	Shelf Controller reload or restart	234
GWC	Restart or reboot a GWC card	235
Session Server	Prepare for a database restore on a Session Server unit	243
Policy Controller	Prepare for a database restore on a Policy Controller unit Perform a database restore to a Policy Controller unit	248 253
Ethernet Routing Switch 8600	Resetting the Ethernet Routing Switch 8600 using a saved configuration file	255
UAS	Restoring UAS configuration files Restoring audio files to a UAS node	257 261
MS 2000 Series	Restoring audio files to a Media Server 2000 Series node	262
APS	Restoring the APS-specific Oracle database and application files	263
USP	Administration: Restore Operations	266
Real-time Transport Protocol (RTP) Media Portal	RTP Media Portal Basics, NN10367-111	
CICM	CICM Security and Administration, NN10252-611	
CORE NETWORK		

Component restoration procedures

Component	Procedure (s)	Page
Multiservice Switch or Media Gateway devices	Restoring Multiservice Switch or Media Gateway service data	272
GATEWAYS		
MG 9000	none (See Note 1)	
MG 4000	none (See Note 1)	
IW SPM	none (See Note 1)	
NETWORK MANAGEMENT		
Core Element Manager (CEM)	Restoring Core Element Manager data	277
CS 2000 Core Manager or CBM	Performing a full restore of the software from S-tape Performing a partial restore of the software from S-tape Recovering backup files from lost backup volumes	279 294 304
CS 2000 Management Tools	Restoring the oracle data on an SSPFS-based server Performing a full system restore on an SPFS-based server	307 313
Integrated EMS	Restoring the oracle data on an SSPFS-based server Performing a full system restore on an SPFS-based server	307 313
Integrated EMS centralized security server	Restoring the central security server	319
MG 9000 Manager	Restoring the oracle data on an SSPFS-based server Performing a full system restore on an SPFS-based server	307 313
Preside MDM	none (See Note 2)	

Component restoration procedures

Component	Procedure (s)	Page
USP Manager	none (See Note 3)	
Note 1: The IW SPM and MG 4000 are automatically restored when the CS 2000 is restored. The MG 9000 is restored when the MG 9000 Manager is restored. Note 2: The Preside MDM is restored by copying files from tape or an off box storage system through UNIX commands or CRON jobs. Note 3: The USP Manager is restored using the two disaster recovery disks created in the "Administration: Creating Disaster Recovery Floppy Disks on page 216" procedure. Insert Disaster Recovery Disk #1 into the A: drive of your OAM&P workstation and follow the instructions.		

Booting the XA-Core from a Reset Terminal

ATTENTION

Booting the switch causes the switch to drop all calls.

This procedure boots the XA-Core from a reset terminal display.

Note: An image loads from a small computer systems interface (SCSI) device. The SCSI device can be in a disk or a digital audio tape (DAT).

Common Procedures

There are no common procedures.

Stepwise Procedure

Use this procedure to boot the XA-Core from a reset terminal display.



CAUTION

Call your next level of support

Contact your next level of support before performing this procedure.



CAUTION

Extended service interruption

A longer recovery time occurs for a switch boot from tape than a switch boot from disk.

To minimize recovery time, boot from disk.



CAUTION

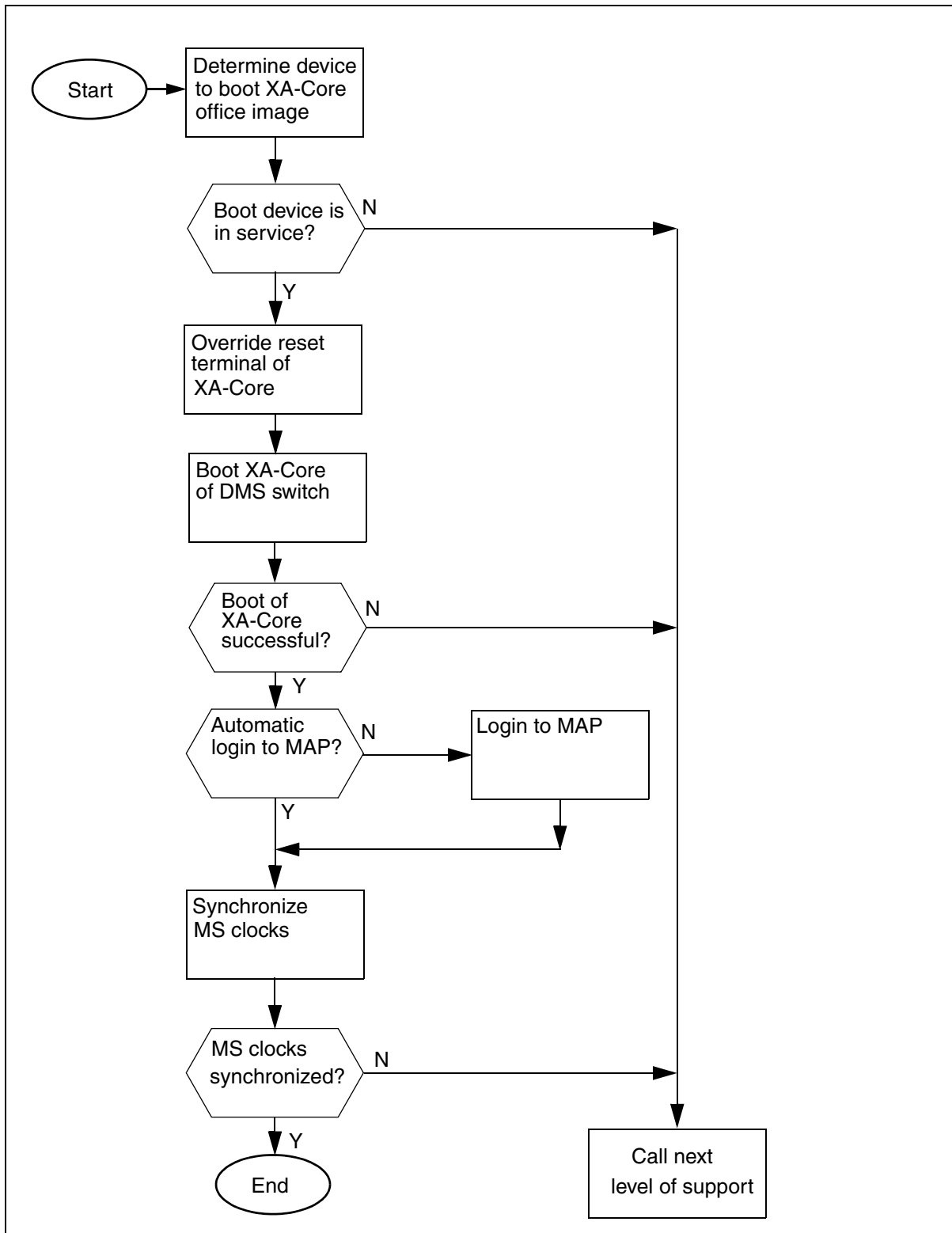
Extended service interruption

Log-in procedures can vary depending on your office configuration.

If you need additional help, contact your next level of support.

The following flowchart summarizes this recovery procedure.

Note: Press the <ENTER> key to execute typed commands.

Booting an XA-Core from a reset terminal

How to boot an XA-Core from a reset terminal

At your current location

- 1 Refer to office records and determine the name of the XA-Core recording device that contains the last office image file.

Note: The XA-Core recording device is a disk drive or a tape drive for a digital audio tape (DAT). Record the name of the XA-Core device.

At the XA-Core shelf

- 2 Make sure that the disk drive or the tape drive that you recorded in [step 1](#) is in-service.

Note: The device is in-service when the green light-emitting diode (LED) is on (illuminated).

If the device is	Do
in service	step 3
not in service	step 13

At the XA-Core reset terminal

- 3 Override the XA-Core reset terminal by typing:

>\OVERRIDE

Example of a reset terminal response

NOW IN SERVICE AFFECTING MODE

- 4 Boot the XA-Core by typing:

>\BOOT <nn> <s> <p>

Where:

<nn> is the slot number parameter value to indicate the number of the physical shelf slot - 0 to 18

<s> is the side parameter value to indicate the circuit pack or packlet location in the physical shelf - front (f) or rear (r)

<p> is the position parameter value that indicates the IOP bay - either upper (u) or lower (l)

Example

>\BOOT 4 F L

Example of system response:

Warning: Boot command will take it out of service.

Please confirm ("YES", "Y", "NO", or "N")

Type **Y** to confirm the command.

- 5 Monitor the reset terminal display to determine if the switch has booted.

Note: The reset terminal displays a response to indicate a boot in progress. The response also displays diagnostic messages and alphanumeric addresses. When the switch has completely booted, a prompt appears on the display.

One possible example of a reset terminal response

CI:

>

Another possible example of a reset terminal response

FWCI>

If the response has**Do**

a prompt

[step 6](#)

no prompt after approximately 15 min

[step 13](#)

At the MAP terminal

- 6 Press the <BREAK> key to determine if you have to log in.

Note: The log-in message indicates that you have to manually log in. An automatic log in can occur if the office parameters have automatic log in.

Example of a MAP response

Please Login.

If log in is**Do**

not automatic

[step 7](#)

automatic

[step 10](#)

- 7 Login to the MAP terminal by typing:

>**LOGIN**

Example of a MAP response

Enter User Name

- 8 Enter your user name by typing:

><user_name>

Where:

<user_name> is the name of the user for the account.

Example of a MAP response

Enter Password

- 9 Enter the password by typing:

><password>

Where:

<password> is the name of the password for the account.

Example of a MAP response

SuperNode_1 Logged in on 1997/01/15 at 20:37:17

- 10 Access the MS Clock level of the MAP display by typing:

>MAPCI;MTC;MS;CLOCK

- 11 Synchronize the clocks by typing:

>SYNC

If the MAP response is**Do**

a successful completion

[step 12](#)

a failure

[step 13](#)

- 12 You have completed this procedure.

Non-standard condition found

- 13 For additional help, contact your next level of support.

Restoring a Call Agent

This procedure describes how to restore an archived call processing application image from tape.

**CAUTION****Possible service interruption**

Do not use this procedure when in an emergency situation with no stable call processing application image.

If in a situation without a restartable image, contact Nortel Global Network Product Support (GNPS) immediate. Attempting to use this method without a valid call processing application image could fail due to constant resets on the Call Agent.

At the SDM

- 1 Insert the DAT cassette with the image to restore.

At the CS 2000 Core Manager

- 2 Restore the image from tape. This step requires root privilege.

```
# cd /swd/3pc
# tar xvf /dev/rmt0
```

At the Call Agent Manager

- 3 Log in to the inactive Call Agent and change directory to the location in which to restore the image. Verify that enough disk space exists to hold the image.

```
[mtc@hostname mtc]$ cd /3PC/sd00/image0
[mtc@hostname image0]$ df -h .
Filesystem                Size  Used Avail Use% Mounted on
172.16.16.24:/nfsserv/3pc/cs/sd00
                        8.0G  6.6G  1.4G   82% /3PC/sd00
```

- 4 Open a file transfer protocol (FTP) session to the CS 2000 Core Manager, and transfer the image. It may be necessary to become the super user to transfer the file.

```
[mtc@hostname image0]$ su
Password:<root_password>
[root@hostname image0]# ftp <core_manager_ip>
Connected to <core_manager_ip>
220 <core_manager_ip> SFTPD Server (Version 19.0.0.0 Nov 14
Name (<core_manager_ip>:mtc): root
Password: <root_passwd>
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> cd /swd/3pc %% or location of restored image
250 CWD command successful.
ftp> get IMG_TO_RESTORE
local: IMG_TO_RESTORE remote: IMG_TO_RESTORE
227 Entering Passive Mode (10,40,44,6,195,224)
150 Opening data connection for IMG_TO_RESTORE (binary mode)
226 Transfer complete.
225820860 bytes received in 332 secs (6.7e+02 Kbytes/sec)
ftp> bye
221 Goodbye.
```

At the MAP

- 5 Enter the DISKUT level and use the **IMPORT** command to make the image available to the call processing application.

```
CI:
>DISKUT
Disk utility is now active.
DISKUT:
>IMPORT SD00IMAGE0 IMG_TO_RESTORE IMAGE 1020
  IMG_TO_RESTORE : Failed to get record length.
Import: IMG_TO_RESTORE      size: 199 MB
      as: IMG_TO_RESTORE    lrecl: 1020      type: image.

Attempting to import 1 file selected on SD00IMAGE0.

Imported IMG_TO_RESTORE as IMG_TO_RESTORE.

Imported 1 file successfully of 1 attempt on SD00IMAGE0.
>
```

Note: If additional space is needed to import the image, the **IMPORT** command offers to expand the volume.

6 Set the image in the Image Table of Contents (ITOC).

```
>QUIT ALL
CI:
>ITOC CI
ITOC User Interface is now active.
ITOC CI:
>SBF CM IMG_TO_RESTORE 15
IMG_TO_RESTORE is registered in CM ITOC.
The updated ITOC is listed directly below.
Image Table Of Contents:
  A Registered          Generic Device      File
  L Date              Time                  Name
  R MM/DD/YYYY HH:MM:SS
-- - - - -
0 * 02/21/2003 16:59:04 SD01ADUMP1          3PC_LAB1_CSNNC06
1   02/24/2003 11:00:53 SD01ADUMP1          3PC_LAB1_CSNNC06
2   02/28/2003 08:15:29 SD00IMAGE0          IMG_TO_RESTORE
>
```

7 The restored image is now available for booting. This procedure is complete.

Restoring files from a DVD-RW

Application

Use this procedure to restore office images from a digital video disk read write optical disk (DVD-RW). Do not restore an image and overwrite one with the same name.

To restore a volume from DVD-RW, contact Nortel support personnel.

Interval

Perform this procedure when required by your office.

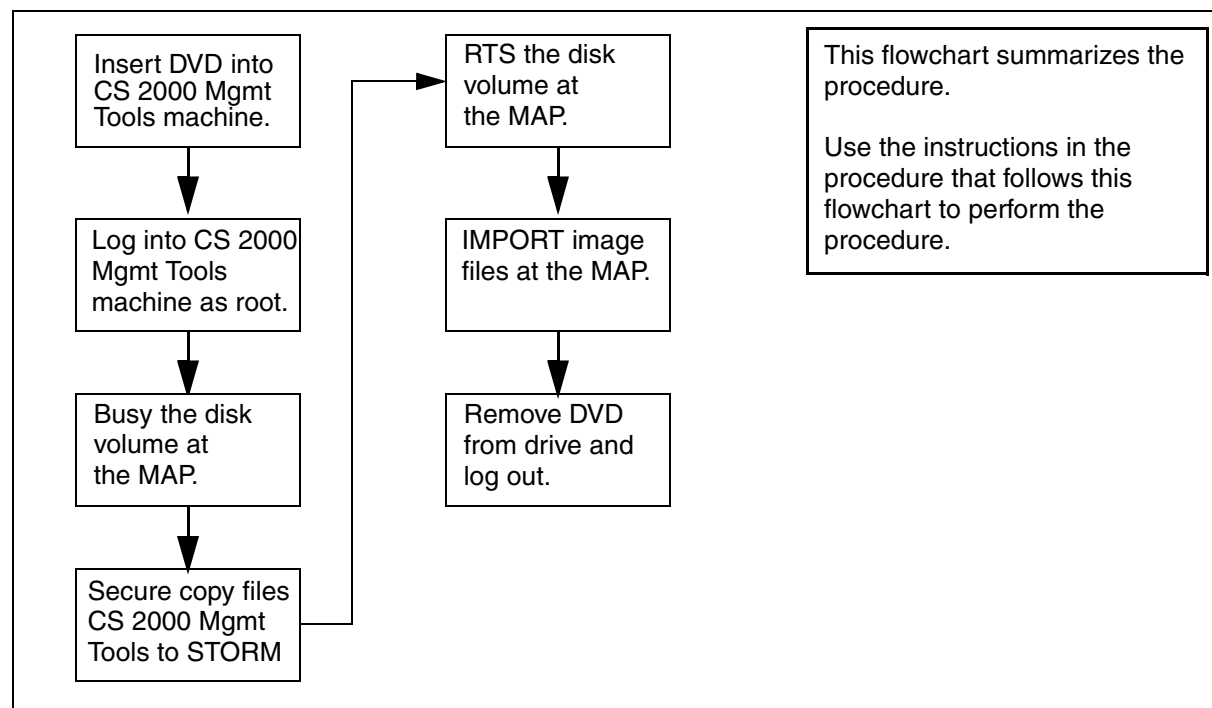
Common procedures

Understanding of the **IMPORT** command in DISKUT, **SCANF** for listing volumes, and the **CBF**, **LBF**, and **SBF** commands in ITOCCI is required. The IP addresses of the STORM units are needed. Use the **mount** command from a Call Agent card to determine the addresses.

Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

Summary of restoring files from a DVD-RW



At the CS 2000 Management Tools server

- 1 Insert the DVD-RW into the DVD tray. If the CS 2000 Management Tools server is a pair of Sun Microsystems Netra 240s, put the DVD in the unit with the USER LED lit.
Volume management software on the CS 2000 Management Tools server operating system mounts the DVD-RW.
- 2 List the contents:

```
$ ls -as /cdrom/cdrom0
```

The contents of the DVD are printed.
- 3 Change directory to the DVD-RW:

```
$ cd /cdrom/cdrom0
```

At the MAP

- 4 Enter the DISKADM level and busy the volumes to copy:

```
> DISKADM <sd0x>; BSY <volname>
```

```
> QUIT
```

sd0x
is SD00 or SD01

volname
is the name of the volume such as TEMP

The BSY command fails if applications have open files on any volume for the device. A busied disk may affect data recording or retrieval for applications. Consider [step 6](#) to RTS the volume as soon as possible or convenient after copying the files.

If applications are active and writing to the volume, determine if the application can ROTATE the disk writing activity to a backup volume. If unsure, contact your next level of support.

At a CS 2000 Management Tools server terminal

- 5 Secure copy the files from the DVD-RW on the CS 2000 Management Tools server to one STORage Management (STORM) unit:

```
$ scp "<image_files>"
```

```
"root@<stormip>:</path_to_files>"
```

image_files
is the file name for a single image file, or a wildcard expression such as "*_CM"

stormip

is the IP Address of the STORM unit such as 172.18.96.6

/path_to_files

is the absolute path to the files on the STORM unit to place the files such as /nfsserv/3pc/cs/sd00/image1

Example

Copy an office image named S040210135002_CM to SD00IMAGE1:

```
$ scp S040210135002_CM
```

```
"root@<stormip>:/nfsserv/3pc/cs/sd00/image1"
```

Note: The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a "y."

The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.

At the MAP

6 Enter the DISKADM level and RTS the volume:

```
> DISKADM <sd0x>; RTS <volname>
> QUIT
```

7 Enter the DISKUT level and IMPORT the image files:

```
> DISKUT; IMPORT SD00IMAGE1
> QUIT
```

The status of the IMPORT command is printed.

IMPORT result

```
> IMPORT SD00IMAGE1
```

```
Attempting to import 1 file selected on SD00IMAGE1.
```

```
Imported S040210135002_CM      as S040210135002_CM      IMAGE 1020.
```

```
Imported 1 file successfully of 1 attempt on SD00IMAGE1.
```

8 List the contents of the volume so the file can be added to the Image Table of Contents (ITOC) in the next step:

```
> SCANF SD00IMAGE1
```

The contents of the volume are printed.

- 9 Enter ITOCCI and register the image in the ITOC:

```
> ITOCCI  
> SBF CM S040210135002_CM <itoc_pos> <alr_flag>
```

itoc_pos

is an integer between 0 and 15, and is a free position in the ITOC.

alr_flag

if this image should be booted for the next restart, specify **ALR**. Otherwise, leave the field blank.

Note: To determine if a free position is available, use the **LBF CM** command. If all positions are used, clear the file in position 15. Determine which volume the position 15 is on, use **SCANF** to list that volume, and then use the **CBF CM FILE <image_name>** command.

At a CS 2000 Management Tools server terminal

- 10 Unmount the DVD-RW, eject it, and exit from root privilege:

```
$ eject cdrom
```

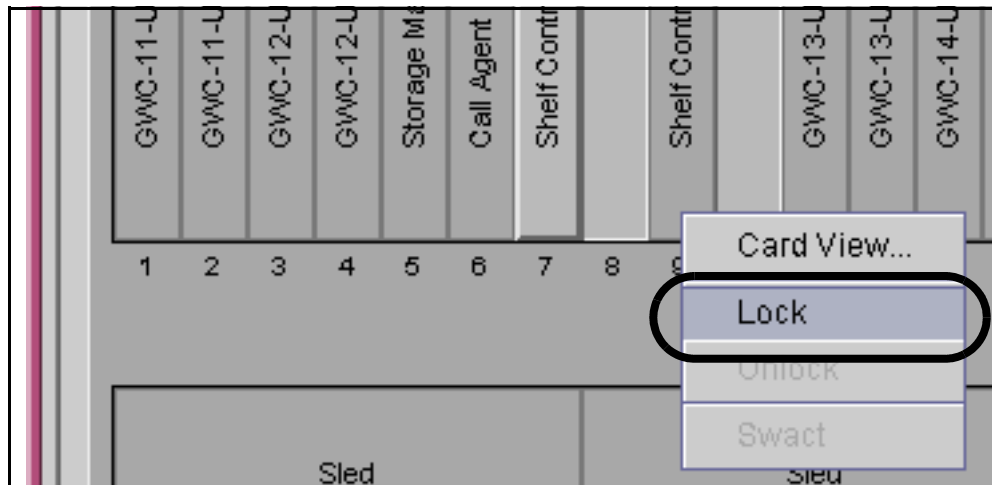
At the CS 2000 Management Tools server

- 11 Remove the DVD-RW from the tray and close the tray.
12 Store the DVD-RW per office procedure.
13 This procedure is complete.

Shelf Controller reload or restart

At the CS 2000 SAM21 Manager client workstation

- 1 From the Shelf View, right click on the card and select Lock from the context menu.



- 2 Wait for the lock icon to appear on the selected card and the other Shelf Controller to indicate that it is in simplex (alarm 2C on the other Shelf Controller).
- 3 Right click on the card again and select Unlock from the context menu.
The card resets, downloads software, and reboots.
- 4 This procedure is complete.

Restart or reboot a GWC card

Purpose of this procedure

Use this procedure to stop all software processes on the GWC card, performs a hardware reset, and reloads the GWC card software from the CS 2000 Core Manager or Core and Billing Manager (CBM).

To restart software applications only, refer to procedure [Restart GWC card services on page 239](#) in this NTP.

When to use this procedure

Use this procedure when you need to reboot a GWC card and force a GWC to download and execute a software load from the The CS 2000 Core Manager or CBM.

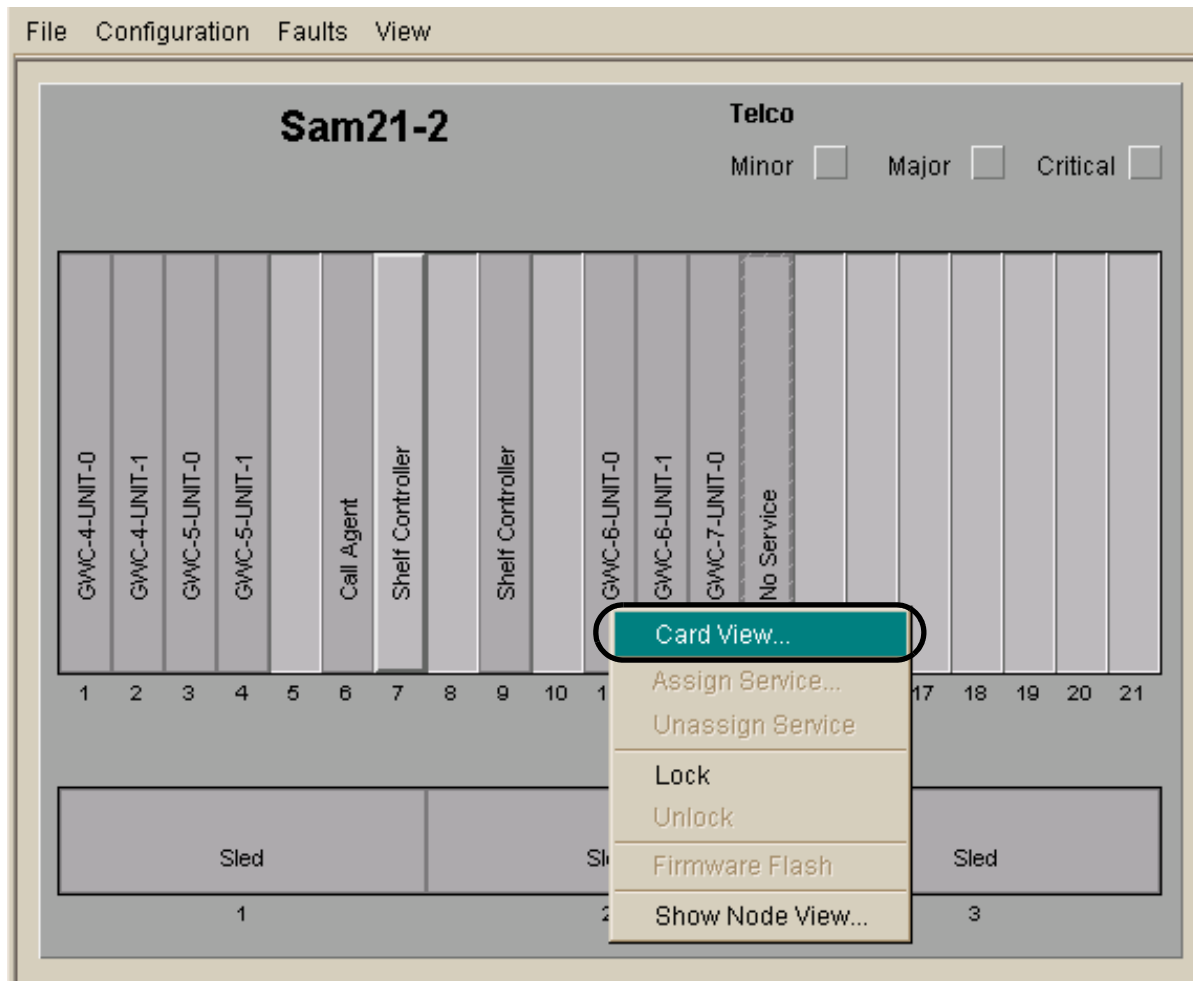
Prerequisites

To reduce the risk of service interruption, you can first busy the GWC applications on specific GWC nodes using the CS 2000 GWC Manager. Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for these procedures.

Action

At the CS 2000 SAM21 Manager client

- 1 From the Shelf View, right-click the GWC card you want to reboot and select **Card View** from the context menu.



- 2 At the Card View, select the **States** tab.

File View

Sam21-2 : Slot 11

Alarms Equip **States** Diags Provisioning

Summary

Critical	Major	Minor
0	0	0

Details

Equip.	ID	Time	Type	Severity	Reason

GWC-6-UNIT-0
11

- 3 Click the **Lock** button to lock the card.

Note: The card must be busy (disabled) before you can lock it. Refer to the procedure “Disable (Busy) GWC card services” in the Gateway Controller Security and Administration NTP, NN10213-611.

File View

Sam21-2 : Slot 12

Alarms Equip States **Diags** Provisioning

OSI

Card Status: Unlocked

Operational: Enabled

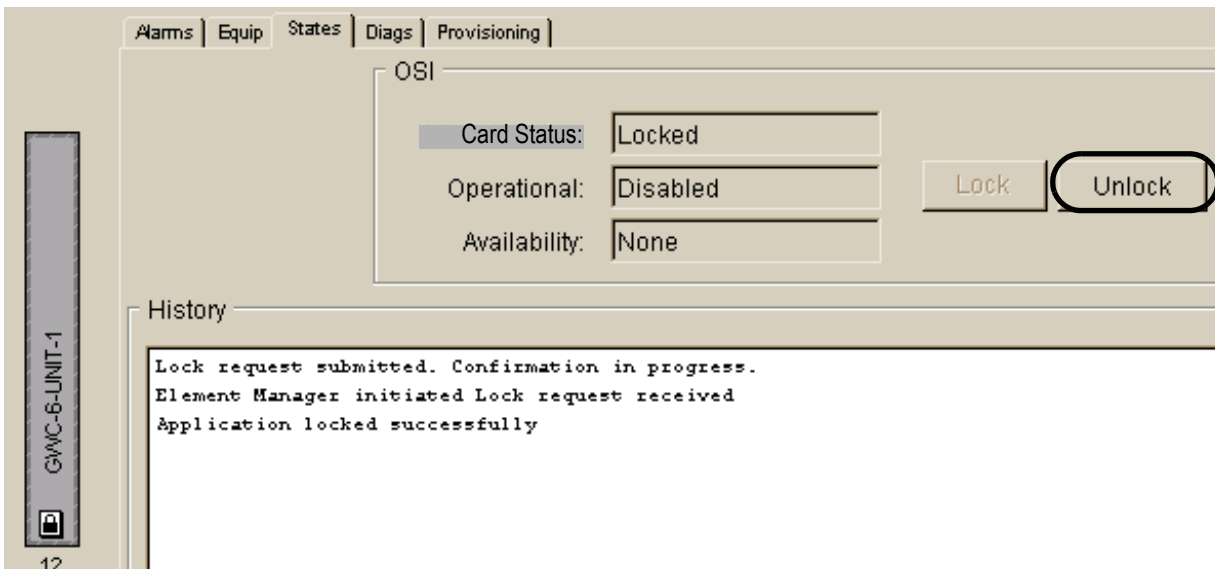
Availability: None

Lock Unlock

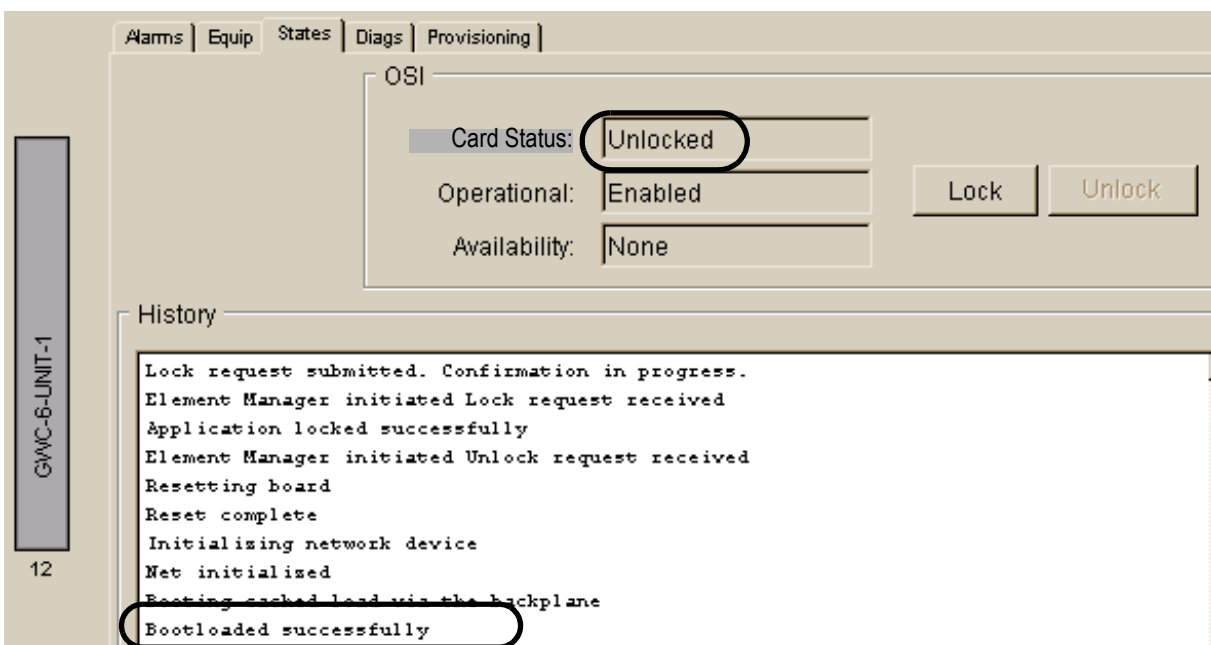
History

3-UNIT-1

- 4 Wait until the Card Status is Locked and the History window indicates “Application locked successfully”. Then, click the **Unlock** button.



- 5 Monitor the reboot process. Wait until the Card Status is “Unlocked” and the History window indicates “Bootloaded successfully”.



- 6 This procedure is complete.

Restart GWC card services

Purpose of this procedure

Use this procedure to stop and restart call processing and network services on a standby GWC card.

To restart the hardware and software on an individual GWC card, refer to procedure [Restart or reboot a GWC card on page 235](#).

When to use this procedure

Use this procedure on a GWC card to determine if a known fault is temporary or persistent and if the fault is limited to the GWC card in question.

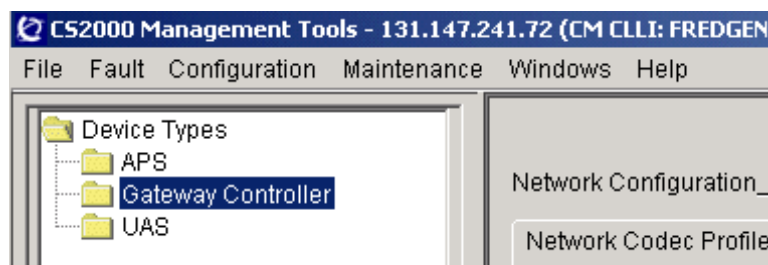
Prerequisites

To reduce the risk of service interruption, ensure that the card you are about to restart is in standby status. Otherwise, perform a call processing switch activity (SwAct) to change the card state from active to standby. Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for procedures to perform a SwAct.

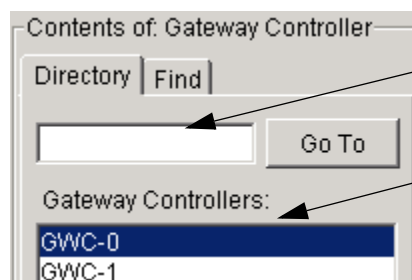
Action

At the CS 2000 GWC Manager client

- 1 At the main CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



- 2 From the Contents of: Gateway Controller frame, select the appropriate GWC node you wish to restart.



Type a GWC node number here,

or

Select a GWC node from the list of provisioned GWC nodes.

- 3 Click the **Maintenance** tab.
- 4 Locate the Activity State field for the GWC unit and determine which unit (card) is active (either unit 0 or unit 1) and which is in standby mode.
- 5 Click the **Busy (Disable)** button for the GWC unit on standby.

Maintenance | Provisioning

GWC-7-UNIT-0

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	coldStandby(2)
Activity state:	standby(2)	Swact state:	noSwAct(0)
Isolation state:	notisolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	GI070BN		

Save Image Busy (Disable) RTS (Enable) Card View

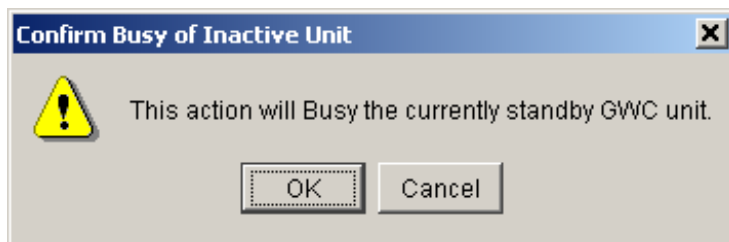
GWC-7-UNIT-1

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	providingService(3)
Activity state:	active(1)	Swact state:	noSwAct(0)
Isolation state:	notisolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	GI070BN		

Save Image Busy (Disable) RTS (Enable) Card View

☐ Force Warm Swact Cold Swact

- 6 At the confirmation box, click **OK** to busy the standby GWC unit.



Wait for the CS 2000 GWC Manager screen to update the Operational state of the card to disabled(2). This indicates that the card has been busied

- 7 Click the **RTS (Enable)** button to return the card to service.

The screenshot shows the CS 2000 GWC Manager interface. It has two sections: "GWC-7-UNIT-0" and "GWC-7-UNIT-1". Each section contains a grid of status fields: Administrative state, Operational state, Activity state, Isolation state, Available state, Loadname, Usage state, Stand by state, Swact state, Alarm state, and Fault state. Below the grid are four buttons: "Save Image", "Busy (Disable)", "RTS (Enable)", and "Card View". In the "GWC-7-UNIT-0" section, the "Operational state" field is "disabled(2)" and the "RTS (Enable)" button is circled. In the "GWC-7-UNIT-1" section, the "Operational state" field is "enabled(1)".

After 30 seconds, the Administrative state field changes to unlocked and the Operational state field changes to enabled.

A close-up of the status fields for GWC-7-UNIT-0. The "Administrative state" field now shows "unlocked (1)", the "Operational state" field shows "enabled (1)", and the "Activity state" field shows "standby (2)".

Note: Normally the state change is automatic. However, if necessary, you can refresh the screen. At the top of the CS 2000 GWC Manager screen, click the **Windows** menu and select **Refresh GWC Status**.



- 8 This procedure is complete.

Prepare for a database restore on a Session Server unit

Purpose of this procedure

Use this procedure to prepare for a restoration of the SIP Gateway application database from a backup copy to the active unit.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of a high level upgrade activity, found in the Session Server Upgrades NTP, NN10349-461.

Limitations and Restrictions



CAUTION

Performing a restore of the SIP Gateway application database to the active unit is a service affecting activity and can cause data mismatches at the CS 2000 call server.

ATTENTION

For security reasons, you can only copy the database file from a remote server to the /users/mtc directory on the unit and you must use the secure copy command **scp** to perform this activity.

Automatic backup of the SIP Gateway application database occurs at 1:00 AM each day on both Session Server units. This configuration setting cannot be modified and does not impact the use of this procedure.

The name of the backup database file is *solid.db*. Do not modify this name.

Prerequisites

You must have secure copy (scp) access to the Session Server unit from the remote system or other server location from where the database backup file *solid.db* is copied.

Action

From the remote server where the backup database file is located

- 1 Log onto the remote server, locate and navigate to the directory where the backup copy of the database file is stored.
- 2 Secure copy the database file to the Session Server unit you are restoring a backup copy of the database to by typing

```
$ scp solid.db mtc@<SS_IP_address>:
```

and pressing the Enter key.

where

SS_IP_address

is the IP address of the Session Server unit

The database file is copied to the /users/mtc directory on the target Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

At the Session Server CLI or Integrated EMS client

- 3 Log onto the Session Server unit you are restoring a backup copy of the database to, and change to the root user.
- 4 Move the solid.db file you copied in [step 2](#) from the /users/mtc directory to the /opt/apps/database/solid/backup directory by typing

```
$ mv /users/mtc/solid.db  
/opt/apps/database/solid/backup
```

and pressing the Enter key.

- 5 Change directory to the backup database directory by typing

```
$ cd /opt/apps/database/solid/backup
```

and pressing the Enter key.

- 6 Verify that the correct version (based on the file date) of the solid.db database file that you want to restore is located in the directory by typing

```
$ ls -l /opt/apps/database/solid/backup
```

and pressing the Enter key.

- 7 Verify that the presence of files *solid.ini* and *solmsg.out* files are also in the `/opt/apps/database/solid/backup` directory.

ATTENTION

The `restorebackup.sh` script does not run if you do not have the *solid.ini* and *solmsg.out* files located in the correct directory.

- 8 If the *solid.ini* file is not present, copy it into the backup directory by typing

```
$ cp /opt/apps/database/solid/dbfiles/solid.ini  
/opt/apps/database/solid/backup/solid.ini
```

and pressing the Enter key
- 9 If the *solmsg.out* file is not present, copy it into the backup directory by typing

```
$ cp  
/opt/apps/database/solid/dbfiles/solmsg.out  
/opt/apps/database/solid/backup/solmsg.out
```

and pressing the Enter key
- 10 Change the ownership of all files in the backup directory by typing

```
$ chown soliddb *
```

and pressing the Enter key.
- 11 Change the group of all files in the backup directory by typing

```
$ chgrp adm *
```

and pressing the Enter key.
- 12 Change the access permissions for all files in the backup directory by typing

```
$ chmod 600 *
```

and pressing the Enter key.
- 13 The database is now ready to be restored. You have completed this procedure. Return to the high-level activity.

Additional information

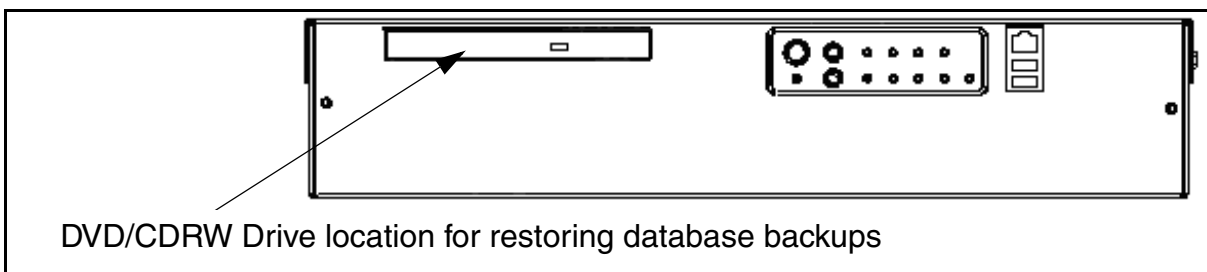
This section provides additional information regarding database restore activities.

To restore a backup database saved to a CD.

If you must restore a database backup that has been saved to a CD, you must first copy the database file from the CD to the default backup directory on the active Session Server unit. The selected backup database file must be restored to the following location:

/opt/apps/database/solid/backup/solid.db

To restore a backup of the database file to the backup directory, you must use a Session Server command line interface to copy the database file from a CD or CD-RW disk containing a copy of the backup database file to the *opt/apps/database/solid/backup* directory.



Ensure that you remove the CD disk from the DVD/CDRW drive, and store it in a safe place when you are done.

To restore a database backup saved to another system

If you must restore a database backup that has been saved to another system, you must first copy the database file from the remote system back to the default backup directory on the active Session Server unit. The selected backup database file must be restored to the following location:

/opt/apps/database/solid/backup

To restore a backup of the database to the backup directory you must use a Session Server command line interface to copy the database file *solid.db* from the remote system to the *opt/apps/database/solid/backup* directory. You may also be able to remote copy the backup database file from the remote system to the Session Server *opt/apps/database/solid/backup* directory. However, for security reasons, you may need to consult your site network administrator for instructions and permission to perform a remote copy.

Perform a database restore to a Session Server unit

Purpose of this procedure

Use this service impacting procedure to restore a SIP Gateway application database from a backup copy to the active Session Server units.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of a high level upgrade activity, found in the Session Server Upgrades NTP, NN10349-461.

Limitations and Restrictions



CAUTION

This procedure can only be executed on the active unit. Performing a restore of the SIP Gateway application database to the active unit is service affecting, and can cause data mismatches at the CS 2000 call server.

Prerequisites

You must first have completed procedure [Prepare for a database restore on a Session Server unit on page 243](#).

Action

At the Session Server CLI or Integrated EMS client

- 1 Log onto the active Session Server unit you are restoring a backup copy of the database to, and change to the root user.
- 2 Change directories by typing

```
$ cd /opt/apps/database/solid_install
```

and pressing the Enter key.
- 3 Run the database restore script by typing

```
$ ./restorebackup.sh
```

and pressing the Enter key.
- 4 You have completed this procedure. Return to the high-level activity.

Prepare for a database restore on a Policy Controller unit

Purpose of this procedure

Use this procedure to prepare for a restoration of the Policy Controller application database from a backup copy.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of the high level upgrade activity “Perform an emergency maintenance release rollback activity” found in the Policy Controller Upgrades NTP, NN1xxxx-461.

Limitations and Restrictions



CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

ATTENTION

For security reasons, you can only copy the database file from a remote server to the /users/mtc directory on the unit and you must use the secure copy command **scp** to perform this activity.

Automatic backup of the Policy Controller application database occurs at 1:00 AM each day on both Policy Controller units. This configuration setting cannot be modified and does not impact the use of this procedure.

The name of the backup database file is *solid.db*. Do not modify this name.

Prerequisites

You must have secure copy (scp) access to the Policy Controller unit from the remote system or other server location from where the database backup file *solid.db* is copied.

Action

From the remote server where the backup database file is located

- 1 Log onto the remote server, locate and navigate to the directory where the backup copy of the database file is stored.
- 2 Secure copy the database file to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
$ scp solid.db mtc@<PC_IP_address>:
```

and pressing the Enter key.

where

PC_IP_address

is the IP address of the Policy Controller unit

The database file is copied to the /user/mtc directory on the target Policy Controller unit. This is the only Policy Controller directory that files can be copied into from an external server.

At a Policy Controller command line interface

- 3 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
> ssh -l <userid> <PC_IP_address>
```

and pressing the Enter key.

where

userid

is a valid userid (like mtc) on the Policy Controller

PC_IP_address

is the IP address of the Policy Controller

Example

```
ssh -l mtc 45.128.54.12
```

- 4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 5 When prompted, enter the root password.

- 6 Move the solid.db file you copied in [step 2](#) from the /user/mtc directory to the /opt/apps/database/solid/backup directory by typing

```
$ mv /users/mtc/solid.db  
/opt/apps/database/solid/backup
```

and pressing the Enter key.
- 7 Change directory to the backup database directory by typing

```
$ cd/opt/apps/database/solid/backup
```

and pressing the Enter key.
- 8 Verify that the correct version (based on the file date) of the solid.db database file that you want to restore is located in the directory by typing

```
$ ls -l /opt/apps/database/solid/backup
```

and pressing the Enter key.
- 9

ATTENTION

The restorebackup.sh script does not run if you do not have the solid.ini and solmsg.out files located in the correct directory.

- Verify that the presence of files *solid.ini* and *solmsg.out* files are also in the /opt/apps/database/solid/backup directory.
- 10 If the solid.ini file is not present, copy it into the backup directory by typing

```
$ cp /opt/apps/database/solid/dbfiles/solid.ini  
/opt/apps/database/solid/backup/solid.ini
```

and pressing the Enter key
 - 11 If the solmsg.out file is not present, copy it into the backup directory by typing

```
$ cp  
/opt/apps/database/solid/dbfiles/solmsg.out  
/opt/apps/database/solid/backup/solmsg.out
```

and pressing the Enter key
 - 12 Change the ownership of all files in the backup directory by typing

```
$ chown soliddb *
```

and pressing the Enter key.

- 13 Change the group of all files in the backup directory by typing
`$ chgrp adm *`
and pressing the Enter key.
- 14 Change the access permissions for all files in the backup directory by typing
`$ chmod 600 *`
and pressing the Enter key.
- 15 The database is now ready to be restored. You have completed this procedure. Return to the high-level activity.

Additional information

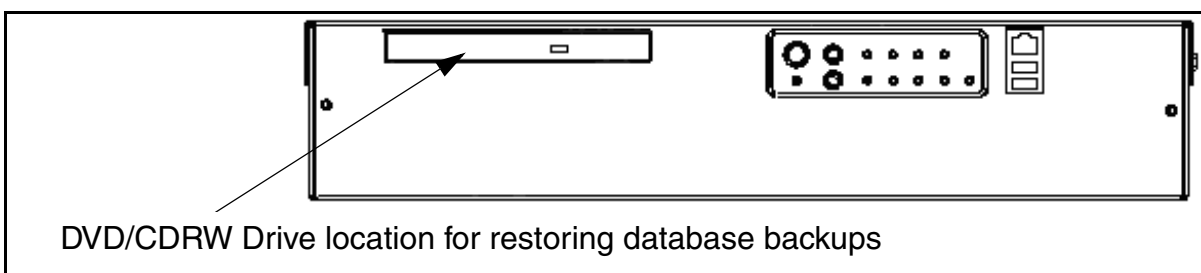
This section provides additional information regarding database restore activities.

To restore a backup database saved to a CD.

If you must restore a database backup that has been saved to a CD, you must first copy the database file from the CD to the default backup directory on the active Policy Controller unit. The selected backup database file must be restored to the following location:

/opt/apps/database/solid/backup/solid.db

To restore a backup of the database file to the backup directory, you must use a Policy Controller command line interface to copy the database file from a CD or CD-RW disk containing a copy of the backup database file to the `opt/apps/database/solid/backup` directory.



Ensure that you remove the CD disk from the DVD/CDRW drive, and store it in a safe place when you are done.

To restore a database backup save to another system

If you must restore a database backup that has been saved to another system, you must first copy the database file from the remote system back to the default backup directory on the active Policy Controller unit.

The selected backup database file must be restored to the following location:

/opt/apps/database/solid/backup

To restore a backup of the database to the backup directory you must use a Policy Controller command line interface to copy the database file `solid.db` from the remote system to the `opt/apps/database/solid/backup` directory. You may also be able to remote copy the backup database file from the remote system to the Policy Controller `opt/apps/database/solid/backup` directory. However, for security reasons, you may need to consult your site network administrator for instructions and permission to perform a remote copy.

Perform a database restore to a Policy Controller unit

Purpose of this procedure

Use this service impacting procedure to restore a Policy Controller application database from a backup copy to either the active or inactive Policy Controller units.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of the high level upgrade activity “Perform an emergency maintenance release rollback activity” found in the Policy Controller Upgrades NTP, NN10431-461.

Limitations and Restrictions



CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

Prerequisites

You must first have completed procedure [Prepare for a database restore on a Policy Controller unit on page 248](#).

Action

At a Policy Controller command line interface

- 1 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
> ssh -l <userid> <PC_IP_address>
```

and pressing the Enter key.

where

userid

is a valid userid (like mtc) on the Policy Controller

PC_IP_address

is the IP address of either Policy Controller unit

Example

```
ssh -l mtc 45.128.54.12
```

- 2 Change to the root user by typing
\$ su - root
and pressing the Enter key.
- 3 When prompted, enter the root password.
- 4 Change directories by typing
\$ /opt/apps/database/solid_install
and pressing the Enter key.
- 5 Run the database restore script by typing
\$./restorebackup.sh
and pressing the Enter key.
- 6 You have completed this procedure. Return to the high-level activity.

Resetting the Ethernet Routing Switch 8600 using a saved configuration file

The Ethernet Routing Switch 8600 boot command allows you to reset or reboot the system using a saved configuration file. You must have access to the Boot Monitor CLI through a direct connection to the switch or a Telnet connection. For more information on accessing the Boot Monitor CLI, refer to "Managing the Ethernet Routing Switch 8000 Series Switch Using the Command Line Interface Release 3.2," 313194-*.

Note: You must be directly connected to the switch to initiate a Boot Monitor session. You can only connect using a Telnet connection if the Boot Monitor CLI is already active.

Resetting the Ethernet Routing Switch 8600 using a saved configuration file

At the Boot Monitor CLI

- 1 Issue the boot command by typing

```
monitor# boot [<file>] [config <value>]
```

where

file

is the software image device and file name in the format [a.b.c.d:]<file> | /pcmcia/<file> | /flash/<file>. The file name, including the directory structure, can be up to 1024 characters.

config <value>

is the software configuration device and file name in the format [a.b.c.d:]<file> | /pcmcia/<file> | /flash/<file>. The file name, including the directory structure, can be up to 1024 characters.

- 2 You have completed this procedure.

Restoring UAS configuration files

At the time of installation, the UAS is configured to automatically back up configuration files each day at 2:00 am. If an APS node is configured in the network, all UAS nodes in the network can be backed up to the APS node. If an APS node is not configured in the network, the configuration files for UAS nodes in the network can be backed up, instead, to a remote UNIX server.

The backed-up files can be restored should a catastrophic system event, such as a hard disk drive failure, create the need for a re-installation. The files are restored by manually transferring the files from the APS node or remote UNIX server to the UAS node after the UAS software (and NGS software, if necessary) has been re-installed. The backed-up files are located in the directory, /opt/uas/uas_conf_backup and include:

- C:\UAS\etc\UAS.conf (all configurations)
- C:\UAS\etc\ugw.conf (for a PRI gateway only)
- C:\UAS\etc\atmconn.con (ATM only)
- C:\UAS\etc\mainasa.conf (all configurations)
- C:\UAS\etc\atmhard.con (ATM only)
- C:\etc\srconf\agt\snmpd.cnf (all configurations)
- C:\Winnt\system32\drivers\etc\hosts (all configurations)
- C:\UAS\etc\atmSvcProfile.con (ATM only)
- C:\UAS\etc\atmhardloop.con (ATM only)

This procedure enables you to restore backed-up UAS configuration files that are stored either on an APS node or on a remote UNIX server.

Restoring UAS configuration files

At the Network Element Status panel of the Universal Audio Server Manager

- 1 In the Network Elements pane, select the appropriate UAS node.
Information about the node displays in the System Identification pane.
- 2 In the pull-down list in the box labeled, "Please select," select Maintenance.
- 3 In the Maintenance Tree pane, select "Node".

- 4 Click the node entry that displays in the table shown in the Node States pane.
- 5 Lock the node by clicking the “Lock Graceful” button located at the bottom of the Node States pane.

At the Windows desktop interface

- 6 Log in as Administrator.
- 7 Stop any applications that are running.
 - a Access the “Services” window as follows:
select **Start -> Programs -> Administrative Tools -> Services**
 - b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.
- 8 Perform the following steps:
 - a Enter the following command:
cd \UAS\etc
 - b Access the APS server directory containing the backed up configuration files by entering the following:
mount * \\<APS IP address>\opt\uas\uas_conf_backup\<UAS node>\current (all of this command is entered on one line)

where <APS IP address> is the address of the server containing the backed up configuration files, and <UAS node> is the full directory path that contains the name of the UAS node that you are restoring the backed up configuration files to.
 - c Execute the following command to confirm that the directory containing the backed-up configuration files is mounted:
net use
 - d Change directories to the location of the newly mounted configuration file backup directory by entering the following:
cd <mounted drive letter>

where <mounted drive letter> is the drive letter (for example, “F”) displayed as the result of the previous command.
 - e List the contents of the configuration file backup directory by entering the following command in response to the prompt:
ls -l

The following backed up files should display:

- UAS.conf (for all configurations)
- ugw.conf (for a PRI gateway only)
- atmconn.conf (for ATM only)
- mainsa.conf (for all configurations)
- atmhard.conf (for ATM only)
- snmpd.cnf (for all configurations)
- hosts (for all configurations)
- atmSvcProfile.conf (for ATM only)
- atmhardloop.conf (for ATM only)

- f** Enter the following command to copy the contents of the mounted configuration file backup directory to the appropriate subdirectory on your UAS:

```
copy *.* c:\UAS\etc\
```

- g** Unmount the configuration file backup directory by entering the following command:

```
umount <drive letter>
```

where <drive letter> is the drive letter that you entered in step [d](#).

- h** At the system console, perform the following steps:

```
mv snmpd.cnf \etc\srconf\agt\snmpd.cnf
```

```
mv hosts \Winnt\system32\drivers\etc\hosts
```

- 9** Restart the network element by performing the following steps:

- a** Access the “Services” window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

- b** Right-click PMGRdaemon service and select Start.

At the Network Element Status panel of the Universal Audio Server Manager

- 10** In the Network Elements pane, select the appropriate UAS node.
Information about the node displays in the System Identification pane.
- 11** In the pull-down list in the box labeled, “Please select,” select Maintenance.

- 12** In the Maintenance Tree pane, select “Node”.
- 13** Click the node entry that displays in the table shown in the Node States pane.
- 14** Unlock the node by clicking the “Unlock” button located at the bottom of the Node States pane.
- 15** You have completed this procedure.

Restoring audio files to a UAS node

In the event that a re-installation of a UAS node is required due to an error condition, audio files must be restored to the unit when it becomes operational. This procedure allows you to enable audio provisioning to the node and to specify which audio files are to be restored to it.

Note: For more information about re-installation of a UAS node, contact your Nortel Networks service representative.

Restoring audio files to a UAS node

At your web browser interface

- 1 After the re-installation of the UAS node has been completed, determine whether you want to enable provisioning of the node occur during the next audio distribution cycle or immediately.

If	Do
you want to enable provisioning of the node to occur during the next audio distribution cycle	step 2
you want audio provisioning of the node to occur immediately	step 3

- 2 Perform the procedure “Enabling provisioning of a UAS node” in the document, NN10095-511, entitled “UAS Configuration Management,” in your UAS document suite.

Note: Provisioning of the node will begin during the next audio distribution cycle. The distribution cycle occurs once per hour.

- a Go to step [4](#).

- 3 Perform the procedure “Provisioning a UAS node” in the document, NN10095-511, entitled “UAS Configuration Management,” in your UAS document suite.

Note: Provisioning of the node will begin immediately although as much as a five-minute delay may occur before actual provisioning activity begins.

- 4 You have completed this procedure.

Restoring audio files to a Media Server 2000 Series node

In the event that a re-installation of a Media Server 2000 Series node is required due to an error condition, audio files must be restored to the unit when it becomes operational. This procedure allows you to enable audio provisioning to the node and to specify which audio files are to be restored to it.

Note: For more information about re-installation of a Media Server 2000 Series node, contact your Nortel Networks service representative.

Restoring audio files to a Media Server 2000 Series node

At your web browser interface

- 1 After the re-installation of the Media Server 2000 Series node has been completed, determine whether you want to enable provisioning of the node occur during the next audio distribution cycle or immediately.

If	Do
you want to enable provisioning of the node to occur during the next audio distribution cycle	step 2
you want audio provisioning of the node to occur immediately	step 3

- 2 Perform the “Enabling provisioning of a Media Server 2000 Series node” (refer to the Media Server 2000 Series Configuration Management document).

Note: Provisioning of the node will begin during the next audio distribution cycle. The distribution cycle occurs once per hour.

- a Go to step [4](#).

- 3 Perform the procedure “Provisioning a Media Server 2000 Series node” (refer to the Media Server 2000 Series Configuration Management document).

Note: Provisioning of the node will begin immediately although as much as a five-minute delay may occur before actual provisioning activity begins.

- 4 You have completed this procedure.

Restoring the APS-specific Oracle database and application files

To ensure successful recovery from a system problem that causes database file corruption, you should periodically back up the database files that support operation of the APS. These files include:

- Oracle database
- Root database files
- Non-Root database files

The Succession Server Platform Foundation Software (SSPFS) base software provides utilities that enable you to restore these files. The “rsimpora” utility restores the APS Oracle database files. The “ufsrestore” utility restores the UNIX file system, including all of the “Root” and “Non-Root” APS database files.

The instructions for performing these backup procedures are found in the document titled *ATM/IP Configuration*, NN10276-500.

In addition to these two utilities, two additional APS utilities and procedures enable you to restore selected files when only the files required for APS operation must be restored. The “ips_export_db.sh -restore” utility restores only the APS Oracle database. A procedure that utilizes the UNIX “tar” command enables you to restore the non-Root files, “/audio_files,” “/PROV_data,” “/user_audiofiles,” and Root file, “/etc/inet/hosts.”

This procedure enables you to restore the APS-specific Oracle database and application files (/PROV_data, /audio_files, and /user_audio_files).

Restoring the APS-specific Oracle database and application files

In a telnet connection to the APS server

- 1 Open an xterm window and log in using the “maint” login and password.
- 2 Become the “root” user by entering:
su - root
- 3 Determine whether you are restoring Oracle database files from tape or from disk.

If

you are restoring from tape

Dostep [4](#)

	If	Do
	you are restoring from disk	step 9
4	Insert the appropriate "ORACLE" backup tape into the DDS-3 tape drive.	
5	Rewind the backup tape by performing the following command:	
		mt -f /dev/rmt/0c rewind
6	Start the restoration of the APS Oracle database from the tape by entering the following command:	
		ips_export_db.sh -t /dev/rmt/0c -restore
	Note: This command is entered on a single line.	
	Messages logging the progress of the restoration display on the screen. When you are prompted about continuing the restoration even if the current database will be destroyed, enter "y" (yes).	
7	After the restoration of the Oracle database is complete, rewind the backup tape by performing the following command:	
		mt -f /dev/rmt/0c rewind
8	Eject the backup tape and store it for possible use later.	
	a Go to step 10 .	
9	Start the restoration of the APS Oracle database from the disk by entering the following command:	
		ips_export_db.sh -diskonly -restore
	Note: This command is entered on a single line.	
	Messages logging the progress of the restoration display on the screen. When you are prompted about continuing the restoration even if the current database will be destroyed, enter "y" (yes).	
10	Insert the appropriate "application file" backup tape into the DDS-3 tape drive.	
11	Change directory to the root directory:	
		cd /
12	Rewind the backup tape by performing the following command:	
		mt -f /dev/rmt/0c rewind
13	Restore the application files (/PROV_data, /audio_files, and /user_audio_files) by entering the following command:	
		tar xvf /dev/rmt/0c

- 14 When the restoration of the application files completes, remove the tape from the tape drive and store for possible use later. Insert another write-enabled DAT tape into the drive to be used for the automatic Oracle system back up that runs daily at 1:00 a.m.
- 15 Verify that the application files have been restored by entering the following commands:

```
cd /PROV_data
```

```
ls -l
```

The files should display on the screen.

```
cd /user_audio_files
```

```
ls -l
```

The files should display on the screen.

```
cd /audio_files
```

```
ls -l
```

The files should display on the screen.
- 16 You have completed this procedure.

Administration: Restore Operations

You can use the restore operation to return your system to a configuration that was saved during a backup operation. The typical use of the restore operation is as follows:

- An emergency situation occurs which requires you to restore a system configuration from a stored data snapshot.
- You use the file manager function to ensure that there are copies of the data snapshot to be restored on both RTC system nodes.
- You make the data snapshot the boot data snapshot for both RTC system nodes.
- You deactivate the linksets and change the path state of the application server process (ASP) paths to Down for your system, as appropriate.
- You perform a COR on your system, which means that you unseat the RTC system nodes, turn off both power switches on the shelf, reseal the RTC system nodes, and then restore power. Your stored data snapshot is now the running data snapshot.

Complete the following procedures to restore data snapshots stored on your alternate boot server or on the RTC system nodes.

Restoring a system configuration from a data snapshot stored on your alternate boot server



CAUTION

Performing a COR on your system is service affecting. Nortel Networks recommends that you do this during off-peak hours and that you ensure that a mated system is available.



WARNING

Do not power down the shelf when the SCSI disk light on the RTC system node is on. To do so could cause a disk failure.

**WARNING**

Wear wrist straps, and use standard anti-static precautions.

At the OAMP workstation

- 1 Click **Administration>File Manager**.
- 2 From the Alternate Boot Server section, select the Snapshot folder, Version folder (for example, v10.0.0) and the snapshot file for the required system configuration.
- 3 From the right side of the window, select the RTC system node in slot 12, the Snapshot folder, and the Version folder (the same version folder as selected in [step 2](#)).
Note: The Version folder may not exist if a snapshot has never been stored on the RTC system node.
- 4 View the content of the Version folder on the right side of the window. If the data snapshot to be restored from the Alternate Boot Server is not listed or the Version folder does not exist, proceed to [step 5](#). If the data snapshot to be restored is listed in the field, proceed to [step 7](#).
- 5 From the Alternate Boot Server section, select the data snapshot to be restored.
- 6 Initiate a copy operation by clicking the suitcase icon. An hourglass is displayed while the snapshot is being copied.
When the copy operation is complete, the fields in the Destination portion of the window update with the information for the copied snapshot.
- 7 Open the RTC system node administration tab for the RTC system node in slot 12. To do this, click **Configuration>platform>node**. Click the **Graphical view** tab, then double-click slot 12 to transfer the Administration panel.
- 8 Change the boot data snapshot setting for the RTC system node. To do this, click the button next to the Boot Data Snapshot field. The system displays the Boot Data Snapshot window. Select the data snapshot to be restored. The Boot Data Snapshot window closes.

- 9 Click **Modify** to save the changes. The change is reflected in the Boot Data Snapshot field.

Note: When you change the boot data snapshot, a minor alarm is generated which indicates that the running data snapshot is different from the boot data snapshot. This alarm is cleared when you perform a COR on your system or if you should change the boot data snapshot back to match the running boot data snapshot.
- 10 Deactivate the linksets for your system, as appropriate. To do this, perform the following steps:
 - a Click **Configuration>MTP>Linksets**.
 - b Locate and post the linksets you want to deactivate.
 - c Click the **Deactivate** button to deactivate the posted linksets. All links in a linkset are deactivated by this command.
- 11 Change the path state of the ASP paths to Down, as appropriate. To do this, perform the following steps:
 - a Click **Configuration>IPS7>Application server process path**.
 - b Locate and post the paths whose state you want to change.
 - c Click **Down** to change the state of the paths.
- 12 If the RTC system node is inactive RTC, perform the following steps. Otherwise, proceed to [step 13](#).
 - a If the RTC system node is locked, proceed to step [b](#). Otherwise, click **Lock** and proceed to step [b](#).
 - b If the RTC system node is off-line, proceed to step [step 13](#). Otherwise, click **Offline** and proceed to step [step 13](#).
- 13 Make note of which RTC system node is the active RTC system node. This information will be required later in the procedure.
- 14 You may want to change the alternate boot data snapshot if the system configuration stored in the boot data snapshot is considerably different from the system configuration stored in the current alternate boot data snapshot. If you do not want to update the alternate boot data snapshot, proceed to [step 15](#). If you do want to update the alternate boot data snapshot, perform [Performing a Backup Operation on page 183](#).
- 15 To perform a COR on your system, do the following:
 - a Unseat the RTC mission card for the inactive RTC system node. Ensure that the LED is off for the SCSI Disk Drive

associated with this RTC system node before unseating the mission card.

To unseat the mission card, press outward on the top and bottom latches of the mission card to release it from the CAM shelf.

Grasp the top and bottom latches of the mission card and gently pull it toward you to disconnect it from the associated TM. Do not remove the mission card from the CAM shelf.

- b** Repeat step [a](#) for the RTC mission card for the active RTC system node.
- c** Turn off both the A and B power switches on the rear of the control CAM shelf of your system.
- d** Reseat the RTC mission card for an RTC system node. To do this, gently slide the mission card back into place. Apply pressure to the faceplate until you feel resistance.

Snap the top and bottom latches of the mission card inward, toward one another. Two audible clicks can be heard when the mission card is seated properly.
- e** Repeat step [d](#) for the RTC mission card for the other RTC system node.
- f** Return power to the shelf. To do this, turn on both the A and B power switches on the rear of the control CAM shelf of your system.

Note: System start up can take several minutes, depending on the configuration of your system.

- 16** Wait for the GUI to re-establish a connection after the USP recovers. To view system node status:

- a** Click **Configuration>platform>node**.
- b** Click the **Graphical View** tab.
- c** Confirm that all system nodes are enabled (green status light).

Note 1: Nortel Networks recommends that you do not attempt any provisioning changes until all system nodes recover.

Note 2: If the GUI fails to log in when it is re-establishing the connection, the boot snapshot may not contain the current user's user-account. Provide another valid user-account that is configured in the snapshot have just booted

- 17 Log into your system.
- 18 Open the RTC system node administration tab for the RTC system node in slot 12. To do this, click **Configuration>platform>node**. Click the **Graphical view** tab, then select slot 12.
- 19 If the data snapshot descriptions match, proceed to step [20](#). If the snapshot descriptions do not match, return to step [1](#) and attempt the procedure again. If the procedure has failed twice in row, contact your next level of support.
- 20 Update the system time settings in the Set Date/Time window, click **Administration> Set Date/Time**.
Note: This step is not required if SNTP is enabled for this system.

Performing a restore operation from a backup tape



DANGER

This procedure can overwrite existing data files on your workstation. Make sure you have a current data backup before you begin this procedure.

At the OAMP workstation

- 1 Insert the tape containing the data that you want to restore.
- 2 Double-click the **Backup Exec** icon on the desktop if you are running a Veritas program or the **Colorado Backup II** icon if you are running a Colorado program.
- 3 Select **Restore files using the Restore Wizard**.
- 4 Click **OK**.
- 5 Click **Next**.
- 6 Select from media in the device.
- 7 Click **Next**. The system loads the information from the backup tape.
- 8 Select the backup date and time for the data that you want to restore.
- 9 Click **OK**. The system loads the information from the backup tape.
- 10 Click the **+** button on the tree control to expand the tree box next to the C: drive. Select any directories that you want to restore.

- 11 Click **Next**.
- 12 Click **Next** a second time.
- 13 Select **Always replace the file on my computer**.
- 14 Click **Start**. The system restores the backup data.
- 15 Click **OK**.
- 16 The data restore procedure is complete.

Restoring Multiservice Switch or Media Gateway service data

This section describes using Passport Service Data Backup and Restore to restore backed up service data from the backup site to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

The Passport Service Data Backup and Restore tools provide three types of restore:

- A *full* restore restores all backed up service data to the selected device or devices.
- An *incremental* restore restores service data based on a specified date. Like the full restore, you can perform an incremental restore on either one or multiple devices.
- A *selective* restore restores specific service data that you select. Like the full restore, you can perform a selective restore on either one or multiple devices.

Note: It is not recommended that an active file (current view) be restored on a Multiservice Switch 7400/15000 or Media Gateway 7400/15000. When you restore the current view, you may overwrite the existing current view with different content. This action will cause an outage of the Backup and Restore tool.

The following information applies to using the Passport Service Data Backup and Restore tool to perform a restore for Multiservice Switch 7400/15000 or Media Gateway 7400/15000 nodes:

- [Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the restore list](#)
- [Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the restore list](#)
- [Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device in the restore list](#)
- [Performing a full restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Performing an incremental restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Performing a selective restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data](#)

Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the restore list

Use the following procedure to add devices to the Devices List.

Procedure steps

- 1 Open the Passport Backup and Restore window. From the Preside MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore
- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select the appropriate restore mode, from the Mode column (full or incremental).
- 6 If a specific userid and password is required for the device, enter the values in the User ID and Password fields and uncheck the Use default checkbox.
- 7 If you wish to use the default userid and password, click the Use default checkbox.
- 8 Click OK.

The IP addresses for the devices are retrieved from HGDS and the device displays in the Devices list.

For devices that are not in HGDS, you are prompted for their IP address. If you are prompted for an IP address, do [step 9](#).
- 9 If you know the IP address, enter the correct IP address in the form and click OK and the device is added to the Devices list.

If the IP address is unknown or the device is not valid, press Cancel and the device is not added to the Devices list.

Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the restore list

Use this procedure to remove nodes from the list of nodes that you wish to backup.

Procedure steps

- 1 Open the Passport Backup and Restore window. From the Preside MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore

- 2 Select the Restore Configuration tab.
- 3 In the Device List, select the devices you wish to remove.
- 4 Click Remove.
- 5 In the confirmation dialog, select Yes to confirm or No to cancel the removal.

Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device in the restore list

A specific userid and password can be defined when you add the device to the restore list or you can set it later using the following procedure.

Procedure steps

- 1 Open the Passport Backup and Restore window. From the Preside MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select a device.
- 3 In the Device Details section, enter a userid and password.
- 4 Clear the Use default checkbox.

Performing a full restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to copy all the files from the repository back to the Passport.

Procedure steps

- 1 Open the Passport Backup and Restore window. From the Preside MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select a device from the Device List.
- 6 Click in the Mode title and select Full from the drop-down list.
- 7 Click Restore.

- 8 After a successful restore, you need to activate the restored data. See [Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data](#).

Performing an incremental restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to copy files, based on a specific date, from the repository back to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

Procedure steps

- 1 Open the Passport Backup and Restore window. From the Preside MDM window, select Configuration->Passport Devices->Administration->PassportService Data Backup/Restore.
- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select a device from the Device List.
- 6 Click in the Mode title and select Incremental from the drop-down list.
- 7 Define a date in the date column. (For example, July 4, 2003)
All the files, with the date and time that are not greater than the specified date, will be restored.
- 8 Click Restore.
- 9 After a successful restore, you need to activate the restored data. See [Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data](#).

Performing a selective restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to copy a specific file from the repository back to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

Procedure steps

- 1 Open the Passport Backup and Restore window. From the Preside MDM window, select Configuration->Passport Devices->Administration->PassportService Data Backup/Restore.

- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select a device from the Device List .
- 6 Click in the Mode title and select Selective from the drop-down list.
- 7 In the View column, select the desired view from the repository using the drop-down list.

Note: This step may take a few seconds to complete because the application must access the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 and list all the views names.

- 8 Click Restore.
- 9 After a successful restore, you need to activate the restored data. See [Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data](#).

Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data

Passport Restore restores the backup configuration data onto the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 disk. After a successful restore, perform the following procedure to activate the restored data.

Procedure steps

- 1 Establish a telnet session to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.
- 2 Download to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 any required application software missing from the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 disk.
- 3 Enter provisioning mode.
- 4 Activate the restored view and confirm the activation.
- 5 If required, commit the activated view.

Restoring Core Element Manager data

Application

Use this procedure to restore Core Element Manager (CEM) data.

Note: The backup procedure is performed through the Synchronous backup restore manager (SBRM). See [Synchronized Backup Manager overview on page 25](#) for details. The information needed by the Core Element Manager to restore data is located in `/opt/nortel/cem/data/coreEMS/configBackup`.

Prerequisites

You must have root user privileges to perform this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the server where the CEM resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Make sure that the `/opt/nortel/cem/data/coreEMS/configBackup` directory contains the following files:
 - `data_dir`
 - `ldapConfig.tar`
 - `nodes.tar`
 - `server`

Enter:

```
# ls /opt/nortel/data/coreEMS/configBackup
```

- 6 Make sure that CEM is not running by typing:

```
# servquery -status -group CEM
```

and pressing the Enter key.

Example response:

CEM server STOPPED

- 7 If the CEM server is running, stop the CEM server by typing:

```
# servstop CEM
```

and pressing the Enter key.

Example response:

CEM server successfully stopped

- 8 Run the restore script by typing

```
# /opt/nortel/cem/data/coreEMS/nodes/server/bin  
/postRestore.sh
```

and pressing the Enter key.

- 9 You have completed this procedure.

Performing a full restore of the software from S-tape

Purpose

Use this procedure to perform a full restore of the core manager software load from the system image backup tape (S-tape).

Prerequisites

You must be a user authorized to perform fault-admin actions.

For information on how to log in to the core manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Application

ATTENTION

You must be a trained AIX system administrator authorized to perform fault-admin actions.

ATTENTION

You must mirror all volume groups on the core manager before you perform this procedure. If you perform this procedure when disk mirroring is not at the Mirrored state, the system displays an error message.

ATTENTION

If your system includes the SuperNode Billing Application (SBA), you must use tape drive DAT0 to perform this procedure.

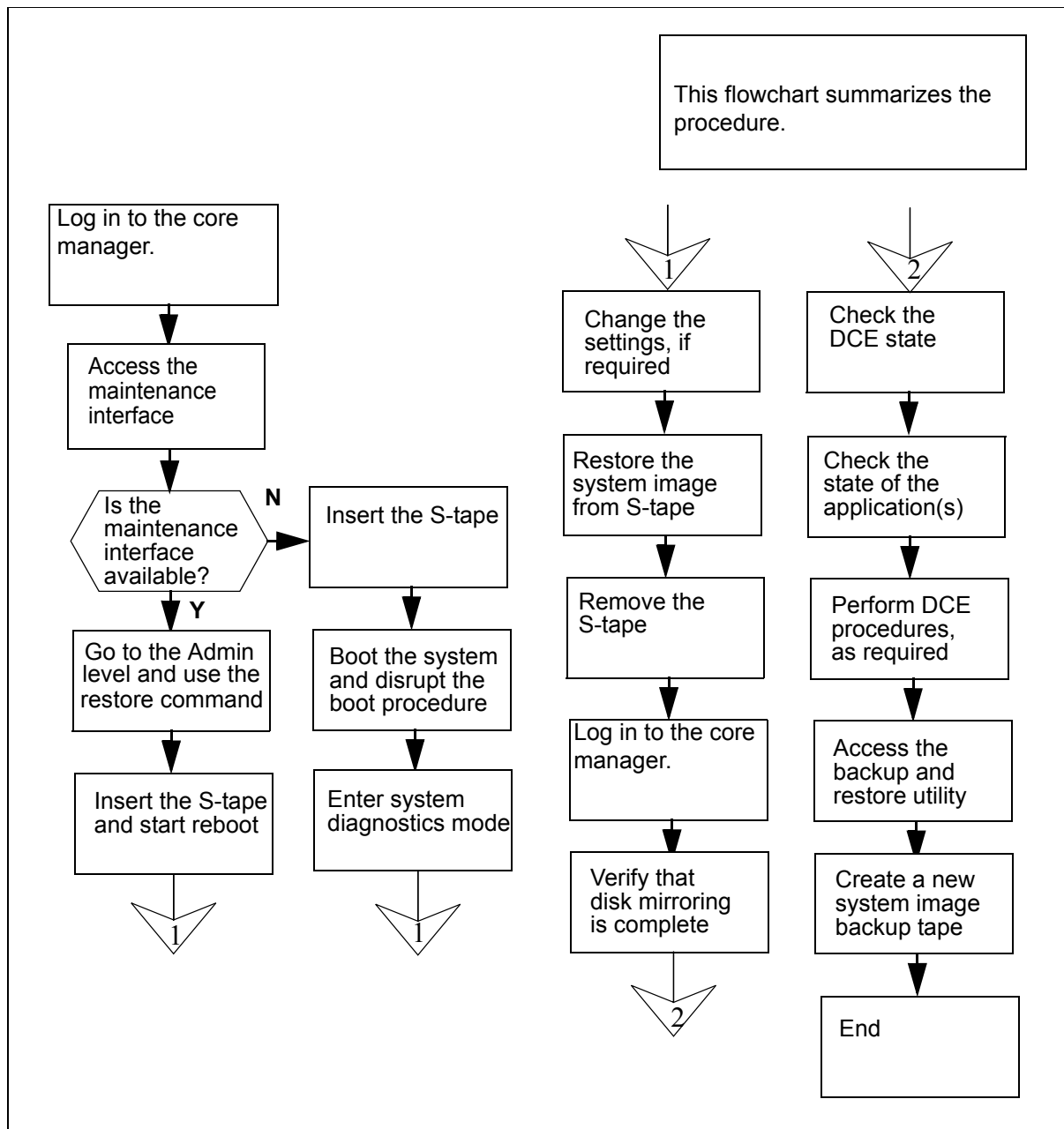
Interval

Perform this procedure when the core manager is out-of-service due to a corrupted software load.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the recovery tasks.

Summary of performing a full restore of the software from the S-tape



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Performing a full restore of the software from S-tape

At the local VT100 console

- 1 Log into the CS 2000 Core Manager as a user authorized to perform fault-admin actions.

- 2 Access the maintenance interface:

sdmmtc

- 3 Determine if the core manager maintenance interface is available.

If	Do
core manager maintenance interface is available	step 4
core manager maintenance interface is not available	step 10

- 4 Access the administration (Admin) level:

admin

- 5 Perform a full restore of the core manager:

restore

Example response:

Select the tape drive you want to restore from,
or type Abort to abort:

Enter 0 for the tape drive in the main chassis
slot 2.

Enter 1 for the tape drive in the main chassis
slot 3.

- 6 Choose the tape drive to use.

If	Do
you want to use the tape drive in slot 2	enter 0
you want to use the tape drive in slot 13	enter 1

- 7 When prompted, confirm that you want to proceed:

y

Example response:

Insert the backup-tape into the tape drive in the main chassis slot 2. When completed press [Enter] to start the restore.

- 8 Insert the back-up tape (S-tape) into the tape drive you specified (slot 2 or 13).

Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

- 9 Press the Enter key to start the restore process, and proceed to [step 17](#).

Note: When you press the Enter key, the system starts the restore procedure by rebooting the core manager from the selected tape drive.

At the core manager

- 10 Ensure that one of the core manager tape drives (slot 2 or 13 in the main chassis) contains the system image backup tape (S-tape).

Note: Use tape drive DAT0 (option for performing a full restore from an S-tape) if your system also includes SBA.

At the Modular Supervisory Panel

- 11 Reboot the core manager. If the prompt is available at a local VT100 console, reboot the core manager:

shutdown -Fr

If the prompt is not available, reboot the core manager by turning the power off, then on, using the MSP breaker that supplies power to the core manager.

At the local VT100 console

- 12 When the system displays “COLD Start”, press the Break key or the Esc key twice to interrupt the boot process. The system takes about 4 minutes to initialize.
- 13 Continue depending on the prompt displayed on the monitor.

If the prompt is	Do
FX-Bug	step 16
FX-Bug and you are in a menu	step 14
FX-Diag	step 15

- 14** From the selection menu, select Go to System Debugger:

3

Go to [step 16](#).

- 15** Switch the directory to FX-Bug:

sd

- 16** View the input/output devices on the core manager to verify the address of the tape drive from the FX-Bug prompt. Enter:

Fx-Bug> ioi

Example response:

CLUN	DLUN	CNTRL-TYPE	DADDR	DTYPE	RM	Inquiry-Data
1	0	IO	0	\$00	N	SEAGATE
ST11200N ST						
3	0	IO	0	\$00	N	31200 0660 SEAGATE
ST12400N						
ST32430						
1	50	IO	5	\$01	Y	0660 ARCHIVE
Python						
28388-XXX						
5.45	6	0	IO	0	\$00	N
ST11200N						
ST31230						
0660	8	0	IO	0	\$00	N
ST12400N						
ST32430						
0660	6	50	IO	5	\$01	Y
Python						
28388-XXX						
5.45						

Note: In the example response, the tape drive is ARCHIVE.

- 17** If you receive the FX-Bug prompt, then continue with this step. Otherwise, go to [step 19](#).

Fx-Bug> pboot <address_for_Archive_Python>

In the example, the following are valid choices:

- pboot 1 50 if the tape drive is located in slot 2
- pboot 6 50 if the tape drive is located in slot 13

- 18** Wait about 4 minutes until the system completes the reboot.
- 19** The system prompts you to define the console setting and the language setting. Define the console setting by selecting option 1 and pressing the Enter key.

Note 1: In case of any failures, contact your next level of support.

Note 2: When you define the console setting, the system does not echo the entry "1" on the screen.

- 20** Enter 1 to select the language setting, and press the Enter key. The Welcome to Base Operating System Installation and Maintenance menu is then displayed.
- 21** Select "Change/Show Installation Settings and Install":

2

The system displays the System Backup Installation and Settings menu.

Example response:

```
System Backup Installation and Settings
```

```
Either type 0 and press Enter to install with
the current settings, or type the number of the
setting you want to change and press Enter.
```

```
Setting:                                Current
Choice(s):
1 Disk(s) where you want to install    hdisk0...
    Use Maps                            No
2 Shrink File System                    No
```

```
>>> 0 Install with the settings listed above.
```

Note: The string "..." shown under Current Choice(s) indicates that more than one disk is currently in use.

- 22** The default disk for the installation is hdisk0 which is located in slot 2 of the main chassis. If your core manager contains one disk drive in each domain of the main chassis, accept the default setting. If you have additional disk drives, you may wish to change the settings.

If	Do
you want to change the current settings	step 23

If	Do
you want to use the current settings	step 27

23 Change the disks where you want to install the backup image:

1

The system displays the Change Disk(s) Where You Want to Install menu.

Example response:

```
Change Disk(s) Where You Want to
Install
```

Type one or more numbers for the disk(s) to be used for installation and press Enter. To cancel a choice, type the corresponding number and Press Enter. At least one bootable disk must be selected. The current choice is indicated by >>>.

```

      Name      Location Code Size(MB) VGStatus
Bootable Maps
>>>1 hdisk0 c1-f2-00-0,0 4056      rootvg
    Yes      No
>>>2 hdisk5 c1-f13-00-0,0 4056
    rootvg    Yes      No
    3 hdisk1 c1-f4-00-0,0 4056      other
vg Yes      No
    4 hdisk2 c1-f4-00-1,0 4056      other vg
Yes      No
    5 hdisk3 c2-f1-00-0    02043      other vg
Yes      No
```

This menu displays the list of all available disks on which you can install the system backup image. The currently selected disks are indicated by >>> symbols.

Note: The system backup must be installed on one disk in each domain to achieve fault-tolerant operation. Valid choices in the example in [step 23](#) are hdisk0 and hdisk5. The rootvg disks for installation must have location codes

- c1-f2-00-0 for domain 0, and
- c1-f13-00-0 for domain 1.

- 24 To select a disk or disks, enter the number of the disk, and press the Enter key.
- 25 To deselect a selected disk, enter its number again and press the Enter key.
- 26 When you have finished entering the settings, the System Backup Installation and Settings menu is displayed. Enter
0
and return to [step 22](#).

- 27 Accept the current settings:

0

This begins the restore process and lasts at least 30 min. During the restore process, the monitor displays the approximate percentage of the tasks completed, and the elapsed time.

Note 1: If an error message appears at the end of the restore process, datavg did not import successfully. Contact the next level of support.

Note 2: You must manually re-boot the system if you are performing this procedure as part of the “Removing an I/O expansion chassis (NTRX50EC)” procedure in the Upgrades document. In this scenario, go to [step 28](#).

Note 3: As part of the restore process, the system reboots automatically and displays the login prompt. Continue with [step 29](#).

- 28 At the FX-bug prompt, manually boot the system:

```
FX-bug> pboot 1 0
```

At the core manager

- 29 Remove the S-tape from the tape drive when the reboot is completed, and store it in a secure location.

At the local or remote terminal

- 30 Log in to the core manager as a user authorized to perform fault-admin actions. Press the Enter key when you see the “TERM=(vt100)” prompt.

- 31 Start the core manager maintenance interface:

```
sdmmtc
```

32 Access the storage level:**> storage***Example response:*

volume Groups	Status	Free (MB)
rootvg	Mirrored	2032
datavg	Mirrored	11712

Logical Volume	Location	Size (MB)	% full/
threshold 1 /	rootvg		88
11/80			
2 /usr	rootvg	600	29/90
3 /var	rootvg	200	5/70
4 /tmp	rootvg	24	5/90
5 /home	rootvg	304	5/70
6 /sdm	rootvg	504	24/90
7 /data	datavg	208	7/ 80

Logical volumes showing: 1 to 7 or 7

33 Determine the mirror status of the disks.

If the disks are	Do
Mirrored	step 35
Integrating or Not Mirrored	step 34

34 You cannot continue this procedure until disk mirroring is Mirrored. If necessary, contact the personnel responsible for your next level of support. When disk mirroring is at the Mirrored state, continue this procedure.**35** Access the LAN level:**lan****36** Check the state of DCE.*Example response:*

DCE State: SysB

37 Access the application (APPL) level to check the state of any DCE-based applications:**appl**

and pressing the Enter key.

Example response:

#	Application	State
1	Table Access Service	.
2	Log Delivery Service	.
3	OM Access Service	.
4	Secure File Transfer	Fail
5	Enhanced Terminal Access	Fail
6	Exception Reporting Fail	

Applications showing 1 to 6 of 6

38**ATTENTION**

DCE and DCE-based applications can fail if the key tab files restored from tape contain obsolete keys.

If the DCE state is displayed as SysB at the LAN menu level of the RMI ([step 35](#)), and the logs displayed indicate an error with the security client service in DCE, restore the service by performing the following procedures in the CS 2000 Core Manager Configuration Management document:

- “Removing a CS 2000 Core Manager from a DCE cell”
- “Configuring a CS 2000 Core Manager in a DCE cell”

- 39** If some DCE-based applications are faulty (Fail state, see [step 37](#)), try to restore them by busying (BSY) and returning to service (RTS) the applications from the SDM APPL level (see [step 37](#)).
- 40** If this approach fails, restore them by performing the procedure to add the application server to the DCE cell in the CS 2000 Core Manager Configuration Management document.
- 41** Reset passwords for users SDM01-04 on the core and SDM. Refer to procedure [Resetting SDM user passwords for DDMS on page 289](#).
- 42** You must create a new system image backup tape. Refer to the procedure “Creating system image backup tapes (S-Tapes)” in the CS 2000 Core Manager Security and Administration document.
- 43** You have completed this procedure.

Resetting SDM user passwords for DDMS

Application

Use this procedure to reset the passwords for users SDM01-04 when both of the following conditions have occurred:

- the DDMS applications, OSS Comms Svcs and OSS and Application Svcs, remain in in-service trouble (ISTb) after busying and returning the DDMS applications to service
- the QUSER command from the core does not show users SDM01-04

Resetting the passwords for users SDM01-04 consists of

- [Resetting the passwords on the CM on page 289](#)
- [Changing passwords in the DDMS configuration file on page 290](#)

Prerequisites

To complete this procedure you need the following:

- access to the core
- root-user access to the CS 2000 Core Manager
- passwords for users SDM01-04

Action

Complete all the steps that follow to reset the password for users SDM01-04.

Resetting the passwords on the CM

At the CI prompt on the switch

1 Enter each of the following commands:

```
> unpermit sdm01
> unpermit sdm02
> unpermit sdm03
> unpermit sdm04
```

- 2 Enter each of the following commands:

```
> permit sdm01 <sdm01_pswd> 4 10000 english all  
> permit sdm02 <sdm02_pswd> 4 10000 english all  
> permit sdm03 <sdm03_pswd> 4 10000 english all  
> permit sdm04 <sdm04_pswd> 4 10000 english all
```

Where

<sdm0n_pswd>

is the password for user SDM0n

Note 1: If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

Note 2: If Enhanced Password Control is in effect on the CM, and any of the SDM01-SDM04 passwords are changed on the CM, you need to apply the same password changes in the DDMS configuration file. Refer to [Changing passwords in the DDMS configuration file](#).

- 3 You have completed this procedure. Proceed to [Changing passwords in the DDMS configuration file on page 290](#).

Changing passwords in the DDMS configuration file

At the CS 2000 Core Manager

- 1 Log in to the CS 2000 Core Manager as the root user.
- 2 Access the application level of the maintenance interface by typing

```
# sdmmtc appl
```

and pressing the Enter key.
- 3 Locate and busy OSS Comms Svcs by typing

```
> bsy <n>
```

and pressing the Enter key.
<n>
is the number next to the OSS Comms Svcs fileset
- 4 Locate and busy OSS and application Svcs by typing

```
> bsy <n>
```

and pressing the Enter key.
<n>
is the number next to the OSS and application Svcs fileset

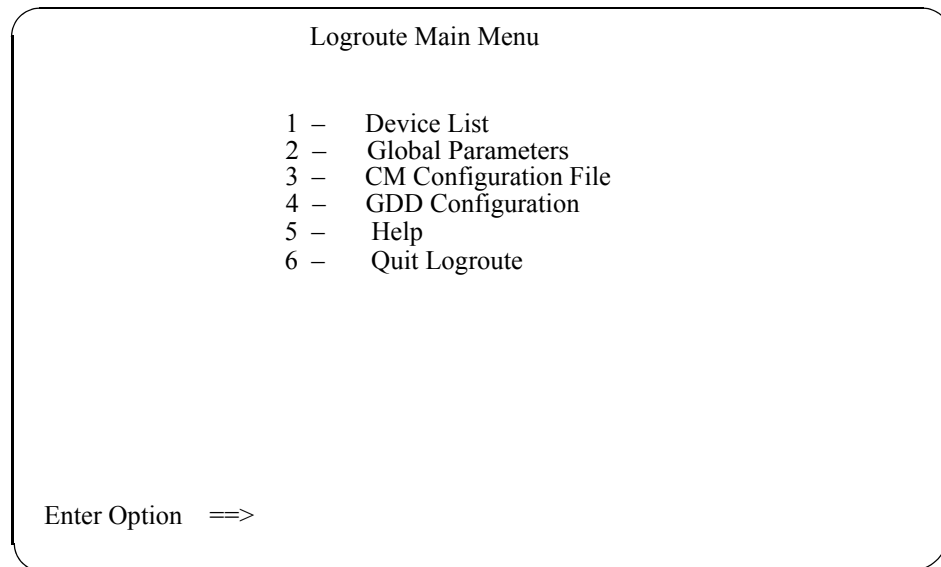
- 5 Exit the application level by typing
`> quit all`
 and pressing the Enter key.
- 6 Access the configuration level of the maintenance interface by typing
`# sdmmtc config`
 and pressing the Enter key.
- 7 Access the OSS Comms Svcs configuration level by typing
`> config <n>`
 and pressing the Enter key.
`<n>`
 is the number next to the OSS Comms Svcs fileset
- 8 Press Enter to begin configuration.
- 9 When prompted to enter the logroute tool, as shown in table [DDMS logroute tool banner](#), press Enter.

DDMS logroute tool banner

```
#####
# Adding DDMS logroute configuration
#####
Please add DDMS log routing:
    Device type      = file
    File             = /data/logs/ossaps/ossapslog
    Routing          = addrep
    log_type         = DDMS
Press <RETURN> when ready
```

The Logroute Main Menu appears, as shown in figure [Logroute tool main menu](#).

Logroute tool main menu



Logroute Main Menu

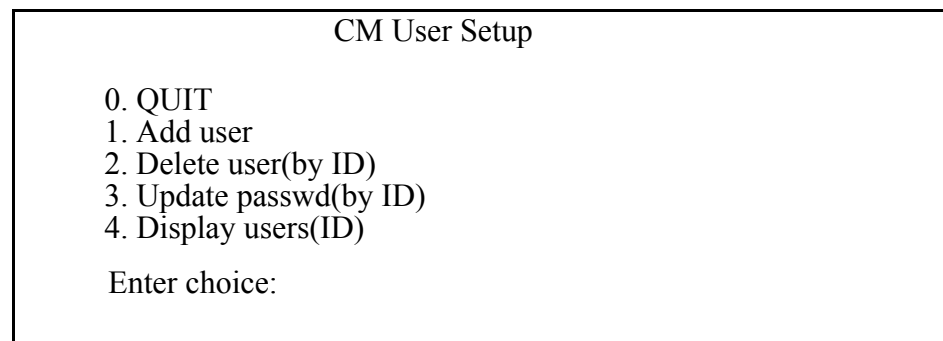
- 1 - Device List
- 2 - Global Parameters
- 3 - CM Configuration File
- 4 - GDD Configuration
- 5 - Help
- 6 - Quit Logroute

Enter Option ==>

- 10** Enter the number next to Quit Logroute.

The CM User Setup screen is displayed as shown in the example that follows.

Example of DDMS CM User Setup screen



CM User Setup

- 0. QUIT
- 1. Add user
- 2. Delete user(by ID)
- 3. Update passwd(by ID)
- 4. Display users(ID)

Enter choice:

- 11** Enter the number next to Display users(ID).
- 12** Note the user ID next to SDM01-04.
- 13** Enter the number next to Update passwd(by ID).
- 14** Enter the user ID (not user name) for SDM01.
- 15** Enter new password for SDM01.

The passwords for SDM0n must be the same as that entered in [Resetting the passwords on the CM on page 289](#).

Note: The userIDs and passwords are not case sensitive.

- 16 Repeat step 15 for SDM02, SDM03, and SDM04, then proceed to step 17.
- 17 Enter the number next to QUIT in the CM User Setup screen.
- 18 Exit all levels of the maintenance interface by typing
`> quit all`
and pressing the Enter key.
- 19 Access the application level of the maintenance interface by typing
`# sdmmtc appl`
and pressing the Enter key.
- 20 Locate and return OSS Comms Svcs to service by typing
`> rts <n>`
and pressing the Enter key.
`<n>`
is the number next to the OSS Comms Svcs fileset
- 21 Locate and return OSS and application Svcs to service by typing
`> rts <n>`
and pressing the Enter key.
`<n>`
is the number next to the OSS and application Svcs fileset
- 22 Exit all levels of the maintenance interface by typing
`> quit all`
and pressing the Enter key.
You have completed this procedure.

Performing a partial restore of the software from S-tape

Purpose

Use this procedure to restore individual files or sets of files from the system image backup tape (S-tape).

Prerequisites

You must be a user authorized to perform fault-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration



CAUTION

Possible loss of data

Use this procedure at the discretion of the system administrator.

Perform a partial restore only if you are familiar with the files, and know exactly which files are to be restored. If you restore the wrong files, you may inadvertently corrupt core manager software.

ATTENTION

This procedure must be performed by a trained AIX system administrator authorized to perform fault-admin actions.

ATTENTION

All volume groups on the core manager must be fully mirrored (Mirrored) before performing this procedure. If you attempt to perform this procedure when disk mirroring is not Mirrored, an error message is displayed on the screen.

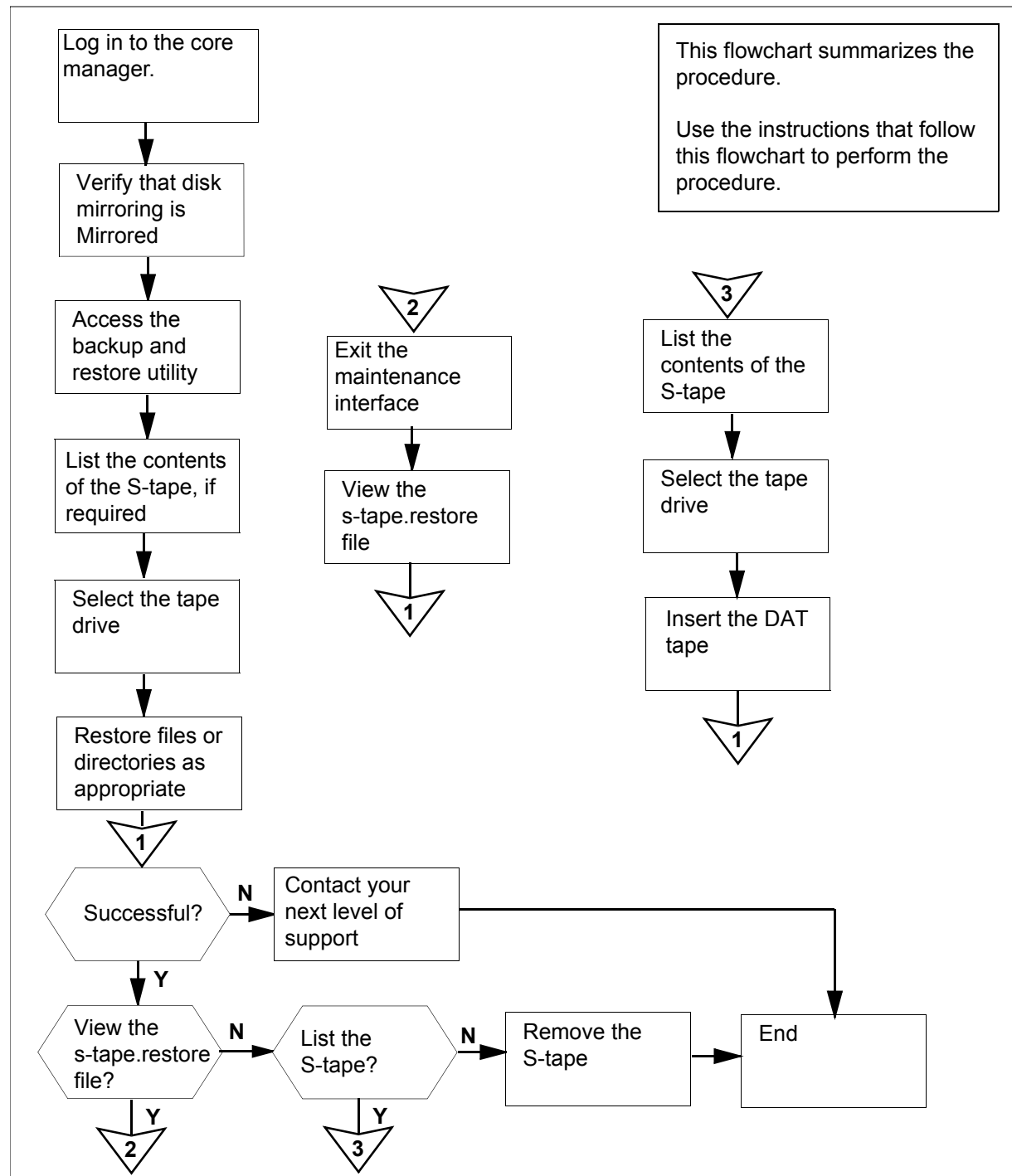
ATTENTION

If your system includes the SuperNode Billing Application (SBA), use tape drive DAT0 to perform this procedure.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the recovery tasks.

Summary of Partial restore from the system image tape (S-tape)



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Partial restore from the system image tape (S-tape)

At the local or remote console

- 1 Log into the core manager as the user authorized to perform fault-admin actions.

- 2 Access the maintenance interface:

sdmmtc

- 3 Access the storage level:

storage

Example response:

Volume Groups (MB)	Status	Free
rootvg	Mirrored	2032
datavg	Mirrored	11712

Logical Volume Size (MB)	%full/threshold	Location	1 /	
		rootvg	88	11/80
2 /usr	29/90	rootvg	600	
3 /var	5/70	rootvg	200	
4 /tmp	5/90	rootvg	24	
5 /home	5/70	rootvg	304	
6 /sdm	24/90	rootvg	504	
7 /data	7/80	datavg	208	

Logical volumes showing: 1

to 7 of 7

- 4 Determine the Mirror status of the disks.

If the disks are	Do
Mirrored	step 6
not Mirrored	step 5

5

**CAUTION****Possible loss of data**

You cannot perform this procedure until disk mirroring of all volume groups is Mirrored.

If necessary, contact the personnel responsible for your next level of support. When disk mirroring is Mirrored, continue this procedure.

6 Access the administration (Admin) menu level of the RMI:

admin

7 Access the System Image Backup and Restore Menu:

backup

Note 1: If disk mirroring for all volume groups is not Mirrored, the system displays an error message. The system then prompts you to return to the System Image Backup and Restore menu.

Note 2: If another person attempts to use the backup and restore utility when it is in use, an error message is displayed on the screen.

Example response:

```
Currently there is a backup running on bnode73.
Please execute yours later.
Exiting...
```

8 Determine the contents of the tape.

If you	Do
wish to list the S-tape	step 9
do not wish to list the S-tape	step 17

9 From the System Image Backup and Restore Menu, select “List Contents of the System Image Tape (S-tape)”:

3

- 10** After you select option 3, you are prompted to select the tape drive.

Example response:

Select a tape drive you wish to use:

```
Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
( 0, 1 or 2 ) ==>
```

Note: Use tape drive DAT0 (option 1) if your system also includes SBA.

- 11** Enter the number for the tape drive you want to use (1 or 2), and press the Enter key.

Note: If your system includes SBA, and you still wish to use DAT1 (option 2), the following message is displayed:

Response:

You have selected DAT 1. This is the default DAT drive for the Billing application, and may currently be in use for the emergency storage of billing records.

If you continue to use DAT 1, make sure that the correct tape is in the drive, and that billing records will not be lost during the backup restore operation.

Do you wish to continue with DAT 1? (y | n)

- if you wish to continue using DAT1, enter y
- if you do not wish to use DAT1, enter n

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

- 12** After you select the tape drive, the system prompts you to insert the S-tape into the appropriate tape drive.

Example response:

```
Please insert your System Image Backup tape
(S-tape) into the tape drive DAT0 and allow at
least 5 minutes to complete the listing.
```

```
A log file will be saved in /tmp/s-tape.toc.
```

```
Are you ready to proceed? ( y | n )
```

At the core manager

- 13** Insert the S-tape into the tape drive you selected.

Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

At the local or remote VT100 console

- 14** When you are ready to continue this procedure, enter:

y

The contents of the S-tape are listed on the screen. When the listing is complete, the system prompts you to return to the System Image Backup and Restore Menu.

Example response:

```
Would you like to return to the previous menu?
( y | n )
```

- 15** Return to the System Image Backup and Restore Menu:

y

- 16** Determine if the file or directory has been restored.

If you are listing the contents of the tape to verify

Do

that the file has been restored [step 25](#)

the file name or directory that you wish to restore [step 17](#)

- 17** From the System Image Backup and Restore Menu, select "Restore Files from the System Image Tape (S-tape)":

4

- 18** After you select option 4, you are prompted to select the tape drive.

Example response:

Select a tape drive you wish to use:

```
Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
( 0, 1 or 2 ) ==>
```

Note: Use tape drive DAT0 (option 1) if your system also includes SBA.

- 19** Enter the number for the tape drive you want to use (1 or 2).

Note: If your system includes SBA, and you still wish to use tape drive DAT1 (option 2), the following message is displayed:

Example response:

You have selected DAT 1. This is the default DAT drive for the Billing application, and may currently be in use for the emergency storage of billing records.

If you continue to use DAT 1, make sure that the correct tape is in the drive, and that billing records will not be lost during the backup/restore operation.

Do you wish to continue with DAT 1? (y | n)

- if you wish to continue using DAT1, enter y
- If you do not wish to use DAT1, enter n

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

- 20** After you select the tape drive, you are prompted to insert the S-tape into the appropriate tape drive. A warning is displayed advising that this procedure must only be completed by qualified core manager system administrators. The warning also advises that files and directories must be entered exactly as they appear in the file listing. Insert the S-tape in the appropriate tape drive.

Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

Example response:

Are you ready to enter the name of the file or directory? (y | n)

- 21** Continue this procedure:

y

Example response:

Enter the name of the directory or file that you wish to restore as
./<your-full-path>/<your-file-or-directory>.

Note: Tape processing may take a few minutes to complete. A log file /tmp/s-tape.restore will be created.
==>

- 22** Enter the full path name of the directory or file that you wish to restore, exactly as shown in the file listing, including "/" at the beginning.

Note 1: A log file /tmp/s-tape.restore is created when the restore is completed.

Note 2: An error message is displayed if the restore is unsuccessful. If this occurs, go to [step 25](#).

- 23** During the restore process, the screen does not display any additional information. When the file restore is complete, the file you have restored is displayed. The system then prompts you to return to the System Image Backup and Restore Menu.

Example response:

Would you like to return to the previous menu?
(y | n)

Note: If the restore has failed, an error message is displayed before the prompt, advising you to list the contents of the tape, and perform the procedure again.

- 24** Return to the System Image Backup and Restore Menu:

y

- 25** Determine if the restore was successful. The system displays the file that you have restored, as described in [step 23](#). You may

also wish to view the s-tape.restore file or list the files on the S-tape.

If	Do
the restore is successful	step 32
the restore failed	contact your next level of support
you wish to view the s-tape.restore file	step 26
you wish to list the S-tape	step 9

26 Exit the System Image Backup and Restore Menu:

0

27 Exit the maintenance interface:

`quit all`

28 Access the s-tape.restore file:

`cd /tmp`

29 Scroll through the file:

`more s-tape.restore`

30 Continue pressing the Enter key until the files that you have restored, and the date of the restore, are displayed.

31 Determine if the restore was successful.

If	Do
successful	step 33
failed	contact your next level of support

32 Exit the System Image Backup and Restore Menu:

0

Note: If you then wish to exit the maintenance interface, type quit all and press the Enter key.

At the core manager

33 Remove the S-tape and store it in a secure place.

34 You have completed this procedure.

Recovering backup files from lost backup volumes

Application

You need to recover backup files from lost backup volumes if the SBA becomes unaware of backed up files when the SWACT and RESTART processes occur when you are configuring backup volumes.

The following procedure swaps back old volumes as the primary backup volumes.

Prerequisites

Before starting the procedure, you need

- the names of the swapped out volumes
- to have configured backup volumes, following the procedure found in NTP NN10126-811 for the CS 2000 Core Manager or NN10363-811 for the Core and Billing Manager, at which point, the SBA completed its recovery of the volumes from the backup volumes you configured during these procedures.

Action

Recovering backup files from lost backup volumes

At the MAP

- 1 Post the billing stream by typing

```
> mapci;mtc;appl;sdbil;post <x>
```

and pressing the Enter key.
Where
<x> is the name of the billing stream.
- 2 Quit back to the appl;sdbil level by typing

```
> quit
```

and pressing the Enter key.

- 3 Confirm that the names of the billing stream's existing backup volumes are the swapped in volumes you created earlier by typing

```
> conf view <x>
```

and pressing the Enter key.

Where

<x> is the name of the billing stream.

Note: SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

- 4 Reference the notes you made when you configured the backup volumes, to confirm that the backup volumes are those that you created during these procedures.
- 5 Refer to the following table to determine your next step.

If the backup volume names are	Do
the names you setup when you configured the backup volumes	continue with step 6
not the names you setup when you configured the backup volumes	determine if someone else re-configured the backup volumes before you continue with step 6

- 6 Configure the billing stream of the logical volumes you created, once you receive confirmation that the files are successfully created by typing

```
> conf set <x> <y> <z>
```

and pressing the Enter key.

Where

<x> is the name of the stream, <y> is the dms_backup_1 volume, and <z> is the dms_backup_2 volume.

Note: SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

- 7 Quit back to the command prompt by typing

```
> quit all
```

and pressing the Enter key.

Note 1: The non-empty backup volumes are automatically detected by the SBA audits. In addition, the SBA places the billing stream into recovery mode and the volumes from the original backup volumes are sent to the CS 2000 Core ManagerCBM.

Note 2: You must alert all operating company personnel who are associated with the DMS switch as to the names of the old and new backup volumes and the procedure you used to swap the volumes. These same personnel must be made aware of that any RESTARTs or SWACTs that occur before the billing stream returns to normal mode can cause a serious loss of billing records.

- 8 You have completed this procedure.

Restoring the oracle data on an SSPFS-based server

Application

Use this procedure to restore the oracle data from a backup tape, CD or DVD on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240). Also use this procedure to restore the data that was automatically backed up to a file on the server by the backup restore manager.

The server can be hosting one or more of the following components:

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

Note: Restoring the oracle data is not applicable to the CBM as it does not use an oracle database.

Prerequisites

This procedure requires the oracle data backup tape, CD or DVD. If the data was saved through the backup restore manager, the name of the file located in directory “/data/bkresmgr/backup” is required.

Action

Use the following table to determine how to start this procedure.

If	Start at
restoring from tape, CD or DVD	step 1
restoring from a file	step 2

At the server

- 1 Insert the tape, CD, or DVD containing the oracle data backup into the drive and proceed to [step 2](#).

At your workstation

- 2 Log in to the server by typing

```
> telnet <server>
```

 and pressing the Enter key.
 where
 server
 is the IP address or host name of the SSPFS-based server on which you are performing the data restore
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing

```
$ su - root
```

 and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Verify the permissions on the restore log directory (bkslog) by typing

```
# ls -alrt /var/opt/nortel
```

 and pressing the Enter key.

Example response

```
total 22
lrwxrwxrwx  1 root  succssn      28 Dec 22  2003 gwc
-> /net/47.141.126.131//swd/gwc
drwxrwxr-x  4 root   other        512 Dec 22  2003 .
drwxr-xr-x  7 root   sys          512 Sep 10 12:41 ..
drwxr-xr-x  2 oracle oinstall    512 Dec  8 15:58 db
```

```
drwxrwxrwt  2 root  other  6656 Dec 15 19:56 bkslog
```

**If the permissions of
bkslog**

Do

are drwxrwxrwt

[step 8](#)

are not drwxrwxrwt

[step 7](#)

- 7 Change the permissions of bkslog by typing

```
# chmod 777 /var/opt/nortel/bkslog
```
- 8 Determine if server applications have been stopped by typing

```
# servquery -status all
```
- 9 If not already done, stop any running server applications on the server.

For

Refer to

CS 2000 Management Tools
server applications

[Stopping the SESM server
application](#)

[Stopping the SAM21
Manager server application](#)

[Stopping the NPM server
application](#)

*ATM/IP Security and
Administration,
NN10402-600*

MG 9000 Manager and
mid-tier server applications

*the MG9000 Security and
Administration,
NN10162-611*

Integrated EMS server
application

*IEMS Security and
Administration,
NN10336-611*

- 10 Use the following table to determine your next step.

If

Do

restoring from tape, CD or
DVD

substep [a](#)

restoring from a file

substep [b](#)

- a Restore the database from backup tape, CD or DVD by typing

```
$ /opt/nortel/sspfs/bks/rsdata
```

and pressing the Enter key.

Proceed to [step 11](#).

- b** Restore the database from the backup file by typing

```
$ /opt/nortel/sspfs/bks/rsdata -f  
/data/bkresmgr/backup/<filename>
```

and pressing the Enter key.

where

filename

is the name of the backup file created by the backup restore manager

Proceed to [step 12](#).

- 11** Remove the tape from the drive, or eject the CD or DVD from the drive as follows:

- a** Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- b** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

Note: If the DVD drive tray does not open (if not busy or being read from or written to), then enter the following commands:

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

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

Press the eject button located on the front of the DVD drive.

- c** Remove the CD or DVD from the drive.

12 Verify that the database restored properly by typing**# queryAllFaults**

If an alarm appears like the following, the database was not restored properly:

```
*** SPFS330 Import of Oracle data caused
corruption ORA-22337: Error importing Oracle
data
cs2kaps=rtp6backupseem;NODE=rtp6backupseem;CLA
SS=SW;SWTYPE=Database Fri Jun 10 15:48:59 2005
```

Use the information in the following table to determine the next step.

If	Do
no alarm appears	step 13
the database did not restore properly	contact Nortel

13 Start the server applications that run on the server.

For	Refer to
CS 2000 Management Tools server applications	Starting the SESM server application Starting the SAM21 Manager server application Starting the NPM server application <i>ATM/IP Security and Administration,</i> NN10402-600
MG 9000 Manager and mid-tier server applications	<i>the MG9000 Security and Administration,</i> NN10162-611
Integrated EMS server application	<i>IEMS Security and Administration,</i> NN10336-611

Note: If one or more applications do not start, contact Nortel for assistance.

You have completed this procedure.

Performing a full system restore on an SPFS-based server

Application

Use this procedure to perform a full system restore from backup media on a Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240).

A full system restore consists of reverting to the previous release of SPFS, restoring the file systems, and restoring the oracle data.

The server can be hosting one or more of the following components:

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

Note: Restoring the oracle data does not apply to the CBM as it does not use an oracle database.

ATTENTION

System logs indicating application and database errors generate until the file systems and oracle data are restored on the system using this procedure and procedure [Restoring the oracle data on an SSPFS-based server on page 307](#). No database errors generate on the CBM as it does not use an oracle database.

Prerequisites

To complete this procedure you need

- the SPFS Installation CD disk#1 for the release you are reverting to
- the tape or DVD on which you backed up the file systems
- the tape or DVD on which you backed up the oracle data

Action

Use one of the methods below according to your office configuration.

- [Simplex configuration \(one server\) on page 314](#)
- [High-availability configuration \(two servers\) on page 316](#)

Note: Only the [Simplex configuration \(one server\)](#) uses a full system restore from tape on a Sun Netra t1400 server.

Simplex configuration (one server)

At the server console

- 1 Log in to the server through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing
`# init 0`
and pressing the Enter key.
- 3 Insert SPFS Installation CD disk#1 into the drive.
- 4 Use the following table to determine your next step.

If restoring from	Do
tape	step 5
DVD	step 6

- 5 Insert the tape with the backed up file systems into the drive.
- 6 At the OK prompt, restore the system by typing
`OK boot cdrom - restore`
and pressing the Enter key.
- 7 When prompted, accept the software license restrictions by typing
`ok`
and pressing the Enter key.
The system reboots.

Note: If the restore process fails at this point due to one or more disks not being labeled, which is reported as “Bad Magic Number in Disk Label”, refer to procedure “Labelling disks on an SSPFS-based server” in *ATM/IP Fault Management*, NN10408-900 to label the disks.

If restoring from DVD, you will be prompted to insert Volume 1 of the backup DVD into the drive. Insert the DVD on which you backed up the file systems. During the restore process, the system will prompt you for additional Volumes if more than one DVD was used during the backup of file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

Note: Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

8 Eject the backup DVD from the drive as follows:

a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

Note: If the DVD drive tray does not open (if not busy or being read from or written to), enter the following commands:

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

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

Then, press the eject button located on the front of the DVD drive.

c Remove the backup DVD from the drive.

9 Use the following table to determine your next step.

If	Do
this SPFS-based server is hosting the CBM	step 13
otherwise	step 10

- 10** List the oracle groups by typing

```
# groups oracle
```

and pressing the Enter key.

If the output is	Do
oinstall data dba or oinstall dbs data	step 11
oinstall dba data	step 12

- 11** Correct the oracle groups by typing

```
# usermod -g oinstall -G data,dba oracle
```

and pressing the Enter key.

- 12** Restore the oracle data using procedure [Restoring the oracle data on an SSPFS-based server on page 307](#). Once the data restore is complete, continue to [step 13](#).

- 13** Reboot the server by typing

```
# init 6
```

and pressing the Enter key.

You have completed this procedure.

High-availability configuration (two servers)

At the console connected to the inactive node

- 1** Log in to the inactive node through the console (port A) using the root user ID and password.

- 2** Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

At the console connected to the active node

- 3** Log in to the active node through the console (port A) using the root user ID and password.

- 4** Access the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

- 5** Insert SPFS Installation CD disk#1 into the drive.

- 6 At the OK prompt, restore the system by typing
`OK boot cdrom - restore`
and pressing the Enter key.
- 7 When prompted, accept the software license restrictions by typing
`ok`
and press the Enter key.
The system reboots.
Note: If the restore process fails at this point due to one or more disks not being labeled, refer to procedure “Labelling disks on an SSPFS-based server” in *ATM/IP Fault Management*, NN10408-900 to label the disks.
- 8 When prompted, insert Volume 1 of the DVD on which you backed up the file systems, into the drive.
Note: During the restore process, the system will prompt you for additional Volumes if more than one DVD was used during the backup of file systems.
The restore process can take several hours to complete depending on the number and size of the files that are being restored.
Note: Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.
- 9 Eject the backup DVD from the drive as follows:
 - a Ensure you are at the root directory level by typing
`# cd /`
and pressing the Enter key.
 - b Eject the CD by typing
`# eject cdrom`
and pressing the Enter key.
Note: If the DVD drive tray does not open (if not busy or being read from or written to), enter the following commands:
`# /etc/init.d/volmgt stop`
`# /etc/init.d/volmgt start`

Then, press the eject button located on the front of the DVD drive.

- c** Remove the backup DVD from the drive.

- 10** Use the following table to determine your next step.

If	Do
this SPFS-based server is hosting the CBM	step 14
otherwise	step 11

- 11** List the oracle groups by typing
groups oracle
 and pressing the Enter key.

If the output is	Do
oinstall data dba or oinstall dba data	step 12
oinstall dba data	step 13

- 12** Correct the oracle groups by typing
usermod -g oinstall -G data,dba oracle
 and pressing the Enter key.

- 13** Restore the data using procedure [Restoring the oracle data on an SSPFS-based server on page 307](#). Once the data restore is complete, execute [step 14](#) and [step 15](#).

- 14** Reboot the server by typing
init 6
 and pressing the Enter key.

- 15** Re-image the inactive node using the active node's image. If required, refer to procedure [Cloning the image of one node in a cluster to the other node](#).

You have completed this procedure.

Restoring the central security server

Use this procedure to restore the security server from a backup file.

ATTENTION

SSL uses certificates. Certificates from one server cannot be used on another server. If you want to take a backup file from a server where SSL is implemented and restore to a different server, you must perform the procedure “Replacing HTTPS certificate on security server for SunOne component” in *ATM/IP Solution-level Security and Administration*, NN10402-600 after the restore is completed. This script is run to set up IS authentication, session and policy traffic to operate under SSL.

Note that servers in the same high availability cluster can use the same SSL certificate.

Note that if the restored IS SSL certificate has expired, you must perform the procedure in “Replacing HTTPS certificate on security server for SunOne component” in *ATM/IP Solution-level Security and Administration*, NN10402-600 after the restore is completed.

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- you must have a backup tar file created using the procedure for [Backing up the central security server](#)

Action

Perform the following steps to restore central security server data.

At your workstation

- 1 Telnet to the server by typing
 > **telnet <server>**
 and pressing the Enter key.
 where
 server
 is the IP address or host name of the server
- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing:
`$ su - root`
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Stop the security services by doing the following:
 - a Type:
`servstop RADSVR`
and press the Enter key.
 - b Type:
`servstop IS`
and press the Enter key.
 - c Type:
`servstop WEBSERVICES`
and press the Enter key.
- 6 Change directories by typing:
`cd
/opt/nortel/applications/security/current_slis
ext/swmgmt/bin`
and pressing the Enter key.
- 7 Perform the restore operation by typing:
`./brr_security.sh -restore /data/bkresmgr/
<date><time>backupSS1.1<host_name>.tar`
where <date><time>backupSS1.1<host_name>.tar is the backup file from which you are restoring.
Press the Enter key.
- 8 Restart the security services by doing the following:
 - a Type:
`servstart WEBSERVICES`
and press the Enter key.
 - b Type:
`servstart IS`
and press the Enter key.

c Type:

servstart RADSVR

and press the Enter key.

- 9** If the restored image was backed up from a different server with a different certificate or if the restored certificate has expired, follow the procedure in “Replacing HTTPS certificate on security server for SunOne component” in *ATM/IP Solution-level Security and Administration*, NN10402-600 to replace the invalid or expired certificate on the Integrated EMS Server.

- 10** Select your next step.

If you are restoring a server	Do
in a simplex configuration	you have completed this procedure
in a high-availability configuration	go to the next step

- 11** Clone the active server to the inactive server. For details, see “Cloning the image of one node in a cluster to the other node” in *ATM/IP Solution-level Security and Administration*, NN10402-600.

- 12** You have completed this procedure.

Component Security

Overview

Security and administration options vary between Succession components and their managers as described below.

Communication Server 2000 Core Manager

The Communication Server 2000 Core Manager provides security for the CS 2000 Core. Core-managed peripherals including the MG 4000, the IW SPM, and the CS 2000 Core are managed from the CM Privclass interface.

The CS 2000 Core Manager is the Nortel Networks operations, administration, and maintenance (OA&M) processing complex for the CS 2000 core. The CS 2000 Core Manager is an applications environment that allows operating companies to operate, administer, maintain and provision network components and services.

The CS 2000 Core Manager primarily uses Telnet/FTP and SSHlogin/SFTP (simple file transfer protocol) for secure file transfer with the CS 2000 Core.

Optionally, distributed computing environment (DCE) secure servers and Passwerks are available for secure file transfer with the CS 2000 Core. CS 2000 Core Manager provides passthrough only.

Media Gateway, Multiservice Switch and Preside MDM

Preside MDM, Multiservice Switch 15000, Media Gateway 7400/15000, and CS 2000 Communication Server LAN (Passport 8600) provide their own security. Preside MDM provides passthrough security only. Preside MDM allows users to manage security for Media Gateway 7400/15000.

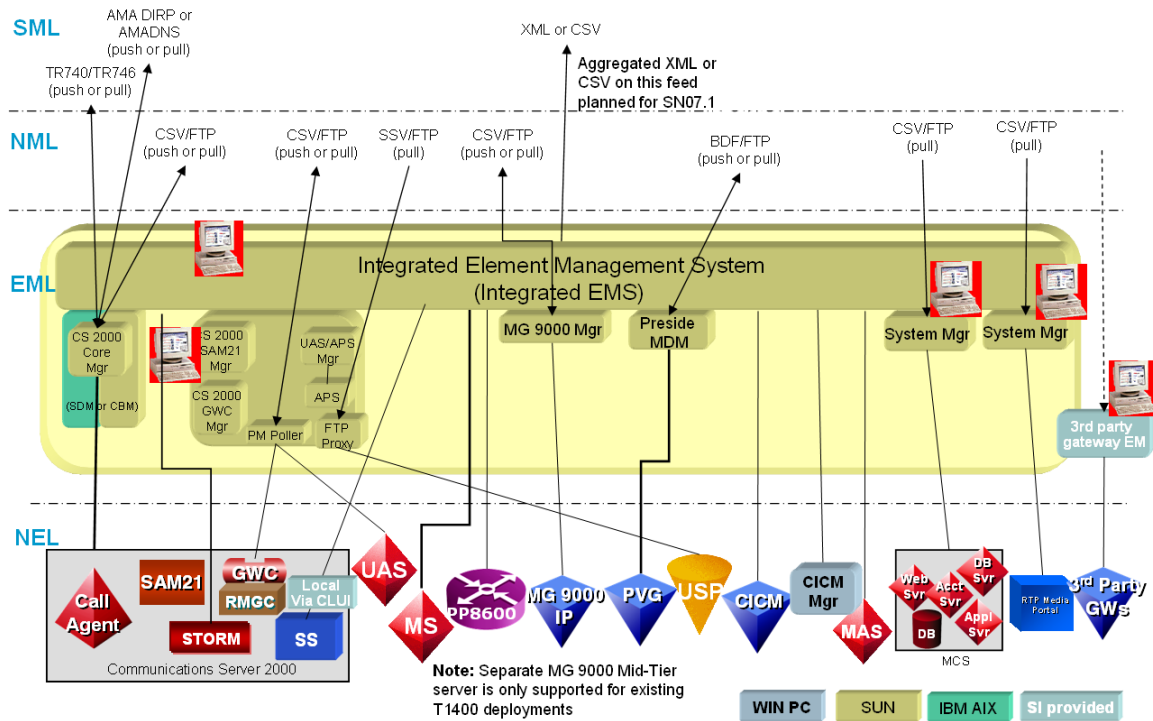
Succession Server Platform Foundation Software

The Succession Server Platform Foundation Software (SSPFS) provides PAM-based user authentication and group-based user authorization for the management of the CS 2000 Management Tools applications, the MG 9000 Manager, Network Patch Manager, and USP Manager.

- PAM-based user authentication supports different authentication technologies without changing login services. For details about PAM, refer to [PAM-based user authentication on page 341](#).
- Group-based authorization controls which operations a user is authorized to perform.

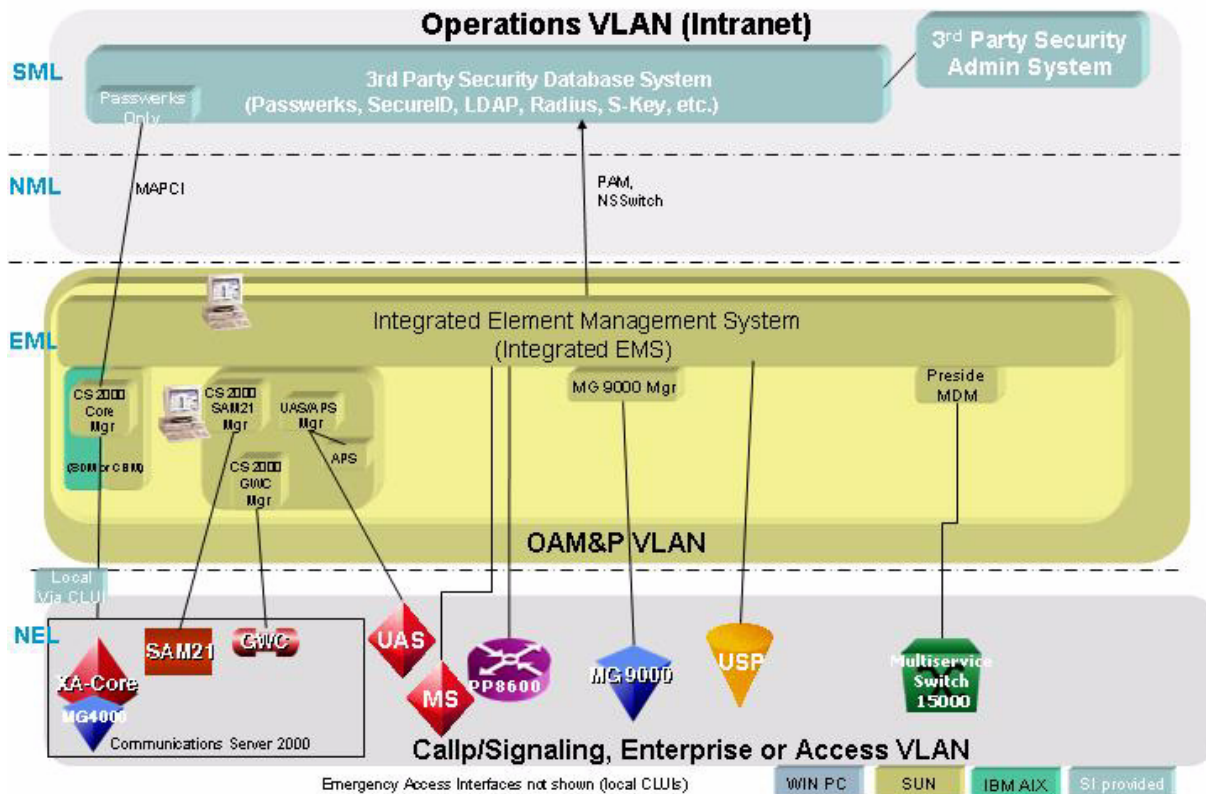
The following figure illustrates the security operations architecture for CS 2000 Server - Compact.

Security architecture for the CS 2000 Server - Compact (IP solutions)



The following figure illustrates the security operations architecture for CS 2000 Server (UA-AAL1).

Security architecture for the CS 2000 Server (UA-AAL1)



Technical Publications

For detailed information about Succession Network Security and Administration, see the following Nortel Networks technical publications (NTPs):

Nortel Networks Network Security and System Administration technical publications

NTP serial number	Title
None	Please consult the Succession Network engineering guidelines documents for your solution. Contact your Nortel Networks account manager for details.
NN10159-611	<i>USP Security and Administration</i>
NN10160-611	<i>USPc (compact) Security and Administration</i>
NN10161-611	<i>Universal Audio Server Security and Administration</i>
NN10162-611	<i>MG 9000 Security and Administration</i>
NN10163-611	<i>Spectrum Peripheral Module Security and Administration</i>
NN10164-611	<i>MG 4000 Security and Administration</i>
NN10165-611	<i>Interworking Spectrum Peripheral Module (ATM) Security and Administration</i>
NN10166-611	<i>Interworking Spectrum Peripheral Module (IP) Security and Administration</i>
NN10167-611	<i>Dynamic Packet Trunking Spectrum Peripheral Module (IP) Security and Administration</i>
NN10168-611	<i>Dynamic Packet Trunking Spectrum Peripheral Module (ATM) Security and Administration</i>
NN10170-611	<i>CS 2000 Core Manager Security and Administration</i>
NN10171-611	<i>Communication Server 2000 Security and Administration</i>
NN10174-611	<i>Succession Communication Server 3000 Security and Administration</i>
NN10175-611	<i>Call Agent Security and Administration</i>
NN10176-611	<i>STORM Security and Administration</i>

Nortel Networks Network Security and System Administration technical publications

NTP serial number	Title
NN10177-611	<i>SAM21 Shelf Controller Security and Administration</i>
NN10213-611	<i>Gateway Controller Security and Administration</i>
NN10252-611	<i>CICM Security and Administration</i>
NN10180-611	<i>Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP</i>
NN10275-909	<i>Succession Fault Management Logs Reference</i>
NN10337-611	<i>MS 2000 Series Security and Administration</i>
NN10346-611	<i>Session Server Security and Administration</i>
NN10336-611	<i>Integrated EMS Security and Administration</i>
NN10367-111	<i>RTP Media Portal Basics</i>

Network Security

Succession network security uses Succession Communication Server LAN (CS LAN) and subnet (VLAN) and firewalls to provide protection at the network level, component level, and management application level. The CS LAN must be a closed network and all access must be secure and controlled.

This section provides a brief overview of CS LAN and subnet and firewall protection.

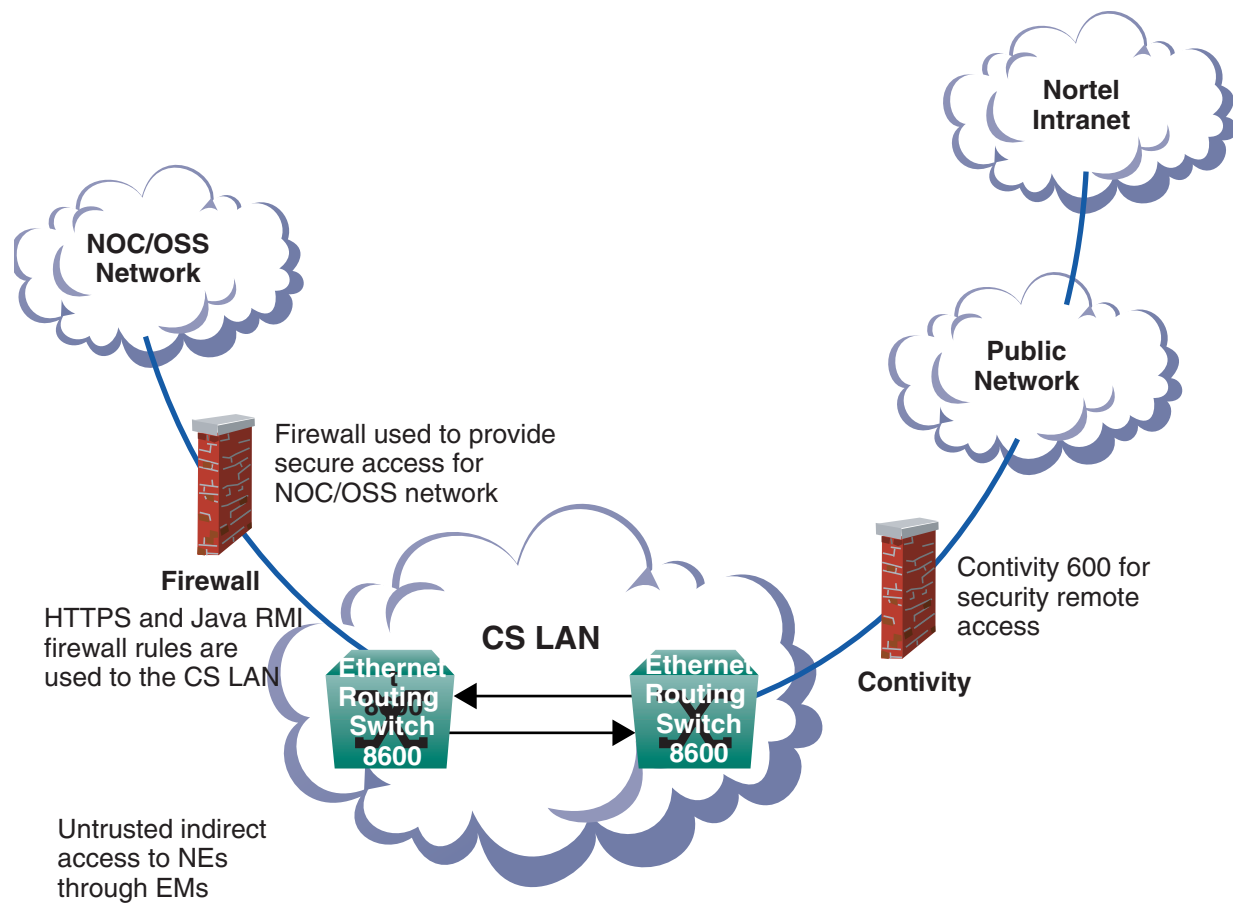
For details, please refer to the following:

- Nortel Networks engineering guidelines for your solution
- [Technical Publications on page 327](#)

CS LAN and Subnets (VLANs)

The following figure provides an overview of how firewalls and VPN technology provide secure access to the CS LAN for Network Operations Center (NOC) and Operations Support System (OSS) connectivity and remote field support.

Secure access to the CS LAN



The Communication Server LAN (CS LAN) provides this connectivity as required for those components that are co-located with the CS 2000 complex.

Different message flows are separated into the following subnets (or VLANs) on the CS LAN redundant routers:

- CallP - for Call Processing (or Call Signaling) traffic flows
- Bearer - for RTP bearer traffic flows
- MLT - intra-Ethernet Routing Switch 8600 traffic flows
- SP-OAM - Service Provider OAM traffic flows (optional)

- OAM - for OAM&P traffic flows
- OOB - Out of Band OAM traffic flows

The components that are configured in the Call Processing subnet are:

- XA-Core and/or CS 2000 compact
- CS 2000 SAM21 (GWC and SC)
- SDM Call Processing interface
- SAM16 (UAS) Call Processing interface
- USP Call Processing interface
- USP-Compact
- MG4000 out-of-band management interface (for UA-AAL1 only)

The components that are configured in the OAM&P messaging subnet are:

- CS 2000 Management Tools
- SDM Management interfaces
- USP Management interfaces
- USP Manager
- Nortel MDM server
- MG 9000 Server (for UA-AAL1 only)
- MG 9000 Mid Tier (for UA-AAL1 only)
- Integrated Element Management System

The components that are configured in the Bearer subnet are as follows:

- UAS
- Media gateways
- IW-SPM
- MG 9000 (UA-AAL1 only)

Domain Name Service in the OAM system

Succession OAM has required DNS since (i)SN05. DNS resolution must be enabled on the Sun server to allow the security certificates to work, and must be enabled prior to the installation of the certificate. Refer to the procedure for Configuring Domain Name Service in ATM/IP Solution-level Configuration Management, NN10276-500 for more

information. The following element management servers and their clients use the DNS Service for the HTTPS protocol.

- CS 2000 Management components
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager (MG 9000 Manager)
- Integrated Element Management System (Integrated EMS)

In addition, Integrated EMS uses the DNS Service for client launching. Integrated EMS utilizes HTTPS proxy on SSPFS for launching some components.

Firewalls

Firewalls can be deployed as an optional security feature at the CS-LAN or Trunk Gateway sites. However, it is recommended to evaluate carefully the amount of traffic that might traverse a firewall, especially when Media Gateways are present in the location to be protected. This is because the most common firewalls have a Gigabit Ethernet as the highest capacity interface. Unfortunately, the throughput drop is on the order of 50-60 per cent, which can seriously impair performance and traffic engineering. Therefore, unless adequate firewall capacity is proven, it is strongly suggested not to rely on firewalls to protect bearer traffic but use instead traffic filtering on routers.

On the other hand, given the fairly small signaling traffic flows, the Call Processing subnet can be protected by a firewall without significant performance drops. The same can be said for the OAM&P subnet, where, depending on the network topology, a firewall is recommended given the sensitivity of the platforms.

The clients of the CS 2000 Management Tools and CS 2000 MG 9000 Manager are able to communicate with their respective server components through multiple firewalls (facing either the client or the server side) using a minimum number of configurable TCP/IP ports. In addition to allowing communication through the firewall, this functionality also ensures that the data is secure.

For details about firewall port configuration, please refer to the Nortel Networks engineering guidelines for your solution and the Succession networks component customer documentation listed in [Technical Publications on page 327](#).

HTTPS for GUI and HTML-based tools

HTTPS is used for Java GUI launching and HTML-based tools in all Succession solutions to secure otherwise unsecure messaging.

In a TCP connection to be secured via SSL, for example, an HTTPS interface, the server side of the connection must have an SSL certificate installed. Before operational communication can start, the certificate presented is validated by the SSL client. If the certificate is validated by the SSL client, further SSL handshake takes place to generate cryptographic keys used to secure the subsequent message exchanges between client and server. Note that standard SSL protocol also supports SSL client authentication. However, SSL client authorization is not used in Nortel Networks Succession applications.

Note: To use HTTPS messaging, customers must have an X.509 certificate installed on the web server. If this is not already installed, refer to [Installing or replacing an HTTPS certificate on an SSPFS-based server](#) in this document.

Domain Naming Service

A Domain Name Server (DNS) serves two independent functions in the CS LAN. The DNS functions are provided by a standard DNS server to be provided by the customer. There are two DNS functions:

- the first OAM DNS function is required in (I)SN07 in an OAM&P system. See [DNS in an OAM&P system](#).

Note: The workaround to deploying DNS is to modify the etc/host files for each of the client machines that access the Carrier VoIP OAM servers using fully qualified domain names (FQDN) which resolve those names in the client machines. However, to use this workaround, you need to configure each client machine and modify each client machine when network changes occur.

- the second DNS function is needed only in a small line gateway deployment, and is optional. See [DNS in a small line gateway application](#).

DNS in an OAM&P system

The DNS service is used in two ways for the OAM system.

- Firstly, DNS is used to secure client /server interaction using the HTTPS protocol. HTTPS is activated by the installation of a security certificate on the Sun server. The browser uses the certificate to authenticate the server and encrypt the connection in both directions between the client desktop browsers and the element management (EM) servers. This protects passwords and user information used within the system. This DNS service is customer provided and can be located in the OAM&P/NOC LAN.
- Secondly, an internal Nortel Networks usage in the CO-LAN is used by the Integrated EMS. The Integrated EMS uses the DNS service for data encryption.

DNS is required by HTTPS in Carrier VoIP OAM. The client desktop browser asks the EM server for the security certificate. The browser must determine if the security certificate is valid and not supplied from an untrusted source. To determine validity of the security certificate the browser will match the Fully Qualified Domain Name (FQDN) of the server hostname in the certificate with the trusted list located in the DNS service. This is done through a DNS lookup. If the DNS lookup works, then the browser continues to validate the rest of the certificate information. It checks with the Certificate Authority (CA) to see if the certificate is valid or not.

If DNS is not provided in the Carrier VoIP OAM and the EM servers are not added as valid entries in a customer's DNS server, the browser will get a failed look up on the FQDN in the certificate. If this fails, the rest of the certificate is not validated, and no HTTPS connection is established to the server.

Carrier VoIP OAM has optionally supported DNS since (I)SN05, but is required in (I)SN07 as secure client access becomes the only supported configuration. DNS resolution must be enabled on the Sun server to allow the security certificates to work, and must be enabled prior to the installation of the certificate. For wireline, refer to the procedure for Configuring Domain Name Service in ATM/IP Solution-level Configuration Management, NN10276-500 for more information. For wireless, refer to the procedure Configuring Domain Name Service in Packet MSC Configuration, NN20000-213. The following EM servers and their clients use the DNS Service for the HTTPS protocol.

- CS 2000 Management components
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager (MG 9000 Manager)
- USP Manager GUI
- Integrated Element Management System (Integrated EMS)

Note: In addition, Integrated EMS uses the DNS Service for Integrated EMS Server to Integrated EMS Client data encryption via Secure Socket Layer (SSL).

- Access to the following clients via HTTPS access proxy:
 - STORM from (I)SN06.2
 - CICM from (I)SN07
 - Session Server from (I)SN07

Note: A maximum of only five DNS entries is needed for each CO (CS 2000 Logical Call Server) to match the IP address to the FQDN.

OAM DNS service configuration

Each of the EM servers defined in an office must be added. This includes all of the virtual IP address and hostnames, along with the physical IP addresses and hostnames.

Each of the clients that access any of the Carrier VoIP servers need to reference the DNS server that has been configured with the EM server entries.

The OAM&P servers must be added to the customer's intranet DNS servers prior to installing security certificates. It is recommended that the certificates are installed at the end of the OAM&P installation process and prior to the upgrade of an existing system.

Types of certificate

There are three types of security certificates that can be used.

- a certificate granted from a well known certificate granting authority (CA)
- company generated: used when the operating company has its own internal CA
- self signed: created locally on the server

These certificates differ in the level of trust that needs to be assigned to a server. This is based on how the server is used.

- If the server is used in a public way, such as for e-commerce websites, then a certificate from a CA is required.
- If the server is used internally within a company, then the company generated certificate can also be used.
- If the server is used in a more restricted manner, then a self-signed certificate can also be used to protect the client to server communications. However, when the server is accessed, the browser presents the certificate and asks whether the certificate can be trusted. If the user answers "yes", the server can be accessed. If the user answers "no", nothing further will be received from the server.

Note: A certificate obtained from a CA must include a PEM header and must not have a password.

DNS in a small line gateway application

The second DNS application is optional and is needed only in a small line gateway deployment, whereas the OAM DNS must be shared across COs and OSSs and across client workstations and remote access. This use of DNS in a small line gateway allows for a more streamlined provisioning of small line gateways by associating the MAC-FQDN for the small line gateway with the gateway IP address, allowing the gateway's IP address in GWC Manager to be set to 0.0.0.0. You can also use DNS when the Redirecting Media Gateway Controller (RMGC) is used for the IAW or IAC solutions to provide ease of engineering GWs across GWCs.

For security reasons, it is not recommended or supported for the DNS for the small lines gateway applications to be the same as the OAM DNS. Protocols and services should not be shared between the subscriber access and the OAM operations sections of the networks. The OAM DNS must be shared across COs, the operator's internal operations LAN, and OSSs.

Redundant DNS servers

The DNS deployment model recommends that more than one DNS server is deployed in the event that a DNS server is down. It is also recommended that the redundant DNS servers have the identical information configured on each. Standard DNS products and standard DNS deployment policies and capabilities support both of these recommendations. The DNS servers need to be accessible from the LANs where the client desktop computers are connected. The DNS servers may also be connected to the rest of the DNS network in the customer's internal network. The customer must define the domain assigned to each office and the hostnames that are given to the servers in the office.

Group-based User Authorization

This section provides overview information about Succession security domains and user groups and references to documentation containing user logs.

SSPFS Security User Groups

A number of new Succession Secure Platform Foundation Software (SSPFS) security domains and user groups are now available. The domains and user groups a user is assigned to control which operations the user is authorized to perform.

The SSPFS user group domains and their target systems are as follows:

- **ln.** This includes line services, line cards, v5.2 services, and small line gateways (port level).
- **trk.** This includes trunks, trunk-based services, v5.2 services, small trunking gateways (port level), carrier, and carrier-based services.
- **mg.** This includes small and large gateways, including UAS, CICM, and Media Gateway.
- **mgc.** This includes CS 3000, CS 2000, USP, GWC, CS 2000 SAM21, MCS 5200, 3PC, and Storm.
- **ems.** This includes SSPFS-based managers, SDM, MDM, MDP, KDC, and others.

The following table maps the available Succession roles and user groups.

Succession User Group Definitions map

Role	Domain				
	Line	Trunk	Media Gateway	MGC	EMS/EML
Administration (adm)	Inadm	trkadm	mgadm	mgcadm	emsadm
Read/Write (rw)	Inrw	trkrw	mgrw	mgcrw	emsrw
Read Only (ro)	Inro	trkro	mgro	mgcro	emsro
Subscriber Provisioning (sprov)	Insprov	trksprov	mgsprov	mgcsprov	emssprov
Maintenance (mtc)	Inmtc	trkmtc	mgmtc	mgcmtc	emsmtc

With group-based authorization, users are created and associated with different groups based on the operations they perform.

Administration of security accounts is not permitted from the client side.

Only users with permissions to login to the Succession Communication Server 2000 Management Tools and who belong to the user group *succssn* on the server can perform security administration activities.

For details about managing user accounts, refer to your Succession networks component documentation.

For details about assigning users to secondary user groups, see [Setting up local user accounts on an SSPFS-based server](#).

Reference Information

For security logs, please refer to the following documents:

NTP number	Document
NN10170-611	<i>CS 2000 Core Manager Security and Administration</i>
NN10180-611	<i>Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP</i>
NN10275-909	<i>Succession Fault Management Logs Reference (multi-volumes)</i>

PAM-based user authentication

Overview

Carrier VoIP network components use the pluggable authentication module (PAM) framework to support different authentication technologies without changing login services. PAM preserves existing system environments while supporting security services such as login, rlogin, and telnet.

PAM can be used to integrate login services with different authentication technologies, such as RSA, DCE, Kerberos, S/Key, and smart card based authentication systems. Thus, PAM enables networked applications to operate in different customer environments which utilize different security mechanisms.

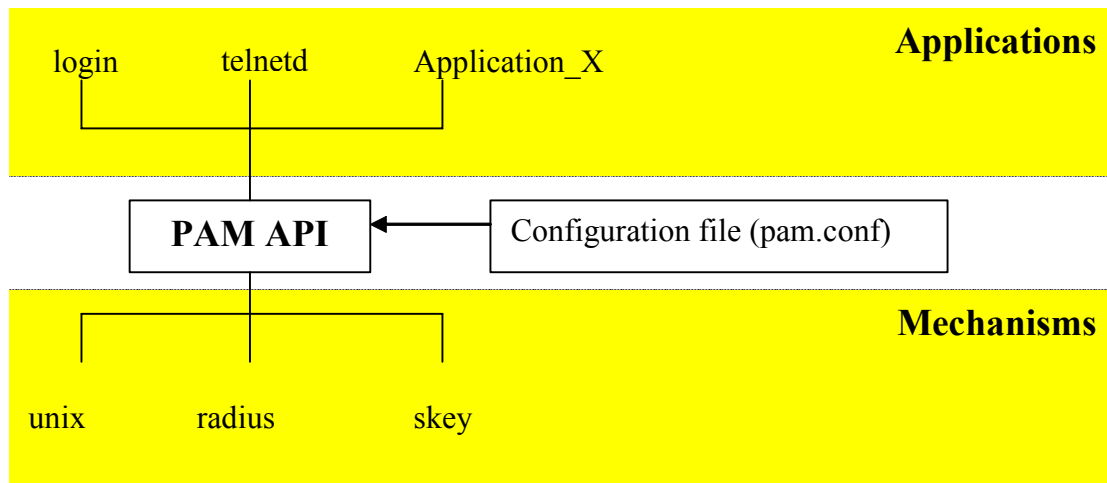
Carrier VoIP solutions' use of PAM provides unified user login interfaces for the following client applications:

- Audio Provisioning Server (APS) Manager
- CS 2000 Management Tools
- Network Patch Manager (NPM)
- Line Maintenance Manager (LMM)
- Trunk Maintenance Manager (TMM)
- CS 2000 SAM21 Manager
- Batch Configuration Monitor
- MG 9000 Manager
- Integrated EMS
- CICM Manager
- USP and USP Manager

PAM addresses the following user access requirements for the Succession Element and Sub-Element Manager (SESM) and the Succession Server Platform Foundation Software (SSPFS) platform:

- Authentication – verify user identity. Set the user credentials like user ID and group ID.
- Password control – manage password aging, changes, and control password strength.

- Account control – check if the user account is active according to expiration date, time-of-day, method or origin of access.
- Session management – Open and close sessions. Log information about the current session.



PAM features

PAM functionality includes the following:

- Provides an abstraction layer so that applications can use numerous security services via PAM modules.
- Has a common API for applications, independent of the operating system, so that applications are not tied to specific security services.
- Has a common SPI (Service Provider Interface) for interfacing to security services.
- The system administrator, not the application, decides on the user authentication mechanism on a per application basis. Thus, changes in the security policy have no impact on the applications.
- For CMT applications the user can be authenticated once with all authentication protocols without retyping the password (excludes Trunk Maintenance Manager (TMM), Batch Provisioning Tool, and MG 9000 Manager)
- Provides a unified login in the presence of different mechanisms. Otherwise, the user often is expected to know about the authentication command of the new authentication module (for example, **kinit**, **dce_login**) after logging into the system, which is not user-friendly.

System Administration Advantages

PAM provides system administrators with the flexibility to do the following:

- Choose any authentication service available on a system to perform end-user authentication for an application.
- Manage user accounts centrally.
- Add new authentication service modules to a system and make them available without having to modify any applications.
- Incorporate mapping services to map user names and authentication tokens between different authentication domains.

CICM element manager integration with PAM+ proxy

Overview

Carrier VoIP user authentication services can use a single centralized third party server which provides authentication services to Carrier VoIP management systems via a pluggable authentication module (PAM) on the Integrated EMS platform.

From (I)SN07 onwards, the CICM element manager is integrated into the Carrier VoIP centralized user authentication strategy. The CICM element manager interfaces to PAM via the HTTPS PAM+ proxy on Integrated EMS.

Prior to (I)SN07, the user name and password supplied when logging into the element manager corresponded to local user accounts on the CICM element manager. For (I)SN07, the user name and password can be configured to be a global Carrier VoIP account managed on a centralized authentication database which interfaces to Carrier VoIP management tools via the PAM+ proxy located on the Integrated EMS.

Centralized user authentication via the SSPFS PAM proxy is not available to TDM deployments of CICM or if connectivity is lost between the CICM element manager and the SSPFS platform.

- For TDM deployments, the authentication functionality passes control of the authentication back to the standard mechanism used for CICM.
- For Carrier VoIP deployments, a method of local user authentication is also provided for use when connectivity is lost to the Integrated EMS platform. Users can select local authentication by prefixing their user name with a period (.). This allows users to access their local user account in the CICM element manager when the PAM proxy is out of service.

For more information on CICM integration with PAM+ proxy, see *CICM Configuration Management*, NN10240-511.

Security Tools and Utilities

This section lists Carrier VoIP network management components and available security applications.

Login Security

Management Component	Login Security
APS GUI	PAM
Contivity 600	Local database
CS 2000 Core Manager	Local database
CS 2000 Management Components (CS2M)	
• APS Manager	PAM
• CS 2000 SAM21 Manager	PAM
• GWC Manager	PAM
• Lines/Trunks/Nodes Provisioning	PAM
• LMM GUI	PAM
• Lines Configuration (Servord+)	PAM
• NPM	PAM
• TMM GUI	PAM
• UAS Manager	PAM
• MS 2000 Series Configuration Tool	PAM
• MG 9000 Manager	PAM
CS 2000 Management Tools Platform Access	
• Telnet	PAM
• FTP Server	SSH PAM FTP does not use PAM directly, but if a user is not found in the ProFTP user database, it authenticates the user with PAM.

Login Security

Management Component	Login Security
Media Gateway 7480	Local database
Media Gateway 15000	Local database
Ethernet Routing Switch 8600 Device Manager	Local database
- Device Manager: Local database - Platform access: RADIUS or local database	
MDM	PAM
Integrated EMS	PAM
USP Manager	
• USP Manager GUI	PAM
• Citrix	Local database
XA Core Manager (SDM platform)	
• FTP Server	Local database
• SFTP	Local database
• SBA	Local database
• ETA/ATA	DCE
• SFT01	DCE
• SFT2 (SSH-based)	Local database

Centralized security administration overview

Integrated EMS provides centralized administration, authentication, authorization, and security logging for most components in the solution.

Integrated EMS provides a pluggable security architecture based on the Pluggable Authentication Module (PAM) and Name Services Switch (NSS).

This architecture provides the following features:

- central administration of user accounts and user groups
- central authentication. Authentication of centrally administered user accounts is performed by the central security server.
- central authorization. Authorization information needed to support user access control is securely managed and provided by the central security server.
- single sign-on (SSO). This capability enables the user to access multiple network elements, applications, and features from a single login session. Session information for a user is shared between Integrated EMS and networks elements which support SSO.
- the ability to plug in a third-party authentication or authorization solution
- the ability to generate centralized security logging for successful and failed authentications

The following table lists the devices and applications that support central security administration features.

Note: To configure a device to use centralized security, refer to the documents listed in the following table. You should configure a device to use central security, only after the Integrated EMS central security server has been configured and activated in the network.

Central security administration - supported devices

Network element/EMS platform	Device authentication and authorization method	Documentation reference
USP	HTTPS	<i>USP Security and Administration</i> , NN10159-611
Passport 8600 (now known as Ethernet Routing Switch 8600)	RADIUS	<i>Configuring and Managing Security</i> , 314724-B
SSPFS CS 2000 Management Tools Audio Provisioning Server (APS) Network Patch Manager (NPM) MG 9000 Manager MG9000 Mid-Tier	PAM_RADIUS and NSS_SAML	<i>ATM/IP Solution-level Security and Administration</i> , NN10402-600
Integrated EMS	HTTPS	<i>Integrated EMS Security and Administration</i> , NN10336-611
CICM Manager	HTTPS	<i>CICM Configuration Management</i> , NN10240-511
Multiservice Data Manager (toolset)	PAM_RADIUS NSS_SAML	<i>Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Succession VoIP Networks Security and Administration - Securing Network Elements</i> , NN10180-612

Central security administration - supported devices

Network element/EMS platform	Device authentication and authorization method	Documentation reference
Multiservice Data Manager (Operator Client)	SAML over HTTPS	<i>Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Succession VoIP Networks Security and Administration - Securing Network Elements, NN10180-612</i>
Passport PVG 7480 (now known as Media Gateway 7480)	RADIUS	<i>Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Succession VoIP Networks Security and Administration - Securing Network Elements, NN10180-612</i>
Passport PVG 15000 (now known as Media Gateway 15000)	RADIUS	<i>Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Succession VoIP Networks Security and Administration - Securing Network Elements, NN10180-612</i>
Multiservice Switch 15000	RADIUS	<i>Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Succession VoIP Networks Security and Administration - Securing Network Elements, NN10180-612</i>
GWC	HTTP	No device-specific configuration needed

Central security administration - supported devices

Network element/EMS platform	Device authentication and authorization method	Documentation reference
MG9000	RADIUS	<i>MG 9000 Security and Administration</i> , NN10162-611
CS 2000 Core Manager (SDM)	PAM_RADIUS	<i>CS 2000 Core Manager</i> , NN10104-511

The following table lists Integrated EMS single sign-on launch points.

Integrated EMS single sign-on launch points

Network element/EMS platform/application	Integrated EMS launch point
USP	USP Command Line USP Manager
Passport 8600 (now known as Ethernet Routing Switch 8600)	PP8600 Command Line
CS 2000 Management Tools	CS 2000 Management Tools
GWC Manager	GWC Manager GWC Manager Network View GUI GWC Unit Node View GUI GWC Unit Command Line GUI
SAM21 Manager	SAM21 Manager
UAS Manager	UAS Manager
LMM	LMM
TMM	TMM
OSSGate	OSSGate BPT Servlet BPT Command Line
MG9000 Manager MG9000 Mid-Tier	MG9000 Manager

Integrated EMS single sign-on launch points

Network element/EMS platform/application	Integrated EMS launch point
APS	APS Manager APS Application
NPM	NPM NPM Command Line
QOS	QOS Command Line
SSPFS	SSPFS Command Line (except CBM platform)
SDM platform	SDM Command Line

Authentication and authorization

Network elements and applications can be configured to use centralized security administration. To enable a device to use centralized security administration, the device must be configured to use the Integrated EMS central security server to authenticate users and access user profile information.

Integrated EMS Central Security Server uses PAM to process the authentication requests and NSSwitch to return user privilege and user profile information to network elements and applications.

PAM services

PAM provides authentication services for clients in the managed network. Customers have the option to use the PAM services that come pre-bundled with the security server or to provide their own. For details on configuring PAM, see [Configuring the Integrated EMS central security server in the network](#).

When a request is forwarded to the Integrated EMS PAM Service Provider (SPI), then authentication is performed against data provisioned and administered by the security administration application on the Integrated EMS client.

Conversely, when PAM services are provided by a customer, incoming authentication requests are forwarded to the customer SPI for resolution against their remote database.

NSSwitch services

NSSwitch provides services to obtain group and profile information for users. Centralized access to network resources depends on the definition of a common set of user groups to map security access for each user. The Nortel Networks solution provides a number of predefined user groups to address the full range of OAM&P functions required across a managed network. For details of these user groups and their categorization, see the [User groups](#) section of [Setting up local user accounts on an SSPFS-based server](#).

Customers can configure NSSwitch to use the service pre-bundled with Integrated EMS or, as with PAM services, provide their own service remotely. When the pre-bundled service is used, group and user profile information is administered from the Integrated EMS security administration GUI. For details, see [Configuring a third-party Pluggable Authentication Module](#).

If NSSwitch services are configured to use a third party system, it is important to note that this security solution supports only the NSSwitch group and password (including shadow) databases. Although other database types may be defined in NSSwitch, they are not used by the central security feature.

Authorization domains

For the mapping details of Integrated EMS devices to authorization domains, see [Mapping of Integrated EMS devices to authorization domains](#).

Single sign-on (SSO)

The single sign-on feature allows users transparent access to multiple network elements and applications through a single login. Once a user has been successfully authenticated for the first time (by user login), an SSO token is created by the Integrated EMS security server that will be used to authenticate the same user on subsequent login attempts.

Network elements and applications use a single sign-on (SSO) interface on the central security server to request SSO tokens whenever authentication is required.

Note: Passport PVG 7480/15000 (now known as Media Gateway 7480/15000), Multiservice Switch 15000, and MDM do not support SSO.

Ports requirements

The following table lists details of port usage.

Process	Port Occupied	Communication
Performance (FTP or SFTP push)	Std.	TCP (out)
SSH	22	TCP (in)
TokenAdmin GUI and HTTPS Pam proxy (non-SSL mode)	80, 8080	TCP (in)
Trap Port	162 (default)	UDP (in and out)
TokenAdmin GUI and HTTPS Pam proxy (SSL mode)	443, 8443	TCP (in)
Syslog client	514	UDP (out)
LDAPS	636	TCP (in)
RADIUS server	1812	UDP (in and out)
SNMP Agent Port	8001 (default)	UDP (in)
Java Client Server Communication	9004, 9005	TCP (in)
NT STD Export	8555	TCP (in)
SCC2-Export Port	8556	TCP (in)
Integrated EMS Server Web Server	9090 (default)	HTTP (in)
Integrated EMS Server Web Server	9091 (default)	HTTPS (in)
Integrated EMS Tomcat	18005, 18009	TCP (in)
SunONE IS (SSL mode)	58081	TCP (in)

Limitations and restrictions

The following are limitations and restrictions:

- Core and Billing Manager (CBM) does not support centralized security administration in (I)SN08
- the maximum number of provisionable central security users is 1000
- third party pluggability is supported for DCE client version 3.2, patch PTF6 for DCE and SunONE directory server 5.1 for LDAP
- for third party pluggability, the only pam.conf edits and the only nns witch.conf edits that are supported are dce and ldap. For details of pam_dce and pam_ldap edits, see [Configuring a third-party Pluggable Authentication Module](#).
- password aging notification is not supported by the following:
 - CICM Manager
 - USP
 - Passport 8600 (now known as Ethernet Routing Switch 8600)
 - Passport PVG 7480/15000 (now known as Media Gateway 7480/15000)
 - Multiservice Switch 15000
 - GWC
 - MG 9000
- in (I)SN07 on SSPFS devices (except CBM), you must set up the user's home directory manually on the device if the user is to support FTP login. FTP to the device does not function for a user if the user's home directory is not set up on the device. In (I)SN08, central authentication for FTP is not supported as there is no longer local caching of user data on the local machine after authentication with a remote server.
- Centrex IP Client Manager (CICM) Element Manager only supports central authentication. CICM Manager does not support single sign-on (SSO).
- The procedure for deleting a user's central account must be followed. If the procedure for disabling or deleting a user session is not followed correctly
 - the user's home directories may be accessible to a new user who inherits the same user ID as the original user
 - the new user who inherits the same user ID as the original user will not be able to log in to the SSPFS security clients

- a certificate must be installed on the Integrated EMS server, before installing Integrated EMS software, to ensure that the system operates correctly
- the total number of groups that a user can belong to cannot exceed sixteen
- a user name is a string of no more than eight bytes consisting of alphabetic characters, numeric characters, period (.), underscore (_), and hyphen (-). The first character should be alphabetic and the field should contain at least one lower case alphabetic character
- a group name consists of characters from the set of lower case alphabetic characters and numeric characters
- Integrated EMS allows you to configure user ID ranges. Sun Solaris security clients such as SSPFS use a user ID to uniquely identify a user. The default Integrated EMS user ID range is 10001-12000. You can change the Integrated EMS user ID. You must ensure that there is no conflict between the new Integrated EMS user ID range and the Sun Solaris system user ID range in /etc/passwd. Such a conflict may severely impact system operation. The following table lists Sun Solaris system accounts and user IDs.

Sun Solaris system accounts and user IDs

root:0, daemon:1, bin:2, sys:3, adm:4, lp:71, uucp:5, nuucp:9, listen:37, nobody:60001, noaccess:60002, nobody4:65534, sshd:100, maint:101, npm:102, npmftp:103, ptm:104, mgems:105, www:106, patcher:107, poller:108, certuser:109, sam21em:110, anonymous:111, image:112, pfrs:113, ntssg:50015, FIELD:50016, oracle:50017, patch:50018

- Passport PVG 7480/15000 (now known as Media Gateway 7480/15000), Multiservice Switch 15000, and MDM do not support SSO.
- User accounts provisioned in the Central Security Administration system:
 - must not have the same numerical user ID or user name as user accounts provisioned in local Unix files on the Integrated EMS server. If a conflict exists where a central user account has the same user name or numerical user ID as a local Integrated EMS server account, then login with the central account may fail on some devices.
 - can not have the same numerical group ID or group name as user groups provisioned in local Unix files on the Integrated EMS Server. If a conflict exists where a central user group has the same group name or numerical group ID as a local Integrated

EMS group, then login involving the central user group may fail on some devices.

- For the reasons explained above, user/group names or numerical IDs among different security database systems should not have duplicate entries. The Carrier VoIP groups listed in the [Secondary user groups](#) table are pre-defined by the Integrated EMS Security Administration system and are an exception to this rule. The Carrier VoIP groups exist in both the Integrated EMS server local Unix files and the Central Security Administrations system.
- When configuring /etc/nsswitch.conf for use with third party security modules, the saml nsswitch entry must always appear before the files entry in the nsswitch stack. The following is an example of the password and group database entries:

Example

passwd: ldap saml files

group: ldap saml files

Centralized user access management using Integrated EMS

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

Integrated EMS user access management

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

- configuring user settings
- configuring scope and group settings

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

Local access requirements

Some MDM userids and groups must be maintained locally on the MDM Server. Local userids are used to access MDM functionality if the connection to the Integrated EMS is not available. MDP tools can only be accessed using local userids. "MDM local userids" and "MDM local groups" lists the userids and groups that remain as local userids and groups after the migration of userids to the Integrated EMS. Other userids may be maintained locally as required

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

MDM local userids

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

MDM local groups

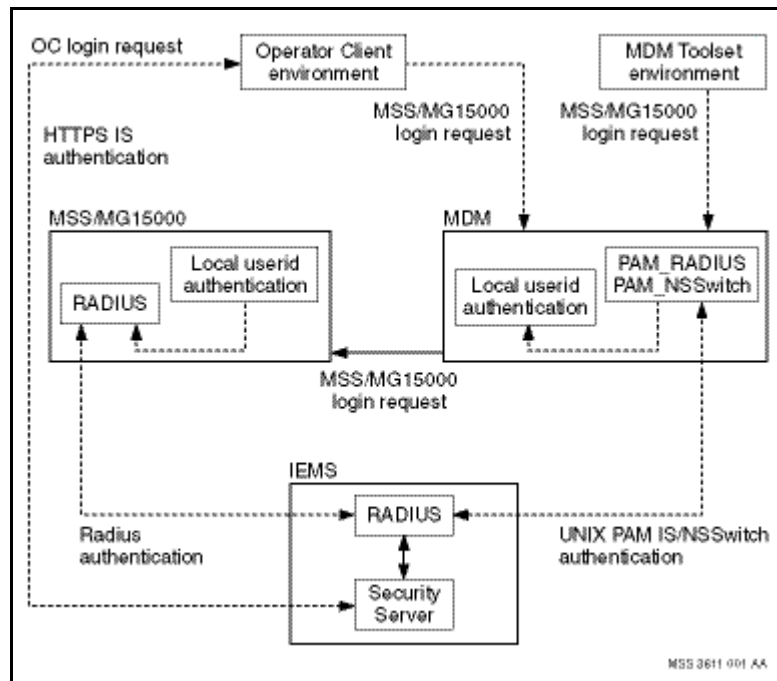
root	adm	staff	noaccess
other	uucp	daemon	nogroup
bin	tty	sysadmin	nortel
sys	nuucp	nobody	<mdpgroup>
Note: For <mdpgroup>, use the MDP administrator group set during installation.			

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

Authentication data flow using Integrated EMS central AAA service

[User authentication and authorization data flow with Integrated EMS on page 360](#) shows the data flow for user authentication and authorization in VoIP solutions using Integrated EMS central AAA service.

User authentication and authorization data flow with Integrated EMS



MDM Toolset environment

The MDM sends an MDM Toolset login message via the PAM_RADIUS interface to the Integrated EMS security server for authentication. When the Integrated EMS security server authenticates a valid userid, it returns information on the authorization level associated with the userid to the MDM. The MDM uses the PAM_NSSwitch interface to determine the associated user information for the MDM system, such as valid groups, shell, and other UNIX information. If the userid is not found on the Integrated EMS system, then MDM local user authentication is invoked.

Operator Client environment

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

MSS/MG15000

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

Integrated EMS user group mappings

The Integrated EMS user groups and the mapping of the MDM and MSS/MG15000 access privileges onto these groups are shown in [Mapping MDM, MSS 15000 and MG 15000 access privileges to Integrated EMS groups in VoIP networks on page 366](#).

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

Administration procedures for Integrated EMS central AAA service

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

- [Updating the MDM Server when the Integrated EMS amadmin password changes on page 361](#)
- [Updating the MDM Server when the Integrated EMS RADIUS shared secret changes on page 362](#)
- [Updating the MSS/MG15000 switch when the Integrated EMS RADIUS shared secret changes on page 363](#)

Updating the MDM Server when the Integrated EMS amadmin password changes

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

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

Procedure steps

At the login session to the MDM server

- 1 Log in to the MDM Server as root.

- 2 Execute the following commands:
cd /opt/nortel/applications/security/current_nssaml/swmgmt/bin
./configure_nssaml.sh -subcomponent password

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

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

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

where

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

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

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

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

Procedure steps

At the login session to the MDM server

- 1 Log in to the MDM Server as root.
- 2 Execute the following commands:
cd
/opt/nortel/applications/security/current_pamradclt/swmgmt/bin
./configure_pamradclt.sh -subcomponent servers
- 3 Enter the Integrated EMS RADIUS shared secret as prompted.

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

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

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

Procedure steps

At the login session to the MSS/MG15000 switch

- 1 Log in to the MSS/MG15000 switch as system administrator.
- 2 Enter provisioning mode:
start prov
- 3 Obtain the provisioning file:
copy prov
- 4 Change the RADIUS shared secret:
set Ac Radius Server/0 sharedSecret <new_shared_secret>
where
 <new_shared_secret>
 is the new Integrated EMS Radius shared secret
- 5 Verify the provisioning change:
check prov
- 6 Save the provisioning change:
save prov
- 7 Activate the provisioning change:
activate prov
- 8 Confirm the provisioning change:
confirm prov
- 9 Commit the provisioning change:
commit prov
- 10 Exit provisioning mode after the commit is complete:
end prov

Updating the MDM Server when the Integrated EMS IP address changes

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

Procedure steps***At the login session to the MDM server***

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

```
cd  
/opt/nortel/applications/security/current_pamradclt/swmgmt/bin  
./configure_pamradclt.sh -subcomponent clients
```
- 3 Enter the Integrated EMS IP address as prompted.

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

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

Procedure steps***At the login session to the MSS/MG15000 switch***

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

```
start prov
```
- 3 Obtain the provisioning file:

```
copy prov
```
- 4 Change the Integrated EMS IP address:

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

where

```
<new_IEMS_IPaddr>
```

is the new Integrated EMS IP address
- 5 Verify the provisioning change:

```
check prov
```
- 6 Save the provisioning change:

```
sav prov
```

- 7 Activate the provisioning change:
 activate prov
- 8 Confirm the provisioning change:
 confirm prov
- 9 Commit the provisioning change:
 commit prov
- 10 Exit provisioning mode after the commit is complete:
 end prov

Updating JWS software when the MDM Server host name changes

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

Procedure steps

At the login session to the MDM server

- 1 Log in to the MDM Server as root.
- 2 Edit the configuration file:
 vi
 /opt/nortel/config/applications/desktop/jws/mft/resources/desktop/DesktopGUI.jnlp
- 3 Change the host name references to the new host name.
- 4 Save and close the file.

Updating the MDM Server when the Integrated EMS host name changes

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

Procedure steps

At the login session to the MDM server

- 1 Log in to the MDM Server as root.
- 2 Execute the following commands:
 cd /opt/nortel/applications/security/current_isclient/swmgmt/bin
 ./configure_isclient.sh
- 3 Enter the Integrated EMS host name as prompted.

Mapping MDM, MSS 15000 and MG 15000 access privileges to Integrated EMS groups in VoIP networks

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

Integrated EMS user group mappings

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

The six Integrated EMS device areas are:

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

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

- ro (read only) level provides the ability to display surveillance information, but not to alter it.
- rw (read/write) level provides the ability to display surveillance information and to do configuration of MSS/MG15000.
- mtc (maintenance) level provides the ability to configure MSS/MG15000 nodes. Operator Client application access is not supported.

- sprov (subscriber provisioning) level is mapped to the system administration impact level for MSS/MG15000 nodes and provides access to MSS/MG15000 administration tools from the Operator Client application.
- adm (administration) level is mapped to the debug impact level for MSS/MG15000 nodes and provides access to all MDM resources except MDP. A special local MDM userid is required to access MDP functionality.

Integrated EMS group mapping for MDM Toolset functionality

[Integrated EMS user group mapping for MDM Toolset functions on page 367](#) shows the mapping between the Integrated EMS groups and the MDM Toolset functions.

Integrated EMS user group mapping for MDM Toolset functions

MDM Toolset functions	Integrated EMS group					MDM local userid
	emsro	emsrw	emsmtc	emssprov	emsadmin	
Alarm Display: Active	allow	allow	deny	allow	allow	allow
Alarm Help	allow	allow	allow	allow	allow	allow
Command Console	allow	allow	deny	allow	allow	allow
Component Information Viewer	allow	allow	deny	allow	allow	allow
Component Status Display	allow	allow	deny	allow	allow	allow
Data Synchronization Administration	allow	allow	allow	allow	allow	allow
Data Viewer	deny	deny	deny	allow	allow	allow
Disruptive Command Safeguard	deny	deny	deny	deny	allow	allow
Enhanced Multiservice Switch interface controller (EPIC)	deny	allow	deny	allow	allow	allow
General management data router (GMDR) administration	deny	allow	deny	allow	allow	allow
Host group directory server (HGDS) administration	deny	allow	deny	allow	allow	allow
Log Browser	allow	allow	deny	allow	allow	allow
MDM license	deny	allow	deny	allow	deny	allow
(Sheet 1 of 3)						

Integrated EMS user group mapping for MDM Toolset functions

MDM Toolset functions	Integrated EMS group					MDM local userid
	emsro	emsrw	emsmtc	emssprov	emsadmin	root
MDM release update	deny	allow	deny	allow	allow	allow
MDP configuration	deny	deny	deny	deny	deny	deny
MDP log viewer	deny	deny	deny	deny	deny	deny
MDP data viewer	deny	deny	deny	allow	allow	deny
Memory utilization	allow	allow	allow	allow	allow	allow
Network Activation Tool	deny	allow	deny	allow	allow	allow
MSS Service Data Backup and Restore	deny	deny	allow	deny	allow	allow
Network Model shared memory utilization	allow	allow	allow	allow	allow	allow
Network Status Bar	allow	allow	deny	allow	allow	allow
Network Viewer	allow	allow	deny	allow	allow	allow
Nodal Provisioning	deny	allow	deny	allow	allow	allow
Nodal Provisioning Template	deny	allow	deny	allow	allow	allow
On-line documentation	allow	allow	allow	allow	allow	allow
Operational commands	allow	allow	deny	allow	allow	allow
Password Change	deny	deny	deny	deny	allow	allow
Password encryption	deny	deny	deny	deny	deny	deny
Query Historical Alarms	allow	allow	deny	allow	allow	allow
Quick Start	deny	deny	deny	deny	deny	allow
Server administration	deny	allow	deny	allow	allow	allow
Service selection	allow	allow	deny	allow	allow	allow
Shelf view	allow	allow	deny	allow	allow	allow
Software download	deny	deny	allow	deny	allow	allow
Succession ATM Software Migration	deny	allow	deny	allow	allow	allow
Succession IP Software Migration	deny	allow	deny	allow	allow	allow
System log display	allow	allow	deny	allow	allow	allow
(Sheet 2 of 3)						

Integrated EMS user group mapping for MDM Toolset functions

MDM Toolset functions	Integrated EMS group					MDM local userid
	emsro	emsrw	emsmtc	emssprov	emsadmin	
UNIX access	deny	deny	deny	deny	allow	allow
Note: MDP configuration and log viewer commands must be accessed using the MDP administrator userid maintained locally on the MDM workstation.						
(Sheet 3 of 3)						

Integrated EMS group mappings for MDM Operator Client

[Integrated EMS user group mapping for MDM Operator Client tools on page 369](#) shows the mapping between the Integrated EMS groups and the tools available through the Operator Client application.

Integrated EMS user group mapping for MDM Operator Client tools

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

Integrated EMS user group mapping for MDM Operator Client tools

MDM Operator Client Resources	Integrated EMS group				
	emsro	emsrw	emsmtc	emssprov	emsadmin
Operator Commands	deny	allow	deny	allow	allow
Command Console	deny	allow	deny	allow	allow
Telnet	deny	allow	deny	allow	allow
NTPs	allow	allow	allow	allow	allow
(Sheet 2 of 2)					

Integrated EMS group mappings for MSS/MG15000 functionality

[Integrated EMS user group mapping for MSS/MG15000 access privileges on page 370](#) shows the mapping between the Integrated EMS groups and the MSS/MG15000 access privileges.

Integrated EMS user group mapping for MSS/MG15000 access privileges

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

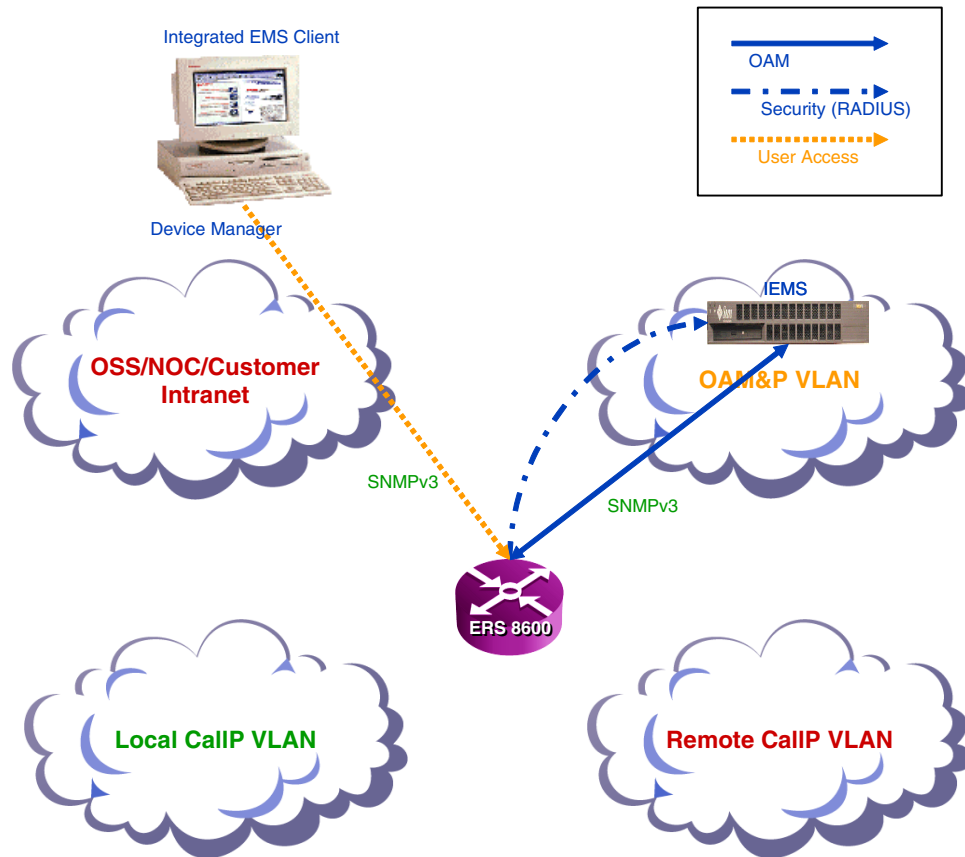
Integrated EMS secure launch to Ethernet Routing Switch 8600 overview

(I)SN08 enhances security measures for communications between management applications and the Ethernet Routing Switch 8600. The management applications include Integrated EMS and Device Manager. All communications between OAM applications and the Ethernet Routing Switch 8600 must be authenticated and encrypted. Authentication and encryption is provided by SNMPv3 and SSHv2. The following security measures are introduced:

- SNMPv3/USM secures all OAM interfaces between the Ethernet Routing Switch 8600, Device Manager, and Integrated EMS
- SNMPv3/USM supports AuthPriv mode
- Integrated EMS uses Device Manager in secure SNMP mode for installation, configuration, and launching procedures
- new engineering rules apply to open and closed ports on the Ethernet Routing Switch 8600

Configuration is required for Ethernet Routing Switch 8600, Integrated EMS, and Device Manager. Configuration on the Ethernet Routing Switch 8600 must be completed before the configuration of Integrated EMS and Device Manager. For details of configuration procedures, see *Integrated EMS Configuration Management*, NN10330-511.

For an illustration of the security architecture for the Ethernet Routing Switch 8600, see the following figure.

Ethernet Routing Switch 8600 security architecture for (I)SN08

CS 2000 Management Tools security and administration

Overview

Security on the CS 2000 Management Tools server is achieved using Pluggable Authentication Module (PAM). PAM is a Unix programming interface that has the ability to integrate with different authentication mechanisms such as Distributed Computing Environment (DCE).

The default authentication mechanism for the CS 2000 Management Tools server is Unix. However, if desired, the authentication mechanism can be changed from Unix to DCE. If required, refer to procedure [Changing the authentication mechanism between UNIX and DCE on page 490](#).

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and SAM21 Element Manager) are able to communicate with their respective server-side application through multiple firewalls facing either the client or the server side, using a minimum number of configurable TCP/IP ports. Communication through multiple firewalls is achieved using a Socks proxy, which is started when the server is started.

Note: The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

The server-side Socks port has a default value of 10080, and the client-side Socks port has a default value of 10090. If the default value is not acceptable, you can change the default value of the server-side and client-side ports using procedure “Configuring client/server ports on an SSPFS-based server for secure firewall communications” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

Centralized security administration

Centralized security administration is provided through the Integrated Element Management System (EMS). The Integrated EMS provides a comprehensive architecture based on PAM and Name Service Switch (NSS). This architecture provides the following features:

- central administration of user accounts
- central authentication and authorization of centrally managed user accounts
- single sign-on (SSO) between the Integrated EMS and applications that support SSO
- third-party authentication and authorization plug-in capability

The Integrated EMS central security server uses PAM to process the authentication requests and NSSwitch to return user privilege and user profile information to the CS 2000 Management Tools applications.

Activating central security administration in the network consists of the following activities:

- configuring and activating the Integrated Element Management System (EMS) central security server in the network (refer to procedure [Configuring the Integrated EMS central security server in the network on page 429](#))
- configuring a central security client, which refers to all the SSPFS-based servers that host the OAM&P applications (refer to procedure [Configuring an SSPFS-based central security client on page 433](#))

To configure the single sign-on (SSO) token time-out values, which are the time the Single Sign-On (SSO) token can remain idle before it becomes invalid, and the time the SSO token id can be used before it expires, refer to procedure [Configuring the Single Sign-On token on page 466](#).

User accounts

As of the SN07 release, you can centrally manage the user accounts on the CS 2000 Management Tools server, through the Integrated Element Management System (EMS) central security server, or you can continue to locally manage the user accounts.

If you opt to centrally manage the user accounts, the following procedures must be completed:

Note: The steps to migrate existing user accounts that are to be centrally managed, are included in the procedures.

- [Configuring the Integrated EMS central security server in the network on page 429](#)
- [Configuring an SSPFS-based central security client on page 433](#)

Users of Nortel Networks OAM&P client applications must belong to the primary group “succssn” for login access, and to one or more secondary user groups to specify the operations the user is authorized to perform. A list of secondary user groups is provided in procedure [Setting up local user accounts on an SSPFS-based server on page 402](#).

To add new users to the Integrated EMS central security server, refer to the Integrated EMS Security and Administration document, NN10336-611.

Password aging

Password aging for local user accounts applies to all user accounts, including the root user account. A password is valid for eight weeks, and the user receives a warning at login two weeks before the password expires. In the event the root password fails with `su: Sorry, use` procedure [Changing an expired root password on an SSPFS-based server on page 423](#).

Note: Password aging for centrally managed user accounts, is configurable. Refer to procedure, “Setting a user profile” in the Integrated EMS Security and Administration document, NN10336-611.

Backup and restore

You can back up file systems and oracle data on a Succession Server Platform Foundation Software (SSPFS)-based server using a Digital Audio Tape (DAT) for Sun Netra t1400-type servers, or a CD or DVD for Sun Netra 240-type servers.

A full system backup on the SSPFS-based server that hosts the CS 2000 Management Tools involves backing up the following information:

- oracle data
- file systems
- APS audio files when APS is present

It is highly recommended you perform a full system backup before and after you upgrade the SSPFS and application software on the SSPFS-based server. The relevant procedures are as follows:

- [Performing a backup of oracle data on an SSPFS-based server on page 168](#).
- [Performing a backup of file systems on an SSPFS-based server on page 174](#).
- [Performing a backup of APS audio files to tape on page 521](#) for Sun Netra t1400-type servers, or [Performing a backup of APS audio files to CD or DVD on page 523](#) for Sun Netra 240-type servers.

The relevant procedure to perform a restore from backup media are as follows:

- [Performing a full system restore on an SPFS-based server on page 313.](#)
- [Restoring the oracle data on an SSPFS-based server on page 307.](#)
- [Performing a restore of APS audio files from tape on page 533](#) for Sun Netra t1400-type servers, or [Performing a restore of APS audio files from CD on page 535](#) for Sun Netra 240-type servers.

File system backup

Applications and the system have several sets of configuration files with static information about the system configuration and operating parameters. This information is backed up in-service using standard Unix commands and a Solaris utility called SNAPFS which takes a snapshot of the file system.

The file system layout on SSPFS-based servers is as follows:

File system	Types of information stored in file system
/	operating system software and administrations
/var	operating system software and administrations
/data	application data in flat files
/opt	third-party software as Platform common services
/opt/nortel	Nortel applications
/data/oradata	Oracle data files (applies to SSPFS-based servers that host the CS 2000 Management Tools, APS, and Integrated EMS)
/data/qca	QoS Collector Application (QCA) data (applies to SSPFS-based servers that host the CS 2000 Management Tools)
/data/mg9kem/logs	MG 9000 Manager logs (applies to SSPFS-based servers that host the MG 9000 Manager)
/PROV_data	audio transaction files before they are sent to the UAS (applies to SSPFS-based servers that host the APS)

File system	Types of information stored in file system
/user_audio files	audio uploaded from the user desktop prior to its import into the database (applies to SSPFS-based servers that host the APS)
/audio_files	audio data that has been imported into the database (applies to SSPFS-based servers that host the APS)

Note: File systems “/”, “/var”, “/data”, “/opt”, and “/opt/nortel” are present on every SSPFS-based server. The other file systems vary according to the applications installed on the server.

Oracle data backup

The application data in the Oracle database is not automatically backed up. You can enable automated Oracle data backups, where the system backs up all application data in the Oracle database on a daily basis at a specified time to a DAT, CD or DVD.

To view or change the current configuration settings for automated backup of Oracle data, refer to procedure [Configuring automated data backups on an SSPFS-based server on page 498](#).

Data on a CD or DVD cannot be overwritten, therefore, you must insert a blank CD or DVD into the drive prior to the next scheduled backup.

If you leave the same DAT in the drive, the contents of the DAT will be replaced with the new backup data when the backup is scheduled to run. If you want to preserve the daily backup of your application data, remove the DAT from the drive and insert a new one prior to the next scheduled backup. It is recommended that you label the DAT with the date, time and content (oracle data backup).

ATTENTION

In order to maintain network functionality, the CS 2000 Management Tools persistent data in the Oracle database and the associated CORE/CM tables must match at all times. Therefore, it is recommended that the CS 2000 Management Tools support person modify the automated oracle data backup schedule to run in parallel to the CORE Image Dump schedule. This will ensure that there are always CORE Images and CS 2000 Management Tools database backups that are 100% identical in configuration information.

Centralized backups

In the SN08 release, the Backup Restore Manager is introduced to provide centralized control of backup capabilities for the following core components of the Communication Server 2000:

- XA-core or third-party core
- CS 2000 Management Tools
- MG 9000 Manager
- Integrated Element Management System (EMS)
- Core Billing Manager (CBM)

The Backup Restore Manager consists of the Synchronous Backup Restore Manager (SBRM) software that resides on the Integrated EMS server, and the Device Backup Restore Manager (DBRM) software that resides on the components. The SBRM software controls and synchronizes backup-related activities across the components through the DBRM software on the components.

Note: The DBRM software on the CBM is only present to enable backups on the XA-core or third-party core. Data on the CBM itself is not backed up through the SBRM.

The SBRM is launched through the Integrated EMS GUI, and enables backups of database tables, configuration files, and property files on the various components. Backup of program store and associated patches is not included in the functionality.

On SSPFS-based components, the backup file is placed in directory “/data/bkresmgr/backup”. On the XA-core or third-party core, the location of the backup file is configurable.

Note: Restore of the backup image is not supported in SN08. To perform a restore from the backup image, refer to procedure [Restoring the oracle data on an SSPFS-based server on page 307](#).

Prior to using the SBRM, the secure shell (SSH) must be configured between the Integrated EMS server where the SBRM software is installed, and the components where the DBRM software is installed. If required, refer to procedure [Configuring SSH between the backup restore manager servers on page 81](#).

To configure the SBRM for automated execution of backups, refer to procedure [Configuring the automated synchronous backup restore manager service on page 89](#).

Tools and utilities

Security and administration procedures are performed on the SSPFS-based server where the CS 2000 Management Tools reside.

Procedures

The security and administration procedures available for the CS 2000 Management Tools are listed under one of the following categories:

- [Local user accounts and passwords on page 379](#)
- [Centralized security configuration on page 380](#)
- [Security on page 380](#)
- [Backup and restore on page 381](#)
- [Client and server applications on page 382](#)
- [Administration on page 383](#)

Local user accounts and passwords

The following table lists the procedures available for local user accounts and passwords.

Local user accounts and passwords procedures

Procedure
Changing the Oracle user password on an SPFS-based server on page 398
Changing the APS Oracle account password on page 400
Setting up local user accounts on an SSPFS-based server on page 402
Changing a user password on an SSPFS-based server on page 417
Changing an expired root password on an SSPFS-based server on page 423
Deleting local user accounts from an SSPFS-based server on page 415
Setting the Oracle Listener password on an SPFS-based server on page 424

Local user accounts and passwords procedures

Procedure
Changing the Oracle Listener password on an SSPFS-based server on page 426
Configuring OSSGate password control on page 419

Note: For details about managing user accounts on network components, refer to your Carrier Voice over IP component documentation (see [Technical Publications on page 327](#)).

Centralized security configuration

The following table lists the procedures available for centralized security configuration.

Centralized security configuration procedures

Procedure
Configuring the Integrated EMS central security server in the network on page 429
Configuring an SSPFS-based central security client on page 433
Configuring a third-party Pluggable Authentication Module on page 446
Replacing HTTPS certificate on security server for SunOne component on page 457
Reverting the client server to its previous configuration on page 462
Configuring the Single Sign-On token on page 466

Security

The following table lists the procedures available for security.

Security procedures

Procedure
Changing the authentication mechanism between UNIX and DCE on page 490
Setting secure FTP proxy on page 495

Backup and restore

The following table lists the procedures available for backup and restore.

Backup and restore procedures

Procedure
Configuring automated data backups on an SSPFS-based server on page 498
Performing a backup of oracle data on an SSPFS-based server on page 168
Performing a backup of file systems on an SSPFS-based server on page 174
Performing a backup of APS audio files to tape on page 521
Performing a backup of APS audio files to CD or DVD on page 523
Performing a full system restore on an SPFS-based server on page 313
Restoring the oracle data on an SSPFS-based server on page 307
Performing a restore of APS audio files from tape on page 533
Performing a restore of APS audio files from CD on page 535
Cloning the image of one node in a cluster to the other node on page 502

Centralized backup and restore

The following table lists the procedures available for centralized backup and restore.

Centralized backup and restore procedures

Procedure
Configuring SSH between the backup restore manager servers on page 81
Configuring the automated synchronous backup restore manager service on page 89
Running the synchronous backup restore manager from a component level on page 99

Client and server applications

The following table lists the procedures available for the client and server applications.

Client and server applications procedures

Procedure
Starting the SESM server application on page 514
Starting the SAM21 Manager server application on page 517
Starting the NPM server application on page 519
Starting the APS server application on page 531
Launching CS 2000 Management Tools and NPM client applications on page 537
Accessing the Network Patch Manager CLUI on page 550
Starting the batch provisioning tool on page 552
Connecting to OSSGate on page 554
Changing modes within OSSGate on page 556
Stopping the SESM server application on page 557
Stopping the SAM21 Manager server application on page 559
Stopping the NPM server application on page 561
Stopping the APS server application on page 563
Disconnecting from OSSGate on page 565
Starting and stopping the PM Poller on page 566
Starting and stopping the QoS Collector Application on page 569
Starting the OMPUSH server application on page 575
Stopping the OMPUSH server application on page 577
Starting or stopping the automated synchronous backup restore manager service on page 95
Initializing the NPM database on page 587

Administration

The following table lists the procedures available for administration.

Administration procedures

Procedure
Increasing the size of a file system on an SSPFS-based server on page 593
Verifying disk utilization on an SPFS-based server on page 606
Installing or replacing an HTTPS certificate on an SSPFS-based server on page 608
Preparing a DVD-RW for use on page 618
Clearing the JWS cache on a client workstation on page 572

Changing the password warning threshold on the central security server

Application

Use this procedure to change the system-wide password warning threshold for user accounts managed by the Integrated EMS Security Server.

Note: The new system-wide password warning threshold will take effect when passwords of existing user accounts are reset or when new user accounts are created.

Prerequisites

You must have root user privileges to perform this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the server where Integrated EMS resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change to the directory where the global password warning script is located by typing:

```
cd  
/opt/nortel/applications/security/slisext_1.1.0/bin/swmgmt/bin
```

and pressing the Enter key.

- 6 Run the global password warning script by typing:
./update/GlobalPasswordWarning.sh
and pressing the Enter key.
- 7 When prompted, enter the number of days you want to set.
Press the Enter key.
- 8 You have completed this procedure.

Changing the amAdmin password

Application

Use this procedure to change the amAdmin password. The amAdmin account is an application account used internally by the Integrated EMS security server components. It is not a user account and thus cannot be used for actual user logins.

ATTENTION

The password of the amAdmin user account is not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, the password and expiry change procedures described in this section must be performed on both servers.

ATTENTION

Changing the amAdmin password disrupts any existing security sessions and so it is recommended that this procedure is performed as a scheduled event.

ATTENTION

Passwords are changed in client machines first and then on the server. This means that changing the password on the client machine will prevent further logins using centrally administered accounts until the password has been changed on the server. As such, it is recommended that passwords on clients running critical applications are changed last. This means that the unavailability of centrally administered accounts will exist for a shorter period of time on these clients.

ATTENTION

If you allow passwords of the system accounts listed above to expire, all access to the system using centrally administered accounts will be denied until the passwords are reset. In this case, local emergency accounts must be used to access all applications or devices. It is strongly recommended that the value for the number of days before the password expires is set to zero (never expire).

ATTENTION

When you run the `configure_nsssaml.sh` script to set the NSSwitch SPI passwords and the `is_passwd.sh` to set the Identity server passwords, you must set the passwords to the same value.

Prerequisites

None

Action

Perform the following steps:

- One each remote NSS-SAML client (not located on an Integrated EMS server), starting with the least critical, change the NSSwitchSPI password ([step 1](#) through [step 13](#)).
- On the inactive Integrated EMS security server, change the NSSwitchSPI password ([step 14](#) through [step 19](#)).
- On the active Integrated EMS security server, change the NSSwitchSPI and the Identity Server passwords ([step 20](#) through [step 26](#)).
- On the inactive Integrated EMS security server, change the Identity Server password ([step 28](#) through [step 32](#)).

At your workstation

- 1 Telnet to the active remote NSS-SAML client by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the server where the NSS-SAML client resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

- 5 Change the NSSwitchSPI password by typing:

```
/opt/nortel/applications/security/current_nsssaml/swmgmt/bin/configure_nsssaml.sh  
-subcomponent password
```

and pressing the Enter key.
- 6 When prompted, enter the new password.
- 7 Telnet to the inactive remote NSS-SAML client by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the server where the NSS-SAML client resides
- 8 When prompted, enter your user ID and password.
- 9 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 10 When prompted, enter the root password.
- 11 Change the NSSwitchSPI password by typing:

```
/opt/nortel/applications/security/current_nsssaml/swmgmt/bin/configure_nsssaml.sh  
-subcomponent password
```

and pressing the Enter key.
- 12 When prompted, enter the new password.
- 13 Repeat [step 1](#) through [step 12](#) for each remote NSS-SAML client (not located on an Integrated EMS server), starting with the least critical.
- 14 Log in to the inactive Integrated EMS security server as root by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the server where the Integrated EMS security server resides

- 15 When prompted, enter your user ID and password.
- 16 Change to the root user by typing
\$ su - root
and pressing the Enter key.
- 17 When prompted, enter the root password.
- 18 Change the NSSwitchSPI password by typing:
/opt/nortel/applications/security/current_nsssaml/swmgt/bin/configure_nsssaml.sh
-subcomponent password
and pressing the Enter key.
- 19 When prompted, enter the new password.
- 20 Telnet to the active Integrated EMS security server by typing
> telnet <server>
and pressing the Enter key.
where
server
is the IP address or host name of the server where the Integrated EMS resides
- 21 When prompted, enter your user ID and password.
- 22 Change to the root user by typing
\$ su - root
and pressing the Enter key.
- 23 When prompted, enter the root password.
- 24 Change the NSSwitchSPI password by typing:
/opt/nortel/applications/security/current_nsssaml/swmgt/bin/configure_nsssaml.sh
-subcomponent password
and pressing the Enter key.
- 25 When prompted, enter the new password.
- 26 Change the Identity server password to the same value as the NSSwitch SPI password by entering:
/opt/nortel/applications/security/current_isclient/bin/nortel/is_passwd.sh -is_passwd write
-exp <n>

where

n is the number of days after which the password for the **amadmin** account will expire. It is strongly recommended that the value for the number of days before the password expires is set to zero (never expire).

27 When prompted, enter the new password.

28 Log in to the inactive Integrated EMS security server as root by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

is the IP address or host name of the server where the Integrated EMS security server resides

29 When prompted, enter your user ID and password.

30 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

31 When prompted, enter the root password.

32 Change the Identity server password to the same value as the NSSwitch SPI password by entering:

```
/opt/nortel/applications/security/current_iscl  
ient/bin/nortel/is_passwd.sh -is_passwd write
```

33 When prompted, enter the new password.

34 You have completed this procedure.

Changing the system account passwords on the central security server

Application

Use this procedure to change passwords and set their expiry status to “never expire” on the following system accounts in a single operation on the Integrated Element Management System (IEMS) security server:

administrator, ndsadmin, puser, dsameuser, amldapuser,
replication manager

Note: The system accounts listed above are application accounts used internally by the IEMS security server components. They are not user accounts and therefore cannot be used for actual user login.

ATTENTION

The passwords of the system accounts listed above are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, the password and expiry change procedures described in this section must be performed on both servers.

ATTENTION

The server automatically restarts if this procedure is performed on the active server and so it is recommended that this procedure is performed as a scheduled event.

ATTENTION

If you allow passwords of the system accounts listed above to expire, all access to the system using centrally administered accounts will be denied until the passwords are reset. In this case, local emergency accounts must be used to access all applications or devices. It is strongly recommended that steps in this procedure are performed to avoid any outage to central security servers.

Prerequisites

To perform this procedure, you must have root user privileges.

Action

Perform the following steps to complete this procedure.

Changing the system account passwords

At your workstation

- 1 Change the amadmin password for the NSS-SAML client on the active and inactive IEMS Security servers. For details, see [Changing the amAdmin password](#).
- 2 Telnet to the active server by typing
`> telnet <server>`
 and pressing the Enter key.
 where
 server
 is the IP address or host name of the server where IEMS resides
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing
`$ su - root`
 and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Change to the directory where the change password script is located by typing:
`cd
/opt/nortel/applications/security/core_1.1.0/bin/`
 and pressing the Enter key.
- 7 To change the sytem account passwords on the active server, type:
`ss_change_passwd.sh`
 and press Enter.

If you are performing this procedure in	Do
a simplex configuration	you have completed this procedure
a high availability (HA) configuration	go to the next step

- 8 Telnet to the inactive server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the server where IEMS resides
- 9 When prompted, enter your user ID and password.
- 10 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 11 When prompted, enter the root password.
- 12 Change to the directory where the change password script is located by typing:

```
cd  
/opt/nortel/applications/security/core_1.1.0/bin/
```

and pressing the Enter key.
- 13 To change the sytem account passwords on the inactive server, type:

```
ss_change_passwd.sh -local
```

and press Enter.
- 14 You have completed this procedure.

Changing the saml password on an SSPFS-based central security client

Application

Use this procedure to change the saml password on an SSPFS-based central security client.

Prerequisites

You need root user privileges to complete this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Log in to the client server by typing
`> telnet <server>`
and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based client server
- 2 When prompted, enter the user ID and password for an account that was migrated to the Integrated EMS central security server.
- 3 Change to the root user by typing
`$ su - root`
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Access the command line interface by typing
`# cli`
and pressing the Enter key.

Example response

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

select -
```

- 6** Enter the number next to the “Configuration” option in the menu.

Example response

Configuration

- 1 - NTP Configuration
- 2 - Apache Proxy Configuration
- 3 - DCE Configuration
- 4 - OAMP Application Configuration
- 5 - CORBA Configuration
- 6 - IP Configuration
- 7 - DNS Configuration
- 8 - Syslog Configuration
- 9 - Database Configuration
- 10 - NFS Configuration
- 11 - Bootp Configuration
- 12 - Restricted Shell Configuration
- 13 - Security Services Configuration
- 14 - Login Session
- 15 - Location Configuration
- 16 - Cluster Configuration
- 17 - Succession Element Configuration
- 18 - snmp_poller (SNMP Poller Configuration)

- X - exit

Select -

- 7** Enter the number next to the “Security Services Configuration” option in the menu.

Example response

Security Services Configuration

- 1 - Socks Configuration
- 2 - IEMS Server Location Configuration
- 3 - PAM Configuration

- x - exit

select -

- 8** Enter the number next to the “PAM Configuration” option in the menu.

Example response

```
PAM Configuration
1 - Central Security Client Configuration

x - exit

select -
```

- 9** Enter the number next to the “Central Security Client Configuration” option in the menu.

Example response

```
Central Security Client Configuration
1 - pam_orig (Use Default PAM Configuration)
2 - pam_radius (Use Security Server)
3 - saml_passwd_conf (Configure saml
    password)

x - exit

select -
```

- 10** Enter the number next to the “saml_passwd_conf” option in the menu.

Example response

```
=== Executing "saml_passwd_conf"

Enter the SAML password (default: slisamadmin):
mypassword

**Confirm Settings**

SAML Password: slisamadmin

Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

11 Confirm the settings by typing**ok**

and pressing the Enter key.

Example response

Configure Password Successful

=== "saml_passwd_conf" completed successfully

You have completed this procedure.

Changing the Oracle user password on an SPFS-based server

Application

Use this procedure to change the default Oracle passwords on a Server Platform Foundation Software (SPFS)-based server.

Note: Refer to procedure [Changing the APS Oracle account password on page 400](#), to change the default password.

ATTENTION

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

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

At your workstation

- 1 Log in to the server by typing
 `> telnet <server>`
and pressing the Enter key.
where
 server
 is the IP address or host name of the SPFS-based server
 Note: In a two-server configuration, log in to the active server using its physical IP address.
- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing
`$ su -`
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change to the Oracle user by typing
`# su - oracle`
and pressing the Enter key.
- 6 Change the password by typing
`$ /opt/nortel/sspfs/db/pfsora_set_pwd <userID>`
and pressing the Enter key.

Where

userID

is the user ID of the Oracle user

Example response:

Enter new password for user SYSTEM:

- 7 When prompted, enter the new password for the system.

Example response:

Re-enter new password:

- 8 When prompted, enter the password a second time to confirm the password.

Example response:

Please wait...

Successfully changed password for Oracle user
SYSTEM

Note: The command takes approximately 15 to 20 seconds to execute.

You have completed this procedure.

Changing the APS Oracle account password

When the APS is installed, a default password is assigned to the Oracle account. This procedure enables you to change the default password, for added system security.

Changing the APS Oracle account password

In a telnet connection to the APS server

- 1 Change to the root user by entering the following command:
su - root
- 2 When prompted, enter the root password.
- 3 If you are unsure whether the password has been changed, obtain the current password by entering the following command:

getNTDBpasswd.ksh

The system displays the current Oracle account password.

- 4 Perform the following steps to change the Oracle account password:
 - a Enter the following command to run the script that enables you to change the password:
/usr/ntdb/uas/scripts/setNTDBpasswd.ksh
 - b At the prompt, enter the current APS Oracle account password.

Note: This is the password that you displayed in step 3.
 - c At the prompt, enter the new APS Oracle account password.
 - d At the prompt, reenter the new APS Oracle account password.

The system changes the password in UNIX and in the Oracle database.

- 5 Restart the APS processes by entering the following command:

servrestart APS

A message eventually displays indicating that APS restarted successfully.

- 6 Enter the following commands to complete the password change:

cd /

. /etc/profile

. ./profile

- 7** You can now check the password change you have made by entering the following command:

getNTDBpasswd.ksh

The system displays the current Oracle account password.

- 8** You have completed this procedure.

Setting up local user accounts on an SSPFS-based server

Application

Use this procedure to add local user accounts on a Succession Server Platform Foundation Software (SSPFS)-based server and assign them to user groups. Also use this procedure to assign existing user accounts to user groups. For information on user groups, see [Additional information on page 404](#).

If you choose to centrally manage your user accounts, refer to procedure “Adding new users” in the Integrated EMS Security and Administration document, NN10336-611.

ATTENTION

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

Prerequisites

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

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Log in to the Active server by typing

```
> telnet <server>
```


and pressing the Enter key.
where

```
server
```


is the IP address or host name of the SSPFS-based server
Note: In a two-server configuration, log in to the Active server using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```


and pressing the Enter key.

- 4 When prompted, enter the root password.
- 5 Use the following table to determine your next step.

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

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

```
# useradd -g succssn <userid>
```

and pressing the Enter key.
where
userid
is a variable for the user name
- 7 Create a password for the user you just added by typing

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

and pressing the Enter key.
where
userid
is the user name you added in the previous step
- 8 When prompted, enter a password of at least three characters.
Note: It is not recommended to set a password with an empty value. Use a minimum of three characters.
- 9 When prompted, enter the password again for verification.
- 10 Proceed to step [13](#).
- 11 Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.
where
userid
is a variable for the user name
- 12 Note the user groups the user currently belongs to.

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

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

and pressing the Enter key.

where

groupA, groupB,...

are the secondary user groups (see table [Secondary user groups on page 404](#)) and any other user groups you noted in step [12](#) to which the user already belonged

Include a comma between groups, but no space.

userid

is a variable for the user name

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

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

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

You have completed this procedure.

Additional information

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

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm
trkrw	lnrw	mgcrw	mgrw	emsrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov
trkmtc	lnmtc	mgcmtec	mgmtc	emsmtec
trkro	lnro	mgcro	mgro	emsro

A secondary user group consists of

- a user group domain
- a user group operation

User group domain

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

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

User group operation

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

Operation	User role mapping
adm (administration)	Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, spro, mtc, and ro user operations.
rw (read/write)	Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do spro, mtc, and ro user operations.

Operation	User role mapping
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do sprov and ro user operations.
sprov (subscriber provisioning)	Can view status and configuration and change provisioning data, but cannot change maintenance state or do base component configuration. The sprov user can also do ro user operations.
ro (read-only)	Can view status and configuration, but cannot make changes.

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

- [Node provisioning operations on page 407](#)
- [Audit operations on page 408](#)
- [Carrier provisioning operations on page 409](#)
- [Alarm operations on page 409](#)
- [Internet transparency operations on page 409](#)
- [Trunk provisioning operations on page 410](#)
- [Trunk maintenance operations on page 410](#)
- [ADSL provisioning operations on page 411](#)
- [Line provisioning operations on page 411](#)
- [Line maintenance operations on page 411](#)
- [V5.2 provisioning operations on page 412](#)
- [Patching operations on page 413](#)
- [Automated upgrade operations on page 414](#)

Node provisioning operations (Sheet 1 of 2)

Command	User group				
	mgcadm	mgcrw	mgcmic	mgcsprov	mgcro
Disassociate a media gateway (MG) from a gateway controller (GWC)		x			
Associate an MG with a GWC		x			
Change the provisioning data for an MG		x			
Query site info					x
Query a GWC					x
Query an MG					x
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			

Node provisioning operations (Sheet 2 of 2)

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			
Perform a swact			x		
Firmware flash			x		
Assign/unassign services		x			

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Configure audit	x				
Run audit	x				
Get audit description					x
Get audit configuration					x
Get list of registered audits					x
Retrieve audit report					x
Take action on problem	x				

Carrier provisioning operations

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

Alarm operations

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

Internet transparency operations

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

Trunk provisioning operations

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

Trunk maintenance operations

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

ADSL provisioning operations

Command	User group				
	Inadm	Inrw	Inmtc	Insprov	Inro
Get subscriber					x
Add subscriber				x	
Add cross connection				x	
Modify subscriber				x	
Modify cross connection				x	
Delete subscriber				x	
Delete cross connection				x	

Line provisioning operations

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

Line maintenance operations

Command	User group				
	Inadm	Inrw	Inmtc	Insprov	Inro
Validate line using DN CLLI					x
Validate line using TID CLLI					x

Line maintenance operations

Command	User group				
	Inadm	Inrw	Inmtc	Insprov	Inro
Get line post info					X
Busy line			X		
Return line to service			X		
Force release line			X		
Installation busy line			X		
Cancel deload			X		
Get CM CLLI					X
Get endpoint state					X
GetGwlp					X
run all TL1 line test commands			X		

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	Inadm	Inrw	Inmtc	Insprov	Inro
Add, delete, modify V5.2 interface		X					X			
View all V5.2 interfaces					X					X
View signalling channel information entry, update list (V5Prov)					X					X
Add, modify, delete signalling channel information entry (V5Prov)		X					X			
View ringing cadence mapping, update list (V5Ring)					X					X

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, modify, delete ringing cadence mapping (V5Ring)		x					x			
View signalling characteristic profile, update list (V5Sig)					x					x
Add, delete, modify signalling characteristic profile (V5Sig)		x					x			
View carrier-to-interface and interface-to-carrier mappings					x					x

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
apply, remove, activate, deactivate, auditd, restart, and smartimage from the NPM GUI or CLUI	x				
Software image from MG 9000 Manager GUI		x			

Automated upgrade operations

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

Deleting local user accounts from an SSPFS-based server

Action

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

If you are centrally managing your user accounts, refer to procedure “Deleting users” in the Integrated EMS Security and Administration document, NN10336-611.

Note: All user account management activities, such as setting up users, removing users, and changing passwords, are performed on the Active server and then propagated from the Active to the Inactive server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Log in to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

5**ATTENTION**

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

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

Delete the user from the server by typing

userdel <**userid**>

and pressing the Enter key.

where

userid

is a variable for the user name

You have completed this procedure.

Changing a user password on an SSPFS-based server

Application

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

ATTENTION

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

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

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server
Note: In a two-server configuration, log in to the active server using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

- 5 Change the password for a specific user by typing
passwd -r files <userid>
and pressing the Enter key.
where
 userid
 is a variable for the user's login identification
- 6 When prompted, enter a password of at least three characters.
 Note: It is not recommended to set a password with an empty value. Use a minimum of three characters.
- 7 When prompted, enter the password again for verification.
You have completed this procedure.

Configuring OSSGate password control

Application

Use this procedure to configure OSSGate password control. When OSSGate password control is turned on, the password will not be echoed on the screen when logging in.

Prerequisites

You need root user privileges to perform this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Log in to the server by typing
 `> telnet <server>`
 and pressing the Enter key.
 where
 server
 is the IP address or host name of the CS 2000
 Management Tools server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing
 `$ su - root`
 and pressing the Enter key.
- 4 When prompted, enter the root password.

5 Execute the SESM configuration script by typing

```
# configure
```

and pressing the Enter key.

Example response

```
SESM configuration
```

- 1 - SESM common configuration (IP addresses, Market, CM CLLI)
- 2 - SESM database tools
- 3 - SESM related applications configuration (MG9K, LMM, CICM)
- 4 - SESM provisioning configuration
- 5 - SESM logging configuration (syslog, sesm debug log)
- 6 - view sesm configuration settings
- 7 - SESM refresh properties

```
X - exit
```

```
select -
```

6 Enter the number next to the “SESM provisioning configuration” option in the menu.*Example response*

```
SESM Provisioning Configuration
```

- 1 - XML Trunk Provisioning configuration
- 2 - OSSGate Provisioning configuration
- 3 - Office Provisioning Type configuration

```
X - exit
```

```
select -
```

7 Enter the number next to the “OSSGate Provisioning configuration” option in the menu.*Example response*

```
SESM OSSGate Provisioning Configuration
```

```
Enter the Primary Port OSSGate will use for telnet connections (default: 10023):
```

- 8** When prompted, press the Enter key to accept the default value for the primary port, or enter another value for the primary port if desired.

Example response

Enter the Secondary Port OSSGate will use for telnet connections (default: 11023):

- 9** When prompted, press the Enter key to accept the default value for the secondary port, or enter another value for the secondary port if desired.

Example response

Enter the OSSGate Timeout period, in seconds (default: 600):

- 10** When prompted, press the Enter key to accept the default value for the timeout period, or enter another value for the timeout period if desired.

Example response

Do you wish to have OSSGate Port Forwarding on for SSH [y/n]:

- 11** When prompted, indicate whether you want to have OSSGate port forwarding turned on for SSH.

Example response

Do you wish to turn on/off OSSGate Password Control option (when this option is turned on, OSSGate will not echo password on screen when logging into it) [default:off]:

- 12** When prompted, indicate whether you want to turn on OSSGate password control, or press the Enter key to accept the default value.

Example response

Primary Port: 10023
Secondary Port: 11023
Timeout: 600
Port Forwarding for SSH: no
Password Control: on

Are these information correct? (y or n):

- 13** When prompted, confirm the configuration by typing

y

and pressing the Enter key.

Example response

Updating the property files with changed values,
please wait...

Reloading the changed property values into
memory, please wait...

- 14** Exit each level of the SESM configuration to eventually return to the root directory level by typing

select - **x**

and pressing the Enter key.

You have completed this procedure.

Changing an expired root password on an SSPFS-based server

Application

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

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

ATTENTION

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

Prerequisites

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

Action

Perform the following steps to complete this procedure.

ATTENTION

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

At the server console

- 1 Log in to the server through the console (port A) using the root user ID and the expired root password.
- 2 When prompted, enter the old (expired) password.
- 3 When prompted, enter a password of at least three characters.

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

- 4 When prompted, enter the password again for verification.
You have completed this procedure.

Setting the Oracle Listener password on an SPFS-based server

Application

The Oracle Listener requires a password to perform most operations within the listener interactive command prompt. A password is required to perform operations such as stop or start services. This procedure demonstrates how to specify your current password.

Note: When the system is installed, the default Oracle Listener password is set to *oracle*. To change this default password, use procedure [Changing the Oracle Listener password on an SPFS-based server on page 426](#).

ATTENTION

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

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

At your workstation

- 1 Log in to the server by typing

> **telnet** <server>

and pressing the Enter key.

where

server

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

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

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the Oracle Listener application by typing

```
# lsnrctl
```

and pressing the Enter key.

Example response

```
Welcome to LSNRCTL, type "help" for information.
```

```
LSNRCTL>
```

6 Initiate the password setting by typing

```
LSNRCTRL> set password
```

and pressing the Enter key.

Example response

```
Password:
```

7 Type your current password at the prompt and press the Enter key.

Example response

```
The command completed successfully
```

```
You have completed this procedure.
```

Changing the Oracle Listener password on an SSPFS-based server

Application

The default password for the Oracle Listener is set to *oracle* during the installation of the Succession Server Platform Foundation Software (SSPFS). This procedure provides the steps to change the Oracle Listener password on an SSPFS-based server.

ATTENTION

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

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

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server
Note: In a two-server configuration, log in to the active server using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- 4 When prompted, enter the root password.
- 5 Access the Oracle Listener application by typing
`# lsnrctl`
and pressing the Enter key.
Example response:
Welcome to LSNRCTL, type "help" for information.
- 6 Initiate the password change by typing
`LSNRCTL> change_password`
and pressing the Enter key.
Example response
Old password:
- 7 When prompted, enter the old (current) password.
Example response
New password:
- 8 When prompted, enter the new password.
Example response
Reenter new password:
- 9 When prompted, enter the new password again to confirm it.
Example response
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=47.143.107.192) (PORT=1521)))
Password changed for LISTENER
The command completed successfully
- 10 Initiate the password setting by typing
`LSNRCTL> set_password`
and pressing the Enter key.
Example response
Password:
- 11 When prompted, enter the new password.
Example response
The command completed successfully

12 Save the new password by typing

```
LSNRCTL> save_config
```

and pressing the Enter key.

Example response

```
Connecting to  
(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)  
(HOST=47.143.107.192) (PORT=1521)))  
Saved LISTENER configuration parameters.  
Listener Parameter File  
/opt/oracle/product/8.1.7/network/admin/listener.ora  
Old Parameter File  
/opt/oracle/product/8.1.7/network/admin/listener.bak  
The command completed successfully
```

You have completed this procedure.

Configuring the Integrated EMS central security server in the network

Application

Use this procedure to configure and activate the Integrated Element Management System (EMS) central security server in the network. The Integrated EMS acts as a proxy to the central security administration system.

ATTENTION

Only one Integrated EMS central security server can be configured in the network.

ATTENTION

Reverting to the previous configuration of the server is not supported. A rollback of the Succession Server Platform Foundation Software (SSPFS) must be performed to revert the security server to its previous configuration.

ATTENTION

Migrating local user accounts on Integrated EMS security server

The procedures described in this section apply to upgrades from (I)SN06.2 to (I)SN08. User accounts managed by Integrated EMS (I)SN07 will be automatically migrated from the Integrated EMS Oracle database to the MFT NDS database when upgrading to Integrated EMS (I)SN08.

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the Integrated Element Management System (EMS) is already installed or upgraded on the server, and it is running Succession Server Platform Foundation Software (SSPFS) release (i)SN07 or greater

- an HTTPS certificate has been properly installed on the server prior to installing or upgrading the Integrated EMS. If required, refer to procedure [Installing or replacing an HTTPS certificate on an SSPFS-based server on page 608](#). The Integrated security server and SunONE component will be automatically configured during installation or upgrade to enable the secure SSL mode.

Action

Perform the following steps to complete this procedure.

- 1 Migrate the user accounts you want to centrally manage, from the local security database on the SSPFS-based server to the central administration system as follows:

Note 1: It is recommended to migrate all user accounts that exist on SSPFS-based servers to the central administration system with the following exceptions:

root, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, and oracle.

Note 2: If the central security administration application is a third-party application and not the Integrated EMS, follow the procedures in the third party documentation.
- 2 If the central administration system is the Integrated EMS, launch the Security Administration tool of the Integrated EMS, and add the user accounts you want to centrally manage. If required, refer to procedure “Adding new users” in the *Integrated EMS Security and Administration* document, NN10336-611.

Note: All users added through the Integrated EMS Security Administration tool, are by default assigned to the “succssn” user group for login access.
- 3 Delete the user accounts you just added to the Integrated EMS central security server.
 - a Telnet to the server by typing

 > **telnet** <server>

and pressing the Enter key.

where

 server
 is the IP address or host name of the SSPFS-based client server

b When prompted, enter the user ID and password for an account that was migrated to the Integrated EMS central security server.

c Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d When prompted, enter the root password.

e Delete the user account by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid

is a variable for the user name

Repeat this step for each user account you migrated to the Integrated EMS central security server.

4 Complete PAM and NSSwitch configuration as follows:

At installation or upgrade, the Integrated EMS replaces the existing PAM and NSSwitch configuration files (pam.conf and nsswitch.conf) with new PAM and NSSwitch configuration files that use the Integrated EMS security application. If the pam.conf or nsswitch.conf files had any special edits, you must re-edit the file to add those special edits.

You can use the Integrated EMS PAM and NSSwitch SPIs, which are pre-bundled with the Integrated EMS load, or you can use your own third-party PAM and NSSwitch SPIs. The Distributed Computing Environment (DCE) and the Lightweight Directory Access Protocol (LDAP) PAM and NSSwitch SPIs are the third-party PAM and NSSwitch SPIs that are supported. If required, refer to procedure [Configuring a third-party Pluggable Authentication Module on page 446](#).

- 5 Set up platform access for central account users. A user's home directory and shell profiles must be set up before a central account user can gain platform access. Refer to [Setting up platform access for central account users on page 443](#).
- 6 You have completed this procedure.

Configuring an SSPFS-based central security client

Application

Use this procedure to configure an SSPFS-based central security client to use the Integrated Element Management System (IEMS) central security server.

ATTENTION

You can revert to the previous configuration of the client server using procedure [Reverting the client server to its previous configuration on page 462](#).

In the event you want to reconfigure the central security client to use a new IEMS server IP, perform steps [2](#) and [3](#) of this procedure.

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the IEMS central security server is already configured and activated in the network (see procedure [Configuring the Integrated EMS central security server in the network on page 429](#), if required)
- perform this procedure on each SSPFS-based server that is not the IEMS central security server to activate centralized security

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Migrate the user accounts you want to centrally manage, from the local security database on the SSPFS-based client to the central administration system as follows:

Note 1: It is recommended to migrate all user accounts that exist on SSPFS-based servers to the central administration system with the following exceptions:

root, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, and oracle.

Note 2: If the central security administration application is a third-party application and not the IEMS, follow the procedures in the third party documentation.

- a If the central administration system is the IEMS, launch the Security Administration tool of the IEMS, and add the user accounts plus any additional required user groups you want to centrally manage. If required, refer to “Adding new users”, “Adding new groups”, and “Assigning a user to a group” in *IEMS Security and Administration*, NN10336-611.

Note: All users added through the IEMS Security Administration tool, are by default assigned to the *succssn* user group for login access.

- b Delete the user accounts you just added to the IEMS central security server.

Log in to the client server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

is the IP address or host name of the SSPFS-based client server

- c** When prompted, enter the user ID and password for an account that was migrated to the IEMS central security server.

- d** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- e** When prompted, enter the root password.

- f** Delete the user account by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid

is a variable for the user name

Repeat this step for each user account you migrated to the IEMS central security server.

- 2** Configure the IEMS security server address as follows:

- a** Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

Command Line Interface

1 - View

2 - Configuration

3 - Other

X - Exit

```
select -
```

- b** Enter the number next to the “Configuration” option in the menu.

Example response

Configuration

- 1 - NTP Configuration
- 2 - Apache Proxy Configuration
- 3 - DCE Configuration
- 4 - OAMP Application Configuration
- 5 - CORBA Configuration
- 6 - IP Configuration
- 7 - DNS Configuration
- 8 - Syslog Configuration
- 9 - Database Configuration
- 10 - NFS Configuration
- 11 - Bootp Configuration
- 12 - Restricted Shell Configuration
- 13 - Security Services Configuration
- 14 - Login Session
- 15 - Location Configuration
- 16 - Cluster Configuration
- 17 - Succession Element Configuration
- 18 - snmp_poller (SNMP Poller Configuration)

- X - exit

Select -

- c** Enter the number next to the “Security Services Configuration” option in the menu.

Example response

```
Security Services Configuration
1 - Socks Configuration
2 - IEMS Server Location Configuration
3 - PAM Configuration
```

```
x - exit
```

```
select -
```

- d** Enter the number next to the “IEMS Server Location Configuration” option in the menu.

Example response

```
IEMS Server Location Configuration
1 - iems_ip (Configure IEMS Server IP)
```

```
x - exit
```

```
select -
```

- e** Enter the number next to the “iems_ip” option in the menu.

Example response

```
===Executing "iems_ip"
```

```
Enter the IEMS Server IP Address (default
45.12.23.56):
```

- f** When prompted, enter the virtual IP address of the IEMS server, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter IEMS Fully Qualified Domain Name
(default :test3iems.us.nortel.com):
```

- g** When prompted, enter the Fully Qualified Domain Name (FQDN) of the IEMS server, or press the Enter key to accept the default value if one is specified.

Example response

```
IEMS IP: 45.12.23.56
IEMS Fully Qualified Domain
Name:test3iems.us.nortel.com
```

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

- h** Accept the IP address and FQDN you just entered by typing **ok** and pressing the Enter key.

Example response

```
=== "iems_ip" completed successfully
```

- i** Return to the Security Services Configuration menu, by typing

```
select - x
```

and pressing the Enter key.

Response

```
Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

x - exit

select -
```

- 3** Configure PAM and NNSwitch SPI configuration as follows:

- a** Enter the number next to the "PAM Configuration" option in the menu.

Example response

```
PAM Configuration
 1 - Central Security Client Configuration

x - exit

select -
```

- b** Enter the number next to the “Central Security Client Configuration” option in the menu.

Example response

```
Central Security Client Configuration
1 - pam_orig (Use Default PAM Configuration)
2 - pam_radius (Use Security Server)
3 - saml_passwd_conf (Configure saml
    password)
```

```
x - exit
```

```
select -
```

- c** Enter the number next to the “pam_radius” option in the menu.

Example response

```
===Executing "pam_radius"
```

```
Activating pam radius components
```

```
IEMS Security Server IP: 45.12.23.56
IEMS Fully Qualified Domain Name:
test3iems.us.nortel.com
Enter the Shared Secret (default:
nortelnetworks):
```

- d** When prompted, enter the shared secret, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter Radius Client Timeout (default: 12):
```

- e** When prompted, enter the Radius Client timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response

```
Enter SAML Server Protocol (default: https):
```

- f** When prompted, enter the SAML server protocol (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response

```
Enter SAML Server Port (default: 58081):
```

- g** When prompted, enter the SAML server port (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response

Enter SAML Connection Timeout (default: 20):

- h** When prompted, enter the SAML connection timeout (used to establish SAML connections with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response

Enter SAML Request Timeout (default: 10):

- i** When prompted, enter the SAML request timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response with default values

** Confirm Settings **

IEMS Security Server IP: 45.12.23.56
IEMS Server Domain Name:
test3iems.us.nortel.com
Shared Secret: nortelnetworks
Radius Client Timeout: 12
SAML server Protocol: https
SAML server Port: 58081
SAML Connection Timeout: 20
SAML Request Timeout: 10
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings

- j** Accept the PAM configuration update by typing

ok

and pressing the Enter key.

Example response

Configuring pam_radius

configuring nsssaml

Updating PAM Configuration to use IEMS
Security Server

Restarting name service daemon

=== "pam_radius" completed successfully

- k** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - **x**

and pressing the Enter key.

- l** If the pam.conf file had any special edits, you must re-edit the file to add those special edits.

- 4** To configure a saml password, from the menu prompt in step 3b above:

- a** enter the number next to the "saml_passwd_conf (Configure saml password)" option
- b** when prompted, enter the default SAML password (slisamadmin) or a new password you have chosen:

Example response

** Confirm Settings **

SAML Password: slisamadmin

Enter "ok" to commit changes

Enter "quit" to exit

Enter anything else to re-enter settings

ok

Configure Password Successful

=== "saml_passwd_conf" completed
successfully

- 5** Set up platform User Environment. Before enabling access to an SSPFS platform, and administrator must set up the user's environment on the platform. Refer to [Setting up platform access for central account users on page 443](#), for details on setting up user environment.
- 6** Set up platform access for central account users. A user's home directory and shell profiles must be set up before a central

account user can gain platform access. Refer to [Setting up platform access for central account users on page 443](#).

You have completed this procedure.

Setting up platform access for central account users

Application

Use this procedure to set up SSPFS platform access on the IEMS server for users that are centrally managed. In a two-server configuration, perform this procedure on both servers (active and inactive).

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the IEMS central security server is already configured and activated in the network (see procedure [Configuring the Integrated EMS central security server in the network on page 429](#))
- the IEMS central security client is already configured and activated in the network (see procedure [Configuring an SSPFS-based central security client on page 433](#))
- the user account group and its group must already be created
- users that are centrally managed, must have their environment set up on the SSPFS platform they have access to, to access that SSPFS platform through telnet, SSH, or other supported login utilities. Only perform this procedure if users are to be granted platform access.

Action

Perform the following steps to

At your workstation

- 1 Determine the user's numerical user ID (UID).
Note: If the central user account is managed by the IEMS security server, use procedure "Setting a user profile" in *IEMS Security and Administration*, NN10336-611, if required, to determine the user's numerical user ID (UID).
- 2 Log in to the SSPFS-based server the user has access to by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server the user has access to
- 3 When prompted, enter the user's ID and password.
- 4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Set up the user's home directory on the SSPFS-based server by typing

```
# mkdir /export/home/<username>
```

and pressing the Enter key.
where
username
is the user's login ID
- 7 Change the ownership of the user's home directory by typing

```
# chown <username> /export/home/<username>
```

and pressing the Enter key.
where
username
is the user's login ID

- 8 Copy the shell profiles from the system's shell skeleton directory by typing

```
# find . -depth -print | cpio -dump
/export/home/<username>
```

and pressing the Enter key.
where
username
is the user's login ID
- 9 Change the ownership of the user's shell profiles by typing

```
# chown <username> /export/home/<username>/.*
```

and pressing the Enter key.
where
username
is the user's login ID
- 10 Log out of the SSPFS-based server by typing

```
# exit
```

and pressing the Enter key.
You have completed this procedure.

Configuring a third-party Pluggable Authentication Module

Application

Use this procedure to configure a third-party Pluggable Authentication Module (PAM) on the Integrated Element Management System (EMS) central security server. Both of the following third-party Pluggable Authentication Modules (PAMs) are supported:

- [Distributed Computing Environment \(DCE\) PAM on page 447](#)
- [Lightweight Directory Access Protocol \(LDAP\) PAM on page 451](#)

Prerequisites

To perform this procedure, you need to have the root user ID and password for the Integrated EMS central security server, and either the DCE or LDAP prerequisites below depending on which third-party PAM you are configuring.

DCE prerequisites

The following prerequisites apply to DCE PAM:

- To configure the DCE PAM, you need administrative privileges for the DCE server.
- DCE must already be configured on the server. If required, refer to procedure “Configuring DCE on a Sun server” in the ATM/IP solution-level Configuration Management document, NN10409-500.

Note: For DCE to function correctly, DCE client 3.2 must be installed and patch PTF6 must be applied. Patches are available at the following link:

<https://www6.software.ibm.com/dl/dcesol/dcesol-p>.

LDAP prerequisites

To configure LDAP PAM, an LDAP server must already be configured with support for Solaris Native LDAP schema.

Note: Information on LDAP schema, is available at the following link:

<http://docs.sun.com/db?q=ldap+configuration+guide&p=doc%2F806-5580>

To configure IEMS Server as an LDAP Client, LDAP PAM and Nsswitch modules must be activated on the server.

Action

Perform the following steps to complete this procedure.

Distributed Computing Environment (DCE) PAM

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the Integrated EMS central security server on which you want to change the PAM
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Disable the Name Service Cache daemon as follows:
 - a Stop the Name Service Cache daemon

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

and pressing the Enter key.
 - b Move the “/etc/nscd.conf” file to a different location.
- 6 Add *dce* as the first option for the password and group in the “/etc/nsswitch.conf” file.
The entries would look similar to “passwd: dce files” and “group: dce files” after the change.
This enables the group information to come from DCE.
- 7 Enable the DCE naming service server by typing

```
# config.dce nsswitch
```

and pressing the Enter key.
- 8 Enable the DCE PAM (Pluggable Authentication Module) by typing

```
# config.dce pam
```

and pressing the Enter key.

- 9** Edit the `/etc/pam.conf` file as follows:
- a** Add `pam_dce` with sufficient setting as the first entry for “other auth”, “sesm auth”, and “secclient auth” iems entries in the “`/etc/pam.conf`” file as indicated:
 - change “other auth” to “other auth sufficient /usr/lib/security/\$ISA/pam_dce.so.1”
 - change “sesm auth” to “sesm auth sufficient /usr/lib/security/\$ISA/pam_dce.so.1 try_first_pass”
 - change “secclient auth” to “secclient auth sufficient /usr/lib/security/\$ISA/pam_dce.so.1”
 - b** Add `pam_dce` with sufficient setting as the first entry for “other account”, “sesm account”, and “secclient account” iems entries in the “`/etc/pam.conf`” file as indicated:
 - change “other account” to “other account sufficient /usr/lib/security/\$ISA/pam_dce.so.1”
 - change “sesm account” to “sesm account sufficient /usr/lib/security/\$ISA/pam_dce.so.1 try_first_pass”
 - change “secclient account” to “secclient account sufficient /usr/lib/security/\$ISA/pam_dce.so.1”
 - c** Add `pam_dce` with sufficient setting as the first entry for “other session”, “sesm session”, and “secclient session” iems entries in the “`/etc/pam.conf`” file as indicated:
 - change “sesm session” to “sesm session sufficient /usr/lib/security/\$ISA/pam_dce.so.1 try_first_pass”
 - change “secclient session” to “secclient session sufficient /usr/lib/security/\$ISA/pam_dce.so.1”

10 Add users and user groups to DCE as follows:

Note: For details on user groups, refer to procedure [Setting up local user accounts on an SSPFS-based server on page 402](#), if required.

- a Log in to DCE using the cell_admin user ID and password.
- b Add a user to DCE by typing

```
dcecp> user create <userid> -group succssn  
-password <password> -organization  
ossaps-users -mypwd <cell_admin_password>
```

and pressing the Enter key.

where

userid

is the user ID of the user you want to add

password

is the password for the user ID you want to add

cell_admin_password

is the password for cell_admin

Note: The above command is entered on one line.

- c Add the necessary user groups in DCE by typing

```
dcecp> group create <groupname>
```

and pressing the Enter key.

where

groupname

is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm, secadm
- trkrw, lnrw, mgcrw, mgrw, emsrw, secrw
- trksprov, lnspov, mgcsprov, mgsprov, emssprov, secprov
- trkmtc, lnmtc, mgcmte, mgmtc, emsmte, secmtc
- trkro, lnro, mgcro, mgro, emsro, secro

Note: Additional information on the Succession user groups is available in procedure [Setting up local user accounts on an SSPFS-based server on page 164](#).

- d** Add the new users to the new groups, one at a time, by typing

```
dcecp> group add <groupname> -member <userid>
```

and pressing the Enter key.

where

groupname

is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm, secadm
- trkrw, lnrw, mgcrw, mgrw, emsrw, secrw
- trksprov, lnspov, mgcsprov, mgsprov, emssprov, secprov
- trkmtc, lnmtc, mgcmte, mgmtc, emsmte, secmtc
- trkro, lnro, mgcro, mgro, emsro, secro

userid

is the user ID of a new user

- e** Verify the user was added by typing

```
dcecp> group list <groupname>
```

and pressing the Enter key.

where

groupname

is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm, secadm
- trkrw, lnrw, mgcrw, mgrw, emsrw, secrw
- trksprov, lnspov, mgcsprov, mgsprov, emssprov, secprov
- trkmtc, lnmtc, mgcmte, mgmtc, emsmte, secmtc
- trkro, lnro, mgcro, mgro, emsro, secro

- f Activate the new user by typing

```
dcecp> acct modify -acctvalid yes <userid>
```

and pressing the Enter key.

where

userid

is the user ID of a new user

You have completed this procedure.

Note: When the DCE authentication mechanism is selected, you must use the UNIX passwd command with the “-r” option to specify a repository. For example, if you want to change the password for a local UNIX user, the command is “passwd -r files <userid>.”

Lightweight Directory Access Protocol (LDAP) PAM

At the LDAP server

- 1 Add users and user groups to LDAP server as follows:

Note 1: For details on user groups, refer to procedure [Setting up local user accounts on an SSPFS-based server on page 402](#), if required.

Note 2: To configure LDAP Security, an LDAP server must be configured with support for Solaris Native LDAP schema and Proxy Authentication. Consult your LDAP server manual for instructions to configure the LDAP server to support Solaris Native LDAP schema.

- a Log in to the LDAP server.
- b Add the necessary user groups to the LDAP server. Consult the LDAP server instructions to add the 25 Succession user groups to the LDAP server.

The user groups are listed below with their corresponding group ID.

- succssn:105
- trkadm:1001, trkrw:1002, trksprov:1003, trkmtc:1004, trkro: 1005
- lnadm:1006, lnrw:1007, lnsprov:1008, lnmtc:1009, lnro:1010
- mgcadm:1011, mgcrw:1012, mgcsprov:1013, mgcmtc:1014, mgcro:1015
- mgadm:1016, mgrw:1017, mgsprov:1018, mgmtc:1019, mgro:1020
- emsadm:1021, emsrw:1022, emssprov:1023, emsmtc:1024, emsro:1025
- secadm:1026, secrw: 1027, secprov: 1028, secmtc: 1029, secro: 1030

Below is a sample ldif file to add the “succssn” group:

```
dn: cn=succssn,ou=group,dc=labnet,dc=us
dc=nortel,dc=com,o=internet
changetype: add
cn:succssn
gidnumber: 105
memberuid: kcaudill
memberuid: ferreira
objectclass: top
objectclass: posixGroup
```

Note: Consult your LDAP server manual for information on loading data into the directory server.

- c Add users to the LDAP server, and associate them to user groups. Consult your LDAP server instructions to add users to the LDAP server and associate them to usergroups.

Below is a sample ldif file to add a user:

```
dn: uid=kcaudill,ou=people,dc=us,dc=nortel,dc=com
cn: kelly Caudill
givenname: Kelly
sn: Caudill
gidnumber: 105
homedirectory: /tmp
uidnmuber: 10002
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: posixaccount
objectclas: account
objectclass: shadowwaccount
uid: kcaudill
shadowlastchange: 6445
loginshell: /bin/ksh
gecos: Kelly Caudill
userpassword: mypassword
```

Note: Consult your LDAP server manual for information on loading data into the directory server.

At your workstation

- 2 Log in to the Integrated EMS server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the Integrated EMS central security server on which you want to change the PAM
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Save a backup copy of the nsswitch.conf file, which is located in the /etc directory.
- 7

ATTENTION

The *ldapclient* command reconfigures the nsswitch.conf file. It is strongly recommended that you make a backup of nsswitch.conf before executing the *ldapclient* command, and then restore the backup nsswitch.conf file after the *ldapclient* command completes.

Configure the Solaris Native LDAP client and set up proxy authentication on the client using the *ldapclient* command.

Note: Information on the *ldapclient* command, is available at the following link:

<http://docs.sun.com/db?q=ldap+configuration+guide&p=doc%2F806-5580>

- 8 Replace the nsswitch.conf file with the backup copy of the nsswitch.conf file.
- 9 Edit the /etc/nsswitch.conf file as follows:
 - a Add “ldap” as the first option for the password and group.
The entries will look similar to “passwd: ldap files” and “group: ldap files” after the change.
This enables the group information to come from LDAP.

- 10** Restart the name service daemon as follows:
- a** # /etc/init.d/nsed stop
 - b** # /etc/init.d/nsed start

- 11** Edit the `/etc/pam.conf` file to include LDAP entries as follows:
- a** Add `pam_ldap` with sufficient setting as the first entry for “other auth”, “sesm auth”, and “secclient auth” iems entries in the “`/etc/pam.conf`” file as indicated:
 - change “other auth” to “other auth sufficient
`/usr/lib/security/$ISA/pam_ldap.so.1`”
 - change “sesm auth” to “sesm auth sufficient
`/usr/lib/security/$ISA/pam_ldap.so.1 try_first_pass`”
 - change “secclient auth” to “secclient auth sufficient
`/usr/lib/security/$ISA/pam_ldap.so.1`”
 - b** Add `pam_ldap` with sufficient setting as the first entry for “other account”, “sesm account”, and “secclient account” iems entries in the “`/etc/pam.conf`” file as indicated:
 - change “other account” to “other account sufficient
`/usr/lib/security/$ISA/pam_ldap.so.1`”
 - change “sesm account” to “sesm account sufficient
`/usr/lib/security/$ISA/pam_ldap.so.1 try_first_pass`”
 - change “secclient account” to “secclient account
sufficient `/usr/lib/security/$ISA/pam_ldap.so.1`”
 - c** Add `pam_ldap` with sufficient setting as the first entry for “other session”, “sesm session”, and “secclient session” iems entries in the “`/etc/pam.conf`” file as indicated:
 - change “other session” to “other session sufficient
`/usr/lib/security/$ISA/pam_ldap.so.1`”
 - change “sesm session” to “sesm session sufficient
`/usr/lib/security/$ISA/pam_ldap.so.1 try_first_pass`”
 - change “secclient session” to “secclient session
sufficient `/usr/lib/security/$ISA/pam_ldap.so.1`”

You have completed this procedure.

Note: When the LDAP authentication mechanism is selected, you must use the UNIX `passwd` command with the `-r` option to specify a repository. For example, if you want to change the password for a local UNIX user, the command is “`passwd -r files <userid>.`”

Replacing HTTPS certificate on security server for SunOne component

Application

Use this procedure to make the SunOne component use the new server certificate to run in secure mode on the central security server and central security clients.

Note: The activation of SunOne SSL mode is now automatic (part of install/upgrade).

Use one of the methods below according to your office configuration:

- [Simplex configuration \(one server\) on page 457](#)
- [High-availability configuration \(two servers\) on page 459](#)

Prerequisites

An HTTPS certificate must already be installed on the Integrated Element Management System (IEMS) server. If required, refer to procedure [Installing or replacing an HTTPS certificate on an SSPFS-based server on page 608](#) to install the Apache server's certificate.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the Integrated EMS server on which you want to configure the security SunOne component
- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Reconfigure the SunOne IS client environment on the system to use SSL as follows:
 - a Change directory to the configuration script by typing

```
# cd /opt/nortel/applications/security/  
current_slisext/swmgmt/bin
```

and pressing the Enter key.
Note: The above command is entered on one line.
 - b Execute the configuration script by typing

```
# ./configure_slisext.sh -ssl
```

and pressing the Enter key.
The above command reconfigures the SunOne IS client environment on the central security server to use SSL.
- 6 Restart the Web Server as follows:
 - a Stop the Web Server by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.
 - b Start the Web Server by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.
- 7 Restart the Web Services as follows:
 - a Stop Web services by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.
 - b Start Web Services by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

- 8 Restart the Radius server as follows:
 - a Stop the Radius server by typing

```
# servstop RADSVR
```

and pressing the Enter key.
 - b Start the Radius server by typing

```
# servstart RADSVR
```

and pressing the Enter key.You have completed this procedure.

High-availability configuration (two servers)

At your workstation

- 1 Log in to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the Active Integrated EMS server on which you want to configure the security SunOne component
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Reconfigure the SunOne IS client environment on the Active server to use SSL as follows:
 - a Change directory to the configuration script by typing

```
# cd /opt/nortel/applications/security/  
current_slisext/swmgmt/bin
```

and pressing the Enter key.

Note: The above command is entered on one line.

- b Execute the configuration script by typing

```
# ./configure_slisext.sh -ssl
```

and pressing the Enter key.
The above command reconfigures the SunOne IS client environment on the Active central security server to use SSL.
- 6 Initiate a failover by typing

```
# swact /Y
```

and pressing the Enter key.
- 7 Reconfigure the SunOne IS client environment on the newly Active server to use SSL as follows:
 - a Change directory to the configuration script by typing

```
# cd /opt/nortel/applications/security/  
current_slisext/swmgmt/bin
```

and pressing the Enter key.
Note: The above command is entered on one line.
 - b Execute the configuration script by typing

```
# ./configure_sspfs_slisext.sh -ssl
```

and pressing the Enter key.
The above command reconfigures the SunOne IS client environment on the Active central security server to use SSL.
- 8 Restart the Web Server on the newly Active server as follows:
 - a Stop the Web Server by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.
 - b Start the Web Server by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.

- 9 Restart the Radius server on the newly Active server as follows:
 - a Stop the Radius server by typing
servstop RADSVR
and pressing the Enter key.
 - b Start the Radius server by typing
servstart RADSVR
and pressing the Enter key.
- 10 Restart Web Services on the newly Active server as follows:
 - a Stop Web services by typing
servstop WEBSERVICES
and pressing the Enter key.
 - b Start Web Services by typing
servstart WEBSERVICES
and pressing the Enter key.

You have completed this procedure.

Reverting the client server to its previous configuration

Application

Use this procedure if you configured an SSPFS-based central security client to use the Integrated Element Management System (EMS) central security server, but want to revert to its previous configuration, which is not to use the Integrated EMS central security server.

Prerequisites

To perform this procedure, you need to have root user privileges.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server on which you want to revert the configuration
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Configure PAM as follows:
 - a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

select -
```

- b** Enter the number next to the “Configuration” option in the menu.

Example response

Configuration

- 1 - NTP Configuration
- 2 - Apache Proxy Configuration
- 3 - DCE Configuration
- 4 - OAMP Application Configuration
- 5 - CORBA Configuration
- 6 - IP Configuration
- 7 - DNS Configuration
- 8 - Syslog Configuration
- 9 - Database Configuration
- 10 - NFS Configuration
- 11 - Bootp Configuration
- 12 - Restricted Shell Configuration
- 13 - Security Services Configuration
- 14 - Login Session
- 15 - Location Configuration
- 16 - Cluster Configuration
- 17 - Succession Element Configuration
- 18 - snmp_poller (SNMP Poller Configuration)

- X - exit

Select -

- c** Enter the number next to the “Security Services Configuration” option in the menu.

Example response

Security Services Configuration

- 1 - Socks Configuration
- 2 - IEMS Server Location Configuration
- 3 - PAM Configuration

x - exit

select -

- d** Enter the number next to the “PAM Configuration” option in the menu.

Example response

```
PAM Configuration
 1 - Central Security Client Configuration

x - exit

select -
```

- e** Enter the number next to the “Central Security Client Configuration” option in the menu.

Example response

```
Central Security Client Configuration
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)

x - exit

select -
```

- f** Enter the number next to the “pam_orig” option in the menu.

Example response

```
===Executing "pam_orig"

Switching to original PAM configuration

Enter "ok" to continue
Enter anything else to exit
```


- g** Accept to switch to the original PAM configuration by typing
ok
and pressing the Enter key.

Example response

```
Stopping pam_radius
```

```
Deconfiguring pam_radius
```

```
=== "pam_orig" completed successfully
```

- h** Exit each menu level of the command line interface to eventually exit the command line interface , by typing
`select - x`
and pressing the Enter key.

- 6** Re-provision the user accounts in Unix. In a two-server configuration, reprovision the user accounts on the active server. If required, refer to procedure [Setting up local user accounts on an SSPFS-based server on page 402](#).

You have completed this procedure.

Configuring the Single Sign-On token

Application

Use this procedure to configure the values for the Single Sign-On (SSO) token and view the current SSO values. The SSO values are the time the Single Sign-On (SSO) token can remain idle before it becomes invalid, and the time the SSO token id can be used before it expires.

The SSO capability enables users to access multiple network elements, applications, and features from a single login session.

Prerequisites

You need root user privileges.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```


and pressing the Enter key.
where
server
is the IP address or host name of the SPFS-based server
on which you want to configure the SSO token
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```


and pressing the Enter key.
- 4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
```

```
1 - View
```

```
2 - Configuration
```

```
3 - Other
```

```
X - exit
```

```
select -
```

6 Enter the number next to the “Configuration” option in the menu.*Example response*

```
Configuration
```

```
1 - NTP Configuration
```

```
2 - Apache Proxy Configuration
```

```
3 - DCE Configuration
```

```
4 - OAMP Application Configuration
```

```
5 - CORBA Configuration
```

```
6 - IP Configuration
```

```
7 - DNS Configuration
```

```
8 - Syslog Configuration
```

```
9 - Database Configuration
```

```
10 - NFS Configuration
```

```
11 - Bootp Configuration
```

```
12 - Restricted Shell Configuration
```

```
13 - Security Services Configuration
```

```
14 - Login Session
```

```
15 - Location Configuration
```

```
16 - Cluster Configuration
```

```
17 - Succession Element Configuration
```

```
18 - snmp_poller (SNMP Poller Configuration)
```

```
X - exit
```

```
Select -
```

- 7** Enter the number next to the “Succession Element Configuration” option in the menu.

Example response

```
Succession Element Configuration
1 - RADSVR Application Configuration
2 - S1IS Application Configuration
3 - RESMON Application Configuration
4 - NPM Application Configuration
5 - PSE Application Configuration
6 - OMPUSH Application Configuration
```

X - exit

select -

- 8** Enter the number next to the “S1IS Application Configuration” option in the menu.

Example response

```
S1IS Application Configuration
1 - LIST_TOKEN_VALUES (List the current session
and idle times set in Sun One.)
2 - TOKEN_ADMIN (Change the token idle and
session expiry time)
```

X - exit

select -

If you want to	Do
view the current SSO values	step 9
configure SSO values	step 10

- 9** Enter the number next to the “LIST_TOKEN_VALUES” option in the menu.

Example response

```
=== Executing "LIST_TOKEN_VALUES"
```

```
30 # Idle time of the token
```

```
365 # Session time of the token
```

```
=== "LIST_TOKEN_VALUES" completed successfully
```

If you	Do
want to re-configure SSO values	step 10
do not want to re-configure SSO values	you have completed this procedure

- 10** Enter the number next to the “TOKEN_ADMIN” option in the menu.

Example response

```
=== Executing "TOKEN_ADMIN"
```

```
Enter the new Token Idle Time:
```

- 11** When prompted, enter the desired value for the idle time of the SSO token, which is the time the token can remain idle before it becomes invalid. The default value is 30 minutes.

```
Enter the new Token Session Time:
```

Example response

- 12** When prompted, enter the desired value for the duration of the SSO token id, which is the time the token id can be used before it expires. The default value is 525600 minutes (365 days).

Example response

```
Enter the new Token Idle Time:60
```

```
Enter the new Token Session Time: 182
```

```
Success 0: Successfully completed.
```

```
NOTE: Operation succeeded.
```

```
=== "TOKEN_ADMIN" completed successfully
```

- 13** Exit each menu level of the command line interface to eventually exit the command line interface, by typing
`select - x`
and pressing the Enter key.
You have completed this procedure.

Mapping of Integrated EMS devices to authorization domains

The following table lists the authorization domain that devices in Integrated EMS use. For a description of user groups, see [Setting up local user accounts on an SSPFS-based server](#)

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

- [MGC and MG user groups](#)
- [TRK user groups](#)
- [EMS user groups](#)
- [LN user groups](#)
- [SEC user groups](#)

MGC and MG user groups

Command	User group									
	mgcadm	mgcsprov	mgcrw	mgcmte	mgcro	mgadm	mgspov	mgrw	mgmtc	mgro
CS 2000 Core										
Launch MAPCI Session	x	x	x	x	x					
GWC (GWC network element)										
GWC Unit Manager	x	x	x	x	x					
Launch Command Line	x									
Launch TMM (see Note 1)	x	x	x	x	x					
Launch LMM (see Note 2)	x	x	x	x	x					
Launch NPM (see Note 3)	x	x	x	x	x					
Launch CS 2000 tools (see Note 4)	x	x	x	x	x					
MG 9000 network element										
Update Radius Secret (see Note 5)						x	x	x	x	x
SAM21										
Launch SCU subnet	x	x	x	x	x					
Launch SCU manager	x	x	x	x	x					

MGC and MG user groups

Command	User group									
	mgcadm	mgcsprov	mgcrw	mgcmte	mgcro	mgadm	mgspov	mgrw	mgmtc	mgro
GWC-CARD / CICMEM-CARD / CICM-CARD / 3PC-CARD / HLR-CARD / MC-CARD / USP-CARD / KDC-CARD / SAM21-UNIT										
Launch SAM21 Card View	x	x	x	x	x					
UAS network element										
Command Line	x	x	x	x	x					
NE-USP / USP										
Launch USP Manager	x	x	x	x	x					
Command Line	x	x	x	x	x					
Passport 8600 (now known as Ethernet Routing Switch 8600)										
PP8600 Device Manager (Launch)	x	x	x	x	x					
PP8600 Device Manager (Configure)	x	x	x	x	x					
Command Line	x	x	x	x	x					
Update Radius Secret (see Note 5)	x	x	x	x	x					
Media Server 2000										
Configure MS2000 Automated INI Backup						x	x	x	x	x
Config and Maintenance Tool						x	x	x	x	x
STORM										
Launch Command Line	x	x	x	x	x					
Launch STORM Manager	x	x	x	x	x					
Session Server NE and Units										
Launch Session Server	x	x	x	x	x					
Command Line	x	x	x	x	x					
Media Application Server										
MAS Manager(P) (Configure)						x	x	x	x	x
MAS Manager(P) (Launch)						x	x	x	x	x

MGC and MG user groups

Command	User group									
	mgcadm	mgcsprov	mgcrw	mgcmte	mgcro	mgadm	mgspov	mgrw	mgmtc	mgro
CALL-AGENT-CORE										
Launch MAPCI Session	x	x	x	x	x					
CALL-AGENT-PLAT										
Call Agent Platform Command Line	x	x	x	x	x					
NE-CICM / CICM-Node										
Launch CICM Manager	x	x	x	x	x					
VSP										
Client-Server IP provisioning	x	x	x	x	x	x	x	x	x	x
MDM Mgr GUI	x	x	x	x	x	x	x	x	x	x
Media Gateway 7480/15000										
Client-Server IP provisioning	x	x	x	x	x	x	x	x	x	x
MDM Manager GUI	x	x	x	x	x	x	x	x	x	x
Legacy MDM tools	x	x	x	x	x	x	x	x	x	x
Command Line	x	x	x	x	x	x	x	x	x	x
Update Radius secret (see Note 5)	x	x	x	x	x	x	x	x	x	x
Passport 20000										
Client-Server IP provisioning	x	x	x	x	x	x	x	x	x	x
MDM Manager GUI	x	x	x	x	x	x	x	x	x	x
Legacy MDM tools	x	x	x	x	x	x	x	x	x	x
Command Line	x	x	x	x	x	x	x	x	x	x
MSS - Unknown										
Client-Server IP Provisioning	x	x	x	x	x	x	x	x	x	x
MDM Manager GUI	x	x	x	x	x	x	x	x	x	x
Command Line	x	x	x	x	x	x	x	x	x	x
APPLN-APS										
APS Manager (CMT)	x	x	x	x	x					
APS Audio Configuration Tool	x	x	x	x	x					
MTX / MSC / HLR / TRI										

MGC and MG user groups

Command	User group									
	mgcadm	mgcsprov	mgcrw	mgcmte	mgcro	mgadm	mgspov	mgrw	mgmtc	mgro
Launch CEM (see Note 6)					x					
IMS/CSE / Media Proxy										
Launch MCP System Management Console						x	x	x	x	x
Command Line						x	x	x	x	x
Launch MCS Client (P) (Configure)						x	x	x	x	x
Launch MCS Client (P) (Launch)						x	x	x	x	x
APPLN-OSSGate										
APPLN-OSSGate						x	x	x	x	x
Launch OSSGate						x	x	x	x	x
Launch BPT Servlet						x	x	x	x	x
Launch BPT Command Line						x	x	x	x	x
MCS Manager										
Launch MCS Client (P) (Configure)	x	x	x	x	x					
Launch MCS Client (P) (Launch)	x	x	x	x	x					
Launch MCP System Management Console	x	x	x	x	x					
Launch MCS Client (P) (Launch)	x	x	x	x	x					
MCS SM Unit / FPM-UNIT										
MCP System Manager Console	x	x	x	x	x					
Command Line	x	x	x	x	x					
EMS-FPM-Mgr										
Launch MCP System Management Console	x	x	x	x	x					

MGC and MG user groups

Command	User group									
	mgcadm	mgcsprov	mgcrw	mgcmte	mgcro	mgadm	mgspov	mgrw	mgmtc	mgro
Command Line	x	x	x	x	x					
Note 1: To launch TMM on the GWC network element, the user must be associated with an MGC user group and a TRK user group. Note 2: To launch LMM on the GWC network element, the user must be associated with an MGC user group and an LN user group. Note 3: To launch NPM on the GWC network element, the user must be associated with an MGC user group and an EMS user group. Note 4: To launch CS 2000 tools on a GWC network, the user must be associated with an MGC user group and an EMS user group. Note 5: To update Radius secret also requires SECADM* privileges. Note 6: To launch CEM requires MGCRO. Only MGCRO can launch CEM. MGC* cannot launch CEM.										

TRK user groups

Command	User group				
	trkadm	trksprov	trkrw	trkmtc	trkro
GWC (GWC network element)					
Launch TMM (see Note)	x	x	x	x	x
APPLN-TMM					
Trunk Maintenance Manager	x	x	x	x	x
APPLN-OSSGate					
Launch OSSGate	x	x	x	x	x
Launch BPT Servlet	x	x	x	x	x
Note: To launch TMM on the GWC network element, the user must be associated with an MGC user group and a TRK user group.					

EMS user groups

Command	User group				
	emsadm	emssprov	emsrw	emsmcprov	emso
EMS-APS-Mgr (APS Manager)					
APS Manager	x	x	x	x	x
CS 2000 Manager (EMS-CS2K-Mgr)					
Launch Core Manager Maintenance	x	x	x	x	x
Launch MAPCI session	x	x	x	x	x
Update Radius Secret (see Note)	x	x	x	x	x
EMS-GWC-Mgr (GWC Manager)					
GWC Manager (CMT)	x	x	x	x	x
GWC Manager Network View	x	x	x	x	x
MG 9000 Manager					
MG 9000 Manager	x	x	x	x	x
IPSec Tool	x	x	x	x	x
EMS-SAM21-Mgr					
SAM21 Manager GUI	x	x	x	x	x
EMS-UAS-Mgr (UAS Manager)					
UAS Manager (CMT)	x	x	x	x	x
CICM Manager (EMS-CICM-Mgr/CICM-Mgr-Node)					
Launch CICM Manager	x	x	x	x	x
Launch Command Line	x	x	x	x	x
MCS Manager					
Launch MCS Client (P) (Configure)	x	x	x	x	x
Launch MCS Client (P) (Launch)	x	x	x	x	x
Launch MCP System Management Console	x	x	x	x	x
Launch MCS Client (P) (Launch)	x	x	x	x	x
MCS SM Unit / FPM-UNIT					
MCP System Manager Console	x	x	x	x	x
Command Line	x	x	x	x	x

EMS user groups

Command	User group				
	emsadm	emssprov	emsrw	emsmcprov	emsro
EMS-FPM-Mgr					
Launch MCP System Management Console	x	x	x	x	x
Command Line	x	x	x	x	x
MDM-Mgr-UNIT					
Update Radius secret (see Note)	x	x	x	x	x
EMS-MDM-Mgr					
Client-Server IP provisioning	x	x	x	x	x
MDM Manager GUI	x	x	x	x	x
Legacy MDM Tools	x	x	x	x	x
Change MDM Centralized Account	x	x	x	x	x
Command Line	x	x	x	x	x
Partition NEs	x	x	x	x	x
MDM Operator Client GUI	x	x	x	x	x
Update Radius secret (see Note)	x	x	x	x	x
PLAT-SSPFS					
Command Line	x	x	x	x	x
Servman Applications Status	x	x	x	x	x
Swact Cluster	x		x		
Restart SSPFS	x		x		
Update Radius secret (see Note)	x	x	x	x	x
SSPFS-UNIT					
Command Line	x	x	x	x	x
Servman Applications Status	x	x	x	x	x
Swact Cluster	x	x	x	x	x
Restart SSPFS	x	x	x	x	x
PLAT-SDM					
Command Line	x	x	x	x	x

EMS user groups

Command	User group				
	emsadm	emssprov	emsrw	emsmcprov	emsro
Update Radius secret (see Note)	x	x	x	x	x
PLAT-MDM					
Command Line	x	x	x	x	x
Update Radius secret (see Note)	x	x	x	x	x
APPLN-QOS					
Launch Command Line	x	x	x	x	x
APPLN-NPM					
Command Line	x	x	x	x	x
Note: To update Radius secret, the user also requires SECADM* privileges.					

LN user groups

Command	User group				
	Inadm	Inspv	Inrw	Inmtc	Inro
GWC (GWC NE)					
Launch LMM (see Note)	x	x	x	x	x
APPLN-LMM					
Line Maintenance Manager	x	x	x	x	x
APPLN-OSSGate					
Launch OSSGate	x	x	x	x	x
Launch BPT Servlet	x	x	x	x	x
Launch BPT Command Line	x	x	x	x	x
Note: To launch LMM on the GWC network element, the user must be associated with an MGC user group and an LN user group.					

SEC user groups

Command	User group				
	secadm	secsprov	secrw	secmtc	secro
CS2k Manager (EMS-CS2K-Mgr)					
Update Radius Secret (also requires EMS* privileges)	x				
MG 9000 NE					
Update Radius Secret (also requires MG* privileges)	x				
Passport 8600 (now known as Ethernet Routing Switch 8600)					
Update Radius Secret (also requires MGC* privileges)	x				
VSP					
Update Radius Secret (also requires MGC* or MG* privileges)	x				
MDM-Mgr-UNIT					
Update Radius Secret (also requires EMS* privileges)	x				
EMS-MDM-Mgr					
Update Radius Secret (also requires EMS* privileges)	x				
Media Gateway 7480/15000					
Update Radius Secret (also requires MGC* or MG* privileges)	x				
PLAT-SSPFS					
Update Radius Secret (also requires EMS* privileges)	x				
PLAT-MDM					
Update Radius Secret (also requires EMS* privileges)	x				

Security Token Administration GUI overview

Integrated EMS Security Token Administration GUI can be used to:

- view user session (or token) information
- terminate user sessions

Integrated EMS Security Token Administration GUI displays all of the user sessions that are available to the Identity Server and displays the expiration time for each session. See [List of valid tokens window](#).

Integrated EMS Security Token Administration GUI displays the following:

- the user sessions that are available
- the amount of time (minutes) remaining for a user session
- the maximum time (minutes) before the session expires after which the user session must re authenticate to regain access
- the time (minutes) that have expired while the user session is idle
- the maximum time (minutes) that a user session can remain idle

For details on how to log in to the Integrated EMS Security Token Administration GUI, see [Launching the Integrated EMS Security Token Administration GUI](#).

List of valid tokens window

Terminate

Logout

Filter

List of valid tokens

	Type	User	Idle Time	Max Idle Time	Time Left	Max Session Time
☐	3-use	amadmin	0	5	525592	525600
☐	3-use	amadmin	0	5	525593	525600
☐	TTL	amadmin	0	5	525589	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	amadmin	0	5	525592	525600
☐	2-use	user1	0	5	525598	525600
☐	TTL	user1	2	5	525595	525600
☐	3-use	amadmin	1	5	525592	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	amadmin	0	5	525593	525600
☐	3-use	amadmin	0	5	525592	525600

Launching the Integrated EMS Security Token Administration GUI

Use this procedure to launch the Integrated EMS Security Token Administration GUI.

Prerequisites

To perform this procedure, the user account you are using to log into the Integrated EMS Security Token Administration GUI must be set up on the Integrated EMS server and have administration privileges.

To verify that the user account is set up, see the procedure for "Listing all groups and users" in *Integrated EMS Security and Administration*, NN10336-611.

Action

At a web browser

- 1 Launch the Integrated EMS Security Token Administration GUI using a URL in the format of:

https://hostname:8443/tokenadmin

The Token Management window is displayed as in the following figure.

Token Management window

Token Management

Please provide your Identity Server account information. A user with admin privilege is needed in order to perform token management.

User Name	
Password	
Login	Reset

- 2 Enter your user name in the User Name field.
- 3 Enter your password in the Password field.
- 4 Click Login. The List of valid tokens window opens.

Terminate

Logout

Filter

List of valid tokens

	Type	User	Idle Time	Max Idle Time	Time Left	Max Session Time
☐	3-use	arnadmin	0	5	525592	525600
☐	3-use	arnadmin	0	5	525593	525600
☐	TTL	arnadmin	0	5	525589	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	arnadmin	0	5	525592	525600
☐	2-use	user1	0	5	525598	525600
☐	TTL	user1	2	5	525595	525600
☐	3-use	arnadmin	1	5	525592	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	arnadmin	0	5	525593	525600
☐	3-use	arnadmin	0	5	525592	525600

- 2 Enter a string in the Filter field.

Note: You can enter any character in the Filter field, including a meta-character (*).

Example

To list all users whose names start with am, enter am*.

To list all users whose names end with min, enter *min.

To list all users whose names contain ad, enter *ad*.

- 3 Click Filter to refresh the List of valid tokens window and view the list of valid tokens using the value in the Filter field.

Terminating a user session

Use this procedure to terminate a user session.

Prerequisites

You require a user account with administration privileges to perform this task.

Action

At the Integrated EMS Security Token Administration GUI

- 1 Log in to the Integrated EMS Security Token Administration GUI.
 - a Open the Token Management dialog box. See [Launching the Integrated EMS Security Token Administration GUI](#).
 - b Enter your user name in the User Name field.
 - c Enter your password in the Password field.
 - d Click Login. The List of valid tokens window opens.

Terminate Logout Filter

List of valid tokens

	Type	User	Idle Time	Max Idle Time	Time Left	Max Session Time
☐	3-use	amadmin	0	5	525592	525600
☐	3-use	amadmin	0	5	525593	525600
☐	TTL	amadmin	0	5	525589	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	amadmin	0	5	525592	525600
☐	2-use	user1	0	5	525598	525600
☐	TTL	user1	2	5	525595	525600
☐	3-use	amadmin	1	5	525592	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	amadmin	0	5	525593	525600
☐	3-use	amadmin	0	5	525592	525600

- 2 Select the appropriate check boxes to select the sessions that you want to terminate.
- 3 Click Terminate Session.

The List of valid tokens window is updated with the list of valid tokens.

Health Monitors overview

If the Central Security Server's framework components fail, no security clients can access security services provided by the Integrated EMS Central Security Server. From (I)SN08, smart health monitors are provided to ensure the crucial security components are not dead or hung. In such situations, the failed components will be automatically restarted. There are three health monitors included on the Integrated EMS server.

- Sun Identity Server health monitor
- Radius Server health monitor
- PAM login servlet health monitor

The health monitors are automatically started by the system after the monitored process starts and are disabled when the monitored process is stopped.

Sun Identity Server health monitor

The identity server health monitor checks the health of the Sun Identity Server with the following three tests:

- Attempts to login with the user 'unknown'. This user should not be in the system and the login should fail with the proper return values from the server to indicate the server is still functioning.
- Performs a policy check with a system user. The policy test should succeed and indicate that the system user was able to login and perform the policy check.
- Confirms that the nsswitch configuration of the server works and the group 'secadm' can be retrieved through a query to nsswitch.

Note: When any test fails a customer log, EMSS 314, is generated and the health monitor restarts the Identity Server process group automatically. For details of this log, see *Succession Fault Management Logs Reference*, NN10275-909.

Radius Server health monitor

The Radius Server attempts to log in through the Radius Server using an invalid user name and password. The Radius Server should reply to a client with a message to indicate that the login failed. When the test fails, a customer log, EMSS 313, is generated. The Radius Server health monitor restarts the RADSVR process group automatically. For details of this log, see *Succession Fault Management Logs Reference*, NN10275-909.

PAM Login Servlet health monitor

The PAM login servlet health monitor attempts to retrieve the following URL:

https://<hostname>:8443/pamlogin/servlet/pamlogin?ReqType=Unknown

If this fails, the health monitor attempts to retrieve the following URL, which does not use SSL:

http://<hostname>:8443/pamlogin/servlet/pamlogin?ReqType=Unknown

After verifying that the WEBSERVICES process group is running, a customer log, EMSS 315, is generated to indicate the PAM login servlet was unhealthy and that WEBSERVICES is being restarted. For details of this log, see *Succession Fault Management Logs Reference*, NN10275-909.

Changing the authentication mechanism between UNIX and DCE

Application

Use one of the following procedures to change the authentication mechanism between UNIX and Distributed Computing Environment (DCE) on a Succession Server Platform Foundation Software (SSPFS)-based server:

- [Switching from UNIX to DCE for authentication on page 490](#)
- [Switching from DCE to UNIX for authentication on page 494](#)

The default authentication mechanism is UNIX.

Prerequisites

To perform this procedure, you need to have the root user ID and password for the SSPFS-based server, and administrative privileges for the DCE server.

Action

Perform the following steps to complete this procedure.

Switching from UNIX to DCE for authentication

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server on which you want to change the authentication mechanism
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

- 5 Disable the Name Service Cache daemon as follows:
 - a Stop the Name Service Cache daemon

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

and pressing the Enter key.
 - b Move the “/etc/nscd.conf” file to a different location.
- 6 Add “dce” as another option for the password and group in the “/etc/nsswitch.conf” file.

The entries would look similar to “passwd: files nis dce” and “group: files nis dce” after the change.

This enables the group information to come from DCE.
- 7 Enable the DCE naming service server by typing

```
# config.dce
```

and pressing the Enter key.
- 8 Enable the DCE PAM (Pluggable Authentication Module) by typing

```
# config.dce pam
```

and pressing the Enter key.
- 9 Change the “sesm” entry in the “/etc/pam.conf” file as “sesm
auth required /usr/lib/security/\$ISA/pam_dce.so.1
try_first_pass”.
- 10 Add users and user groups to DCE as follows:

Note: For details on user groups, refer to procedure [Setting up local user accounts on an SSPFS-based server on page 402](#) in this document.

 - a Log in to DCE using the cell_admin user ID and password.

b Add a user to DCE by typing

```
dcecp> user create <userid> -group succssn  
-password <password> -organization  
ossaps-users -mypwd <cell_admin_password>
```

and pressing the Enter key.

where

userid

is the user ID of the user you want to add

password

is the password for the user ID you want to add

cell_admin_password

is the password for cell_admin

c Add the necessary user groups in DCE by typing

```
dcecp> group create <groupname>
```

and pressing the Enter key.

where

groupname

is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnspvov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmte, mgmtc, emsmte
- trkro, lnro, mgcro, mgro, emsro

- d** Add the new users to the new groups, one at a time, by typing

```
dcecp> group add <groupname> -member <userid>
```

and pressing the Enter key.

where

groupname

is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnspov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtec, mgmtc, emsmtec
- trkro, lnro, mgcro, mgro, emsro

userid

is the user ID of a new user

- e** Verify the user was added by typing

```
dcecp> group list <groupname>
```

and pressing the Enter key.

where

groupname

is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnspov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtec, mgmtc, emsmtec
- trkro, lnro, mgcro, mgro, emsro

You have completed this procedure.

Note: When the DCE authentication mechanism is selected, you must use the UNIX passwd command with the *-r* option to specify a repository. For example, if you want to change the password for a local UNIX user, the command is “passwd -r files <userid>”.

Switching from DCE to UNIX for authentication

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change the “sesm” entry in the “/etc/pam/conf” file as “sesm
auth required /usr/lib/security/\$ISA/pam_unix.so.1”.
- 6 Remove “dce” as another option for the password and group in
the “/etc/nsswitch.conf” file.
The entries would look similar to “passwd: files nis” and “group:
files nis” after the change.
- 7 Disable the DCE naming service server by typing

```
# /etc/dcesetup unconfig.nssdce
```

and pressing the Enter key.
- 8 Enable the Name Service Cache daemon as follows:
 - a Restore the “/etc/nscd.conf” file.
 - b Start the Name Service Cache daemon

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

and pressing the Enter key.
You have completed this procedure.

Setting secure FTP proxy

Application

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

- [Setting up SSH port forwarding on Unix on page 495](#)
- [Setting up SSH port forwarding on Windows on page 496](#)

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

Prerequisites

You need to have SSH software.

Action

Perform the following steps to complete this procedure.

Setting up SSH port forwarding on Unix

At your workstation

- 1 Install the SSH software.
- 2 Establish a port-forwarding session between your workstation and the SPFS-based server by typing

```
# ssh -L 9999:<remote-host>:9999 <remote-host>
```

and pressing the Enter key.

The first time you run the above command on your workstation in an attempt to forward data to remote-host, you will receive the following message and prompt:

```
The authenticity of host "remote-Host  
(1.2.3.4)" can't be established. RSA key  
fingerprint is <finger print information>. Are  
you sure you want to continue connecting  
(yes/no)?
```

SSH is verifying whether the host "remote-host" is a trusted host and whether you want to continue connecting to it.

- 3 When prompted, confirm you want to continue connecting by typing

yes

and pressing the Enter key.

- 4 When prompted, enter your password.

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

Example

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

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

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

```
# telnet localhost 9999
```

The telnet connection automatically gets secured between machine A and the SPFS-based server.

You have completed this procedure.

Setting up SSH port forwarding on Windows

At your workstation

- 1 Install PuTTY software.
- 2 Launch PuTTY to display the PuTTY Configuration window.
- 3 Configure SSH port forwarding as follows:
 - a Click Session and complete the following fields:
 - In the Host Name (or IP address) field, enter the host name or IP address of the SPFS-based server.
 - In the Port field, enter 22.
 - Under Protocol: select SSH.

b Click Tunnels and complete the following fields:

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

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

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

5 When prompted, enter your user ID and password.

This port-forwarding session is established.

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

6 Establish a secure connection as follows:

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

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

The PuTTY Configuration window opens.

c Click Session and complete the following fields:

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

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

You have completed this procedure.

Configuring automated data backups on an SSPFS-based server

Application

Use this procedure to view or change the configuration settings for an automated data backup on a Succession Server Platform Foundation Software (SSPFS)-based server. The automated backup backs up Oracle and critical data.

Note: Log SPFS320 is generated when an automated data backup fails, and when the backup failure is cleared and the backup completes successfully. Refer to the *Carrier Voice over IP Fault Management Logs Reference document*, NN10275-909, for log details.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server on which you want to configure automated data backups
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

5 Access the command line interface by typing

cli

and pressing the Enter key.

Response

Command Line Interface

1 - View

2 - Configuration

3 - Other

X - exit

select -

6 Enter the number next to the “Configuration” option in the menu.*Example response*

Configuration

1 - NTP Configuration

2 - Apache Proxy Configuration

3 - DCE Configuration

4 - OAMP Application Configuration

5 - CORBA Configuration

6 - IP Configuration

7 - DNS Configuration

8 - Syslog Configuration

9 - Database Configuration

10 - NFS Configuration

11 - Bootp Configuration

12 - Restricted Shell Configuration

13 - Security Services Configuration

14 - Login Session

15 - Location Configuration

16 - Cluster Configuration

17 - Succession Element Configuration

18 - snmp_poller (SNMP Poller Configuration)

X - exit

Select -

- 7** Enter the number next to the “Database Configuration” option in the menu.

Example response

Database Configuration

- 1 - change_db (Change Database Host)
- 2 - change_orabackup (Configure database backup)

X - exit

select -

- 8** Enter the number next to the “change_orabackup” option in the menu.

Example response

===Executing “change_orabackup”

Current setting:

Automated Backup Enabled N

Backup Time 6:00 Hours

Enable Automated backup (default: N):

- 9** When prompted, enter **y** to enable automated backup or press the Enter key to accept the default value (N) to disable automated backup.

Example response

Set backup hour to: (default: 22):

- 10** When prompted, enter the time you want the automated backup to occur, or press the Enter key to accept the default value.

Example response

New settings:

Automated Backup Enabled Y

Backup Time 22:00 Hours

Enter “ok” to commit changes

Enter “quit” to exit

Enter anything else to re-enter settings

- 11** Commit the changes by typing

ok

and pressing the Enter key.

Example response

```
=== "change_orabackup" completed successfully
```

Note: If enabled, automated backup will start within the first 45 seconds of the backup hour. If the backup hour is set to the current hour, automated backup will occur 24 hours from the current hour.

- 12** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - **x**

and pressing the Enter key.

You have completed this procedure.

Cloning the image of one node in a cluster to the other node

Application

Use this procedure to clone the image of the active node in a cluster to the inactive node.

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need console access to the Inactive node if this is the first time you clone, or if you replaced the Inactive unit or executed a reverse restore (switched unit 0 and 1)

ATTENTION

Ensure no provisioning activities are in progress, or are scheduled to take place during this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Establish a login session to the Active node using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the Active node using telnet (unsecure) as follows:
 - a Log in to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the cluster IP address, which automatically defaults to the Active node in the cluster
 - b When prompted, enter your user ID and password.

- c Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
 - d When prompted, enter the root password.
Proceed to step [4](#).
- 3 Log in using ssh (secure) as follows:
 - a Log in to the Active node by typing

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

and pressing the Enter key.
where
server
is the cluster IP address, which automatically defaults to the Active node in the cluster
Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.
 - b When prompted, enter the root password.
- 4 Verify the status of replicated disk volumes by typing

```
# udstat
```

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 5
not ACTIVE	contact your next level of support

5 Determine the server profile as follows:**a** Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
```

```
X - exit
```

```
select -
```

b Enter the number next to the “View” option in the menu.*Example response*

```
View
```

```
1 - sspfs_soft (Display Software
  Installation Level Of SSPFS)
2 - chk_sspfs (Check SSPFS Processes)
3 - sw_conf (The software configuration of
  the wrtypyxp)
4 - cpu_util (Overall CPU utilization)
5 - cpu_util_proc (CPU utilization by
  process)
6 - port_util (I/O port utilization)
7 - disk_util (Filesystem utilization)
```

```
X - exit
```

```
select -
```

c Enter the number next to the “sspfs_soft” option in the menu.*Example response*

```
=== Executing "sspfs_soft"
```

```
SSPFS version: 08.0 Build: 200508421 Server
Profile: cbm850
```

```
=== "sspfs_soft" completed successfully
```


d Note the Server Profile.

If the Server Profile is	Do
cbm850	step 16
anything else	step 6

- 6 Verify that all applications on the server are running by typing
servquery -status all
 and pressing the Enter key.

Example response:

```

APP NAME                                STATUS
=====                                =====
SNMP_POLLER                            RUNNING
DELEGATE                               RUNNING
PROP_SRV                              RUNNING
WEBSERVER                             RUNNING
DATABASE                              RUNNING
SAM21EM                               RUNNING
SESMSERVICE                           RUNNING
CORBA                                  RUNNING
ORA_ARCHIVE_ROTATOR                    RUNNING
OMPUSH                                 RUNNING
BOOTP                                  RUNNING
WEBSERVICES                           RUNNING
ORA_AUTO_BACKUP                        RUNNING
APS                                    RUNNING
NPM                                    RUNNING

```

- 7 Use the following table to determine your next step.

If	Do
all applications are running	step 10
one or more applications are not running	step 8

- 8 Start each application that is not running by typing
servstart <app_name>
 and pressing the Enter key.

where

app_name

is the name of the application that is not in a "RUNNING" state, for example, SAM21EM

- 9 Use the following table to determine your next step.

If	Do
one or more applications do not start	contact your next level of support
all applications are running	step 10

- 10 Use the following table to determine your next step.

If this server is	Do
running the NPM software	step 11
not running the NPM software	step 13

Note: The Network Patch Manager (NPM) software is running on this server if NPM appeared in the response from step [6](#).

- 11 Verify the Patching Server Element (PSE) server application is running by typing

pse status

and pressing the Enter key.

If PSE is	Do
running	step 13
not running	step 12

- 12 Start the PSE server application by typing

pse start

and pressing the Enter key.

If PSE	Do
does not start	contact your next level of support
starts	step 13

- 13 Use the following table to determine your next step.

If this server is	Do
running the CS 2000 Management Tools software	step 14
not running the CS 2000 Management Tools software	step 16

- 14 Verify that the SESMservice application is fully functional by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS
```

```
-----  
COMPONENT          STATUS  
-----  
Proxy Agent        RUNNING  
RMI Registry        RUNNING  
Snmpfactory         RUNNING  
MI2 Server          RUNNING
```

```
Current number of SESM processes running: 4 (of 4)
```

```
SESM APPLICATION STATUS: All Applications ready
```

- 15 Use the following table to determine your next step.

If the SESMService is	Do
not fully functional	contact your next level of support
fully functional	step 16

- 16 Use the following table to determine your next step.

If	Do
this is the first time you are cloning the unit, or you replaced the unit or executed a reverse restore (i.e. switched unit 0 and unit 1)	step 17
this is not the first time you are cloning the unit, and you did not replace the unit or execute a reverse restore (i.e. switched unit 0 and unit 1)	step 20

- 17 Use the following table to determine your next step.

If you	Do
know the Ethernet address of the Inactive unit	step 19
do not know the Ethernet address of the Inactive unit	step 18

At the console connected to the inactive node

- 18 Determine the Ethernet address of the Inactive node as follows:

- a Log in to the inactive node through the console (port A) using the root user ID and password.

Note: Ensure you are on the Inactive server by typing `ubmstat`. If `ClusterIndicatorACT` is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display `ClusterIndicatorSTBY`, which indicates you are on the Inactive server.

- b Bring the system to the OK prompt by typing

`init 0`

and pressing the Enter key.

- c At the OK prompt, display the Ethernet address of the inactive node by typing

OK **banner**

and pressing the Enter key.

Example response:

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc.
All rights reserved. OpenBoot 4.8.0.build_04,
2048 MB memory installed, Serial #52964131.
Ethernet address 0:3:ba:28:2b:23, Host ID:
83282b23.
```

- d Take note of the Ethernet address that is displayed.

At your workstation (login session to the Active node)

- 19 Start the cloning process by typing

startb <Ethernet address>

and press the Enter key.

where

Ethernet address

is the Ethernet address of the Inactive unit

Proceed to step [21](#)

- 20 Start the cloning process by typing

startb

and press the Enter key.

- 21 Use the following table to determine your next step.

If the system	Do
prompts you to enter the command "boot net - image"	step 22
does not prompt you to enter the command "boot net - image"	step 26

- 22 Connect to the console port of the Inactive node.

If the console displays	Do
the OK prompt	step 25
the login prompt	step 23

At the console connected to the inactive node

- 23** Log in using the root user ID and password.
- 24** Bring the system to the OK prompt by typing
`# init 0`
and pressing the Enter key.
- 25** At the OK prompt, boot the inactive node from the image of the active node by typing
`OK boot net - image`
and press the Enter key.

Note: There must be a space between the “-” and “image”.

Example response:

SC Alert: Host System has Reset

Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.

Rebooting with command: boot net - image

.
.
.

SC Alert: Host System has Reset

At your workstation (login session to the Active node)

- 26** Monitor the progress of the cloning from the active node. Cloning the inactive node takes approximately one hour to complete.

Example response:

```
Waiting for network response from unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become
normal.
Deleted snapshot 0.
Deleted snapshot 1.
Deleted snapshot 2.
Deleted snapshot 3.
d99: Soft Partition is cleared
```

- 27** Once the cloning is complete, wait approximately 5 minutes before you proceed to the next step.

At your workstation (login session to the Active node)

- 28** Verify the status of replicated disk volumes by typing

udstat

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 29
not ACTIVE	contact your next level of support

At your workstation

- 29** Establish a login session to the Inactive node using one of the following methods:

If using	Do
telnet (unsecure)	step 30
ssh (secure)	step 31

- 30** Log in to the Inactive node using telnet (unsecure) as follows:

- a** Log in to the Inactive node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

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

- b** When prompted, enter your user ID and password.

- c** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- d** When prompted, enter the root password.

Proceed to step [32](#).

- 31** Log in using ssh (secure) as follows:

- a** Log in to the Inactive node by typing

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

and pressing the Enter key.

where

server

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

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

- b** When prompted, enter the root password.

- 32** Verify the status of replicated disk volumes by typing
udstat
and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 33
not ACTIVE	contact your next level of support

At your workstation (login session to the Active node)

- 33** Complete the cloning process by typing
finishb
and pressing the Enter key.
You have completed this procedure.

Starting the SESM server application

Application

Use this procedure to start the Succession Element and Subelement Manager (SESM) server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

ATTENTION

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

At your workstation

- 1 Log in to the server by typing

> **telnet <server>**

and pressing the Enter key.

where

server

is the IP address or host name of the CS 2000 Management Tools server

Note: In a two-server configuration, enter the physical IP address of the active server (unit 0 or unit 1).

- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing

\$ **su - root**

and pressing the Enter key.

- 4 When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

- 5 Verify the status of the SESM server application by typing

```
# servman query -status -group SESMSERVICE
```

If SESMSERVICE is	Do
not running	step 6
running	you have completed this procedure

- 6 Start the SESM server application by typing

```
# servstart SESMSERVICE
```

and pressing the Enter key.

- 7 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.

Note: Starting SESM for the first time after an upgrade from a pre-SN07 release, can take up to 90 minutes depending on the number of GWs provisioned in the office. This is a one-time event that occurs during an upgrade to facilitate better topological management of data.

8 Verify the SESM server application started as follows:**a** Verify the SESM services started by typing

```
# servman query -status -group SESMService
```

and pressing the Enter key.

Example response prior to SN08:

```
Executing: /opt/servman/bin/servquery  
-status - group SESMService
```

```
Succession CS2K Management Tools VERSION:  
SESM_8_019_0
```

Current status of the CS2K Management Tools:

```
LMM is running  
TMM is running  
GWCEM is running  
UASEM is running  
OSS Gate is running
```

Example response for SN08 and up:

```
Succession CS2K Management Tools is running
```

b Verify the SESM applications started by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS -----
```

COMPONENT -----	STATUS -----
Proxy Agent	RUNNING
RMI Regisry	RUNNING
Snmpfactory	RUNNING
MI2 Server	RUNNING

Current number of SESM processes running: 4 (of 4)

SESM APPLICATION STATUS: All Applications Ready

You have completed this procedure.

Starting the SAM21 Manager server application

Application

Use this procedure to start the SAM21 Manager server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

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

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

is the IP address or host name of the CS 2000 Management Tools server

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 5 Verify the status of the SAM21 Manager server application by typing

```
# servman query -status -group SAM21EM
```

If SAM21EM is	Do
not running	step 6
running	you have completed this procedure

- 6 Start the SAM21EM server application by typing

```
# servstart SAM21EM
```

and pressing the Enter key.

- 7 Verify the SAM21EM server application started by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

Example response:

```
Executing: /opt/servman/bin/servquery -status -
group SAM21EM
```

```
Succession SAM21 Element Manager version:
SAM21EM_8_017_0
```

```
Current status of the Succession SAM21 Element
Manager:
```

```
SNMP Access Gateway is running.
```

```
SAM21 Element Manager Server is running.
```

You have completed this procedure.

Starting the NPM server application

Application

Use this procedure to start the Network Patch Manager (NPM) server application on a Succession Server Platform Foundation Software (SSPFS)-based server.

Prerequisites

You need root user privileges to perform this procedure, and CORBA must be running in order for the NPM to come up.

Action

Perform the following steps to complete this procedure.

ATTENTION

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

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server where the NPM server application resides
Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

- 5 Verify the status of the NPM server application by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

If the NPM server application is	Do
not running	step 6
running	you have completed this procedure

- 6 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

- 7 Verify the NPM server application is running by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

You have completed this procedure.

Performing a backup of APS audio files to tape

Application

Use this procedure to back up APS audio files to a 4mm Digital Audio Tape (DAT).

ATTENTION

This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure [Performing a backup of APS audio files to CD or DVD on page 523](#).

Prerequisites

You need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the audio files.

Action

Perform the following steps to complete this procedure.

At the server

- 1 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides.

At the server console

- 2 Log in to the server through the console (port A) using the root user ID and password.
- 3 Rewind the tape by typing

```
# mt -f /dev/rmt/0c rewind
```

and pressing the Enter key.
- 4 Change directories to the root filesystem by typing

```
# cd /
```

and pressing the Enter key.
- 5 Back up the APS audio files by typing

```
# /usr/ntdb/uas/scripts/backup_appl_data.sh
```

and pressing the Enter key.

Note: This command backs up file systems /PROV_data, /audio_files, and /user_audio_files.

- 6 Rewind the backup tape by typing

```
# mt -f /dev/rmt/0c rewind
```

and pressing the Enter key.
- 7 To ensure that the backup was successful, list the content of the tape by typing

```
# tar tvf /dev/rmt/0c | more
```

and pressing the Enter key.
- 8 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen) to prevent the data on the tape from being accidentally over-written. Store the tape for later use.
- 9 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Performing a backup of APS audio files to CD or DVD

Application

Use this procedure to back up APS audio files to a CD or DVD, or move the backup of audio files to another server if the backup is more than 2 GB.

ATTENTION

This procedure only applies to a Sun Netra 240 server with a CD/DVD drive. Use procedure [Performing a backup of APS audio files to tape on page 521](#) for a Sun t1400 server with a DAT drive.

Prerequisites

You need one blank CD-R, DVD-R, CD-RW or DVD-RW to store the data if the data is less than 2 GB. Otherwise you need a server accessible through FTP with adequate space to hold the data.

Note 1: The backup utility limits the storage to 2 GB on a DVD-R, or DVD-RW.

Note 2: If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

Action

ATTENTION

In a two-server configuration, execute this procedure on the active server.

At the server

- 1 Insert a blank CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the active server.

At your workstation

- 2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

is the IP address or host name of the server on which you are performing the backup

In a two-server configuration, enter the physical IP address of the active server.

- 3 When prompted, enter your user ID and password.

- 4 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- 5 When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing **ubmstat**. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

- 6 Change directories to the root file system by typing

```
# cd /
```

and pressing the Enter key.

- 7 Create a “tar” file of the APS audio files by typing

```
# tar cvf AudioFiles.tar /audio_files  
/user_audio_files /opt/uas/uas_conf_backup
```

and pressing the Enter key.

Note: The above command is entered on one line, and includes a space between each directory.

- 8** Verify the size of the “AudioFiles.tar” file by typing
- ```
ls -l AudioFiles.tar
```
- and pressing the Enter key.
- 
- | If the “AudioFiles.tar” file is | Do                      |
|---------------------------------|-------------------------|
| under 2 GB                      | step <a href="#">10</a> |
| over 2 GB                       | step <a href="#">9</a>  |
- 
- 9** Move the “AudioFiles.tar” file onto another server using File Transfer Protocol (FTP).  
Proceed to step [13](#)
- 10** Create a temporary directory by typing
- ```
# mkdir /tmp/.iso
```
- and pressing the Enter key.
- Note:** The directory may already exist.
- 11** Backup the tar file of the APS audio files onto the CD or DVD by typing
- ```
/opt/nortel/sspfs/bks/cdwrite AudioFiles.tar
```
- and pressing the Enter key.
- 12** Remove the CD or DVD from the drive, label it, and store it in a safe place.
- 13** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

---

## Performing a backup of APS oracle data to tape

---

### Application

Use this procedure to back up APS oracle data to a 4mm Digital Audio Tape (DAT).

#### ATTENTION

This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure [Performing a backup of APS oracle data to CD or DVD on page 528](#).

### Prerequisites

You need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the oracle data.

### Action

Perform the following steps to complete this procedure.

#### *At the server*

- 1 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides.

#### *At the server console*

- 2 Log in to the server through the console (port A) using the root user ID and password.
- 3 Rewind the tape by typing  

```
mt -f /dev/rmt/0c rewind
```

and pressing the Enter key.
- 4 Change directories to the root filesystem by typing  

```
cd /
```

and pressing the Enter key.
- 5 Back up the APS oracle files by typing  

```
ips_export_db.sh -t /dev/rmt/0 | tee ./export_log
```

and pressing the Enter key.

- 6 Rewind the backup tape by typing  

```
mt -f /dev/rmt/0c rewind
```

and pressing the Enter key.
- 7 To ensure the backup was successful, list the content of the tape by typing  

```
tar tvf /dev/rmt/0c | more
```

and pressing the Enter key.
- 8 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen) to prevent the data on the tape from being accidentally over-written. Store the tape for later use.
- 9 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

---

## Performing a backup of APS oracle data to CD or DVD

---

### Application

Use this procedure to back up APS oracle onto a CD or DVD.

#### ATTENTION

This procedure only applies to a Sun Netra 240 server with a CD/DVD drive. Use procedure [Performing a backup of APS oracle data to tape on page 526](#) for a Sun t1400 server with a DAT drive.

### Prerequisites

You need one blank CD-R, DVD-R, CD-RW or DVD-RW to store the data

**Note 1:** The backup utility limits the storage to 4 GB on a DVD-R, or DVD-RW.

**Note 2:** If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

### Action

#### ATTENTION

In a two-server configuration, execute this procedure on the active server.

#### *At the server*

- 1 Insert a blank CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the active server.



***At your workstation***

- 2** Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the server on which you are performing the backup

Enter the physical IP address of the active server in a two-server configuration.

- 3** When prompted, enter your user ID and password.

- 4** Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- 5** When prompted, enter the root password.

- 6** Back up the APS oracle data to hard disk by typing

```
ips_export_db.sh -diskonly
```

and pressing the Enter key.

- 7** Change directories to where the backup is by typing

```
cd /audio_files/aps_db_backup
```

and pressing the Enter key.

- 8** Create a tar file of the APS oracle files by typing

```
tar cvf aps_oracle_bkup.tar *
```

and pressing the Enter key.

- 9 Verify the size of the “aps\_oracle\_bkup.tar” file by typing

```
ls -l aps_oracle_bkup.tar
```

and pressing the Enter key.

| If the<br>“aps_oracle_bkup.tar” file<br>is | Do                           |
|--------------------------------------------|------------------------------|
| under 2 GB                                 | step <a href="#">11</a>      |
| over 2 GB                                  | step <a href="#">10</a> only |

- 10 Move the “aps\_oracle\_bkup.tar” file onto another server using File Transfer Protocol (FTP).

You have completed this procedure.

- 11 Create a temporary directory by typing

```
mkdir /tmp/.iso
```

and pressing the Enter key.

**Note:** The directory may already exist.

- 12 Backup the tar file of the APS oracle data onto the CD or DVD by typing

```
/opt/nortel/sspfs/bks/cdwrite
aps_oracle_bkup.tar
```

and pressing the Enter key.

- 13 Remove the CD or DVD from the drive, label it, and store it in a safe place.

You have completed this procedure.

---

## Starting the APS server application

---

### Application

Use this procedure to start the APS server application on the Server Platform Foundation Software (SPFS)-based server where the APS resides.

**Note:** The APS resides on the same server as the CS 2000 Management Tools software (CS2M).

### Prerequisites

None

### Action

Perform the steps that follow to complete this procedure.

**ATTENTION**

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

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SPFS-based server where the APS resides  
**Note:** In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.  
**Note:** In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.
- 5 Start the APS server application by typing  
`# servstart APS`  
and pressing the Enter key.
- 6 Verify the APS server application started by typing  
`# servman query -status -group APS`  
and pressing the Enter key.  
You have completed this procedure.

---

## Performing a restore of APS audio files from tape

---

### Application

Use this procedure to perform a restore of APS audio files from a backup tape on a Server Platform Foundation Software (SPFS)-based server (Sun t1400) running the SN06.2 or greater release of the SSPFS.

#### ATTENTION

This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure [Performing a restore of APS audio files from CD on page 535](#).

### Prerequisites

You need the tape on which you backed up the APS audio files.

#### *At the server*

- 1 Insert the tape on which you backed up the APS audio files into the DAT drive on the server where the APS resides.

#### *At the server*

- 2 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SPFS-based server on which you are restoring the APS audio files
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 5 When prompted, enter the root password.

- 6 Change directory to the root file system by typing

```
cd /
```

and pressing the Enter key.

- 7 Restore the audio files to the file system by typing

```
tar xvf /dev/rmt/0
```

The files are read from tar and placed in the following file systems: /audio\_files and /user\_audio\_files.

You have completed this procedure.

---

## Performing a restore of APS audio files from CD

---

### Application

Use this procedure to perform a restore of APS audio files from a backup CD or DVD on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra 240) running the SN06.2 or greater release of the SSPFS.

#### ATTENTION

This procedure only applies to a Sun Netra 240-type server with a CD/DVD drive. If you have a Sun Netra t1400-type server, use procedure [Performing a restore of APS audio files from tape on page 533](#).

### Prerequisites

You need the CD or DVD on which you backed up the APS audio files.

#### *At the server*

- 1 Insert the CD or DVD on which you backed up the APS audio files into the drive on the server where the APS resides.

#### *At the server*

- 2 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SSPFS-based server on which you are restoring the APS audio files
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 5 When prompted, enter the root password.

- 6 Change directory to the root file system by typing

```
cd /
```

and pressing the Enter key.

- 7 Restore the audio files to the file system by typing

```
cp /cdrom/cdrom0/* /
```

and pressing the Enter key.

The files are read from cd and placed in the following file systems: /audio\_files and /user\_audio\_files.

You have completed this procedure.



---

## Launching CS 2000 Management Tools and NPM client applications

---

### Application

Use this procedure to launch any one of the following client applications:

- Trunk Maintenance Manager (TMM)
- CS2000 Management Tools
- Line Maintenance Manager (LMM)
- SAM21 Element Manager
- Batch Configuration Monitor
- Network Patch Manager (NPM), when installed and enabled on the same server as the CS 2000 Management Tools

**Note:** The NPM also has a command line user interface (CLUI). Refer to procedure [Accessing the Network Patch Manager CLUI on page 550](#).

This procedure provides the following four methods to launch a CS 2000 Management Tools client application:

- [Launching applications from a web browser on page 539](#). You must use this method when launching an application for the first time.
- [Launching applications from the JWS Application Manager on page 542](#).

**Note:** You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- [Launching applications from a desktop icon or Start menu \(Windows only\) on page 545](#).

**Note:** You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- [Launching specific applications using a URL on page 548](#).

**Note:** You can also launch applications from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to the Integrated Element Management System Basics document, NN10329-111.

## Prerequisites

Ensure the client workstation meets the minimum requirements. Refer to section "Client workstation requirements" under "CS 2000 Management Tools" in the Basics document, NN10320-100 (ATM solution) or NN10300-100 (IP solution).

### ATTENTION

If you have an ATI Raedon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you can experience the "blue screen of death" in your Windows environment. You can obtain information on this issue at the following website:

<http://developer.java.sun.com/developer/bugParade/bugs/4713003.html>

A workaround for this issue is to download the latest ATI graphics driver from the following web site:

<http://mirror.ati.com/support/driver.html>

Contact your IT support team if you need assistance.

You need the IP address or host name of the server where the CS 2000 Management Tools are installed, and a valid user name and password to launch an application.

**Note:** Users of the CS 2000 Management Tools client applications must belong to the primary user group "succssn" for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure "Setting up local user accounts on a Sun server" in the ATM/IP Security and Administration document, NN10402-600.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2\_05 and Java™ Web Start (JWS) version 1.2.0\_02 installed to launch the following applications:

- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

**Note:** JWS 1.2.0\_02 is included as part of JRE 1.4.2\_05.

## Action

### Launching applications from a web browser

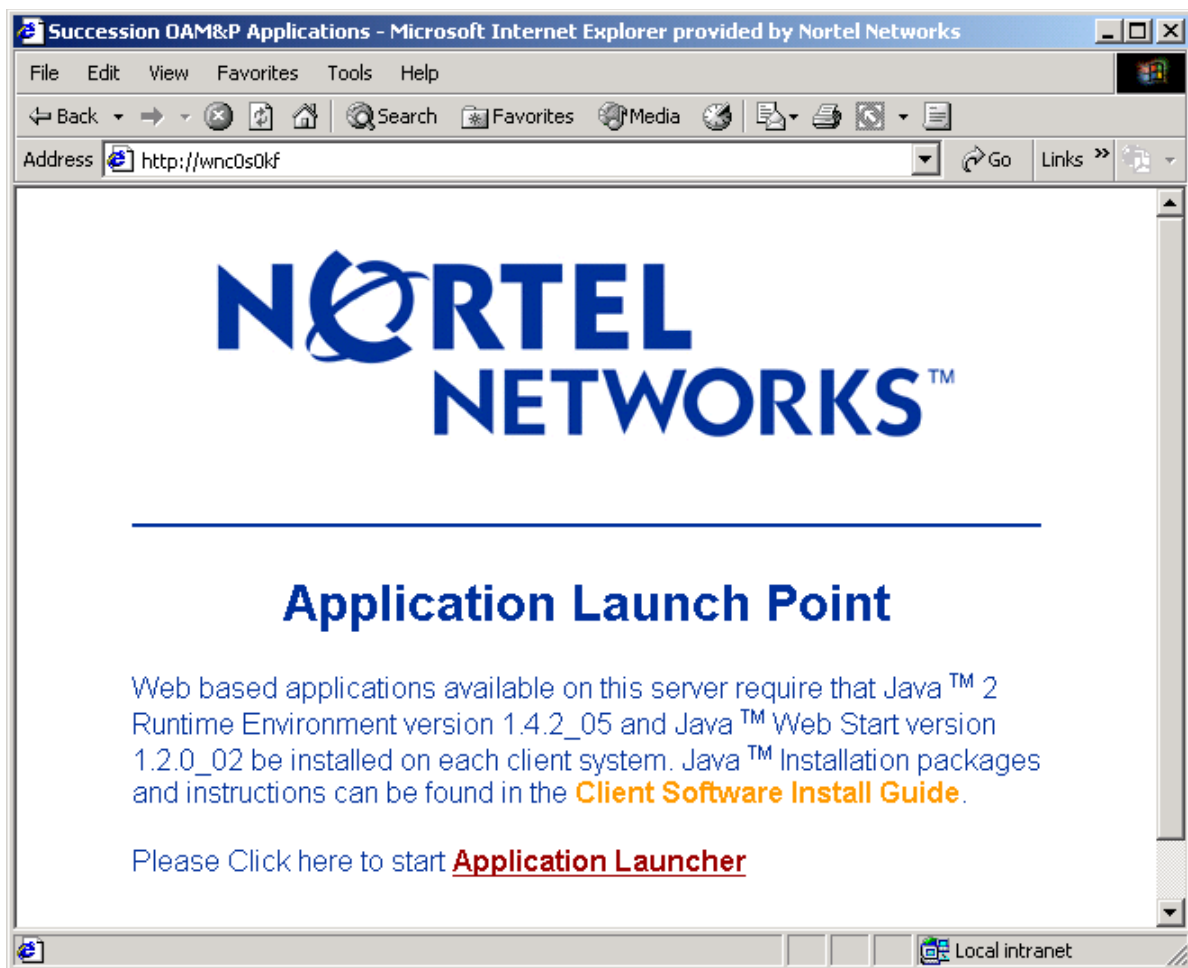
#### *At your workstation*

- 1 Launch your web browser.
- 2 In the Address field, enter the name or IP address of the CS 2000 Management Tools server.

#### **Example**

`http://47.142.89.70`

The “Application Launch Point” page appears.



- 3 Refer to the following table to determine your next step.

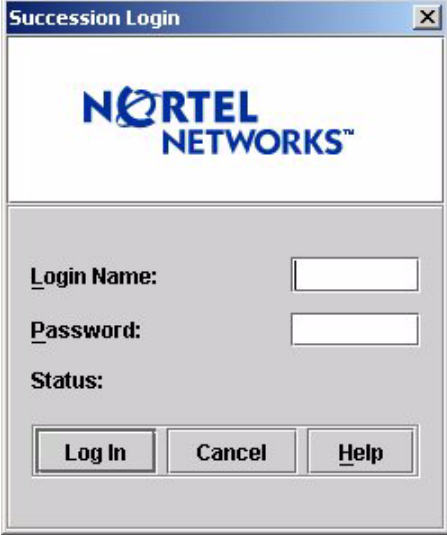
| If                                                      | Do                     |
|---------------------------------------------------------|------------------------|
| you have JRE 1.4.2_05 and JWS 1.2.0_02 installed        | <a href="#">step 9</a> |
| you do not have JRE 1.4.2_05 and JWS 1.2.0_02 installed | <a href="#">step 4</a> |
| you do not know which version of JRE and JWS you have   | <a href="#">step 4</a> |

- 4 Click **Client Software Install Guide** and follow the instructions under *How to check version* to verify your client setup.

| If                                                      | Do                     |
|---------------------------------------------------------|------------------------|
| you have JRE 1.4.2_05 and JWS 1.2.0_02 installed        | <a href="#">step 8</a> |
| you do not have JRE 1.4.2_05 and JWS 1.2.0_02 installed | <a href="#">step 5</a> |

- 5 Click **Java 2 Runtime Environment Install Guide** under *Microsoft Windows* or *Sun Solaris* for system requirements and installation instructions.
- 6 Once you have read through the Java 2 Runtime Environment Install Guide, click the **Back** button to return to the Client Software Installation page.
- 7 Click **Java 2 Runtime Environment Software Download** under *Microsoft Windows* or *Sun Solaris* to download and install the software.
- Note:** You must have administrative privileges to install the software on the workstation.
- 8 Click the **Back** button to return to the Application Launch Point.

- 9 Click **Application Launcher**.  
The Login window appears.



A screenshot of a web browser window titled "Succession Login". The window has a blue header bar with the title and a close button. Below the header is the Nortel Networks logo. The main content area is a light gray box containing three labels: "Login Name:", "Password:", and "Status:". Each label is followed by a text input field. At the bottom of the gray box are three buttons: "Log In", "Cancel", and "Help".

- 10 Enter your user name and password, then click **Log In**.  
The Application Launch Point, similar to following, appears.



A screenshot of a web browser window titled "Application Launch Point - 47.142.117.20 (CM CLI: RLGHNCPR5M8)". The window has a blue header bar with the title and standard window controls. The main content area is white and features the Nortel Networks logo at the top. Below the logo is the heading "Application Launch Point" in blue. Underneath is the text "Web based applications available on this server ( 47.142.117.20 )". A bulleted list of applications follows: "CS2000 Management Tools", "Line Maintenance Manager", "Trunk Maintenance Manager", "Batch Configuration Monitor", "Succession SAM21 Element Manager", and "Network Patch Manager". At the bottom of the window is a status bar that says "Applet running..."

- 11 Click the link for the application you want to launch.

The interface for the application you launched, is displayed.

**Note:** If you delay clicking an application link by 5 minutes or more after you log in, the login window will appear requiring you to log in again.

You have completed this procedure.

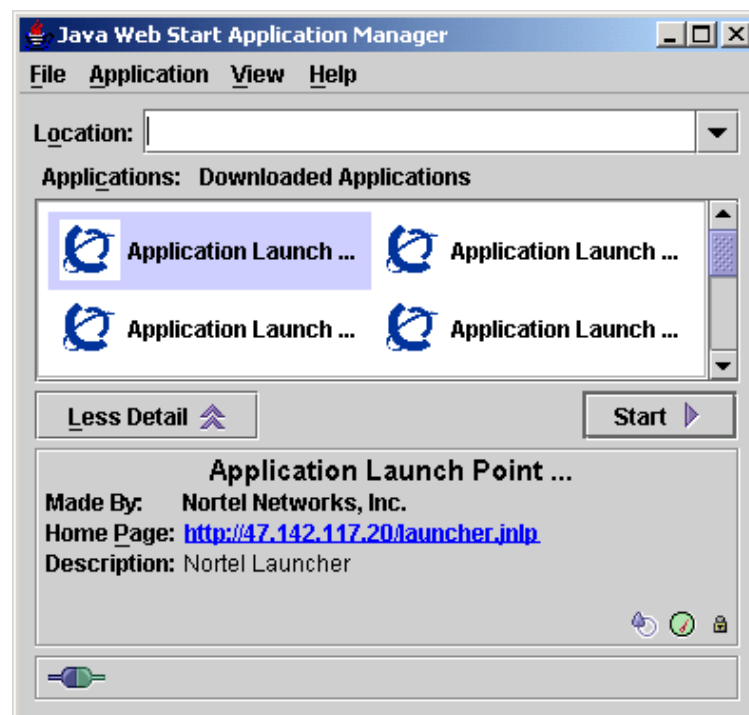
## Launching applications from the JWS Application Manager

### ATTENTION

You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

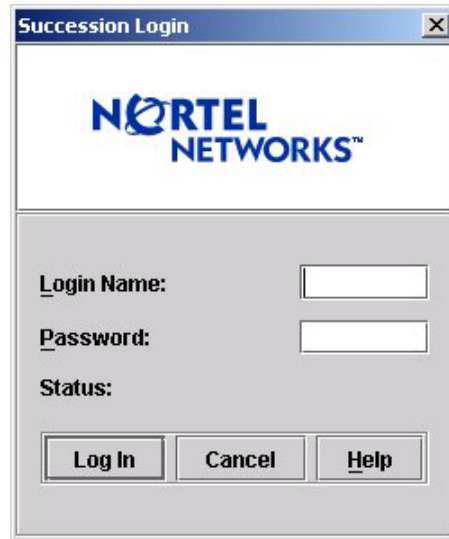
### At your workstation

- 1 Launch the Java Web Start Application Manager.

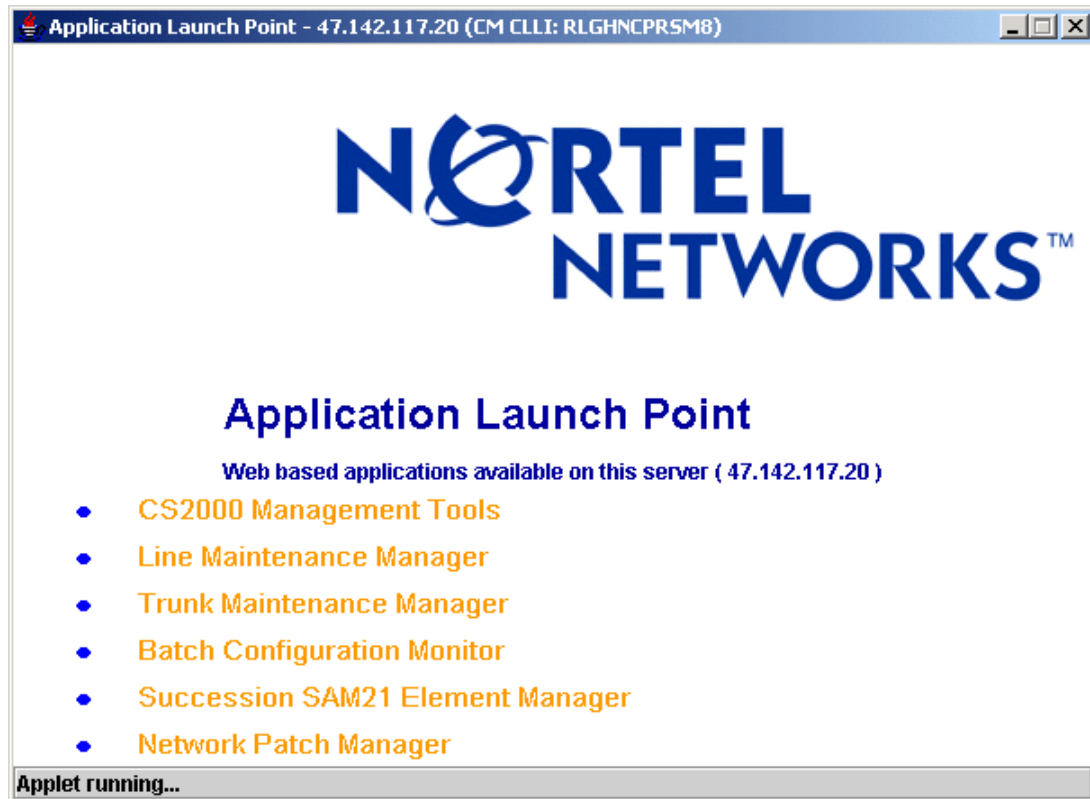


**Note:** If you do not see the downloaded applications as shown in the example above, on the **View** menu, click **Downloaded Applications**.

- 2 Double click on the Application Launch Point you want to access, or select the Application Launch Point and click **Start**.  
The Login window appears.
- 3 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



- 4 Click the link for the application you want to launch.  
The interface for the application you launched, is displayed.  
You have completed this procedure.



## Launching applications from a desktop icon or Start menu (Windows only)

### ATTENTION

You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

### *At your workstation*

- 1 Perform [step a](#) to launch an application from a desktop icon, or [step b](#) to launch an application from the Start menu.
  - a To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double click on it to start the application.

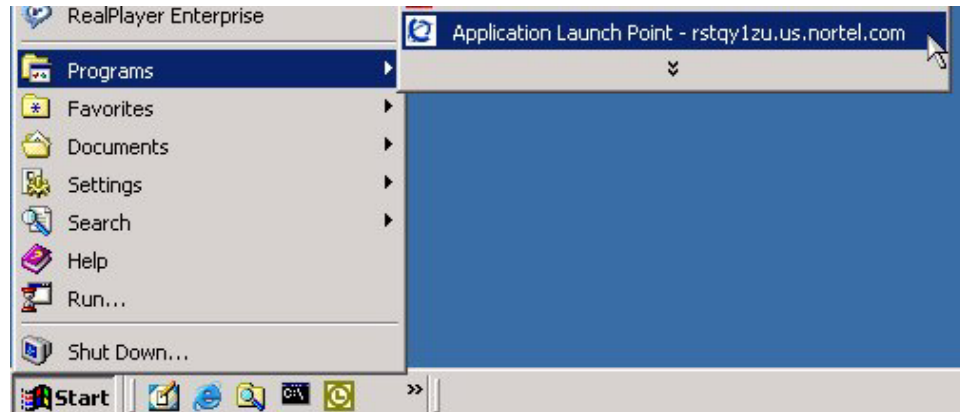
**Note:** For short-cut icons to be present on your desktop, you must have the right settings under the Shortcut Options tab, which is accessed through **File->Preferences** in the JWS Application Manager.



The Login window appears.

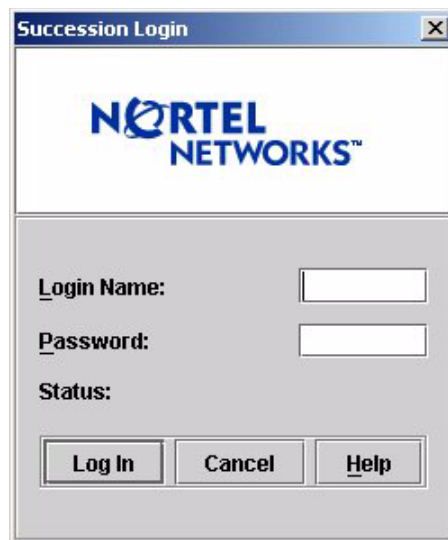
Proceed to [step 2](#).

- b To launch a CS 2000 Management Tools client application from the Start menu, click **Start->Programs**, then click the CS 2000 Management Tools client application you want to launch.

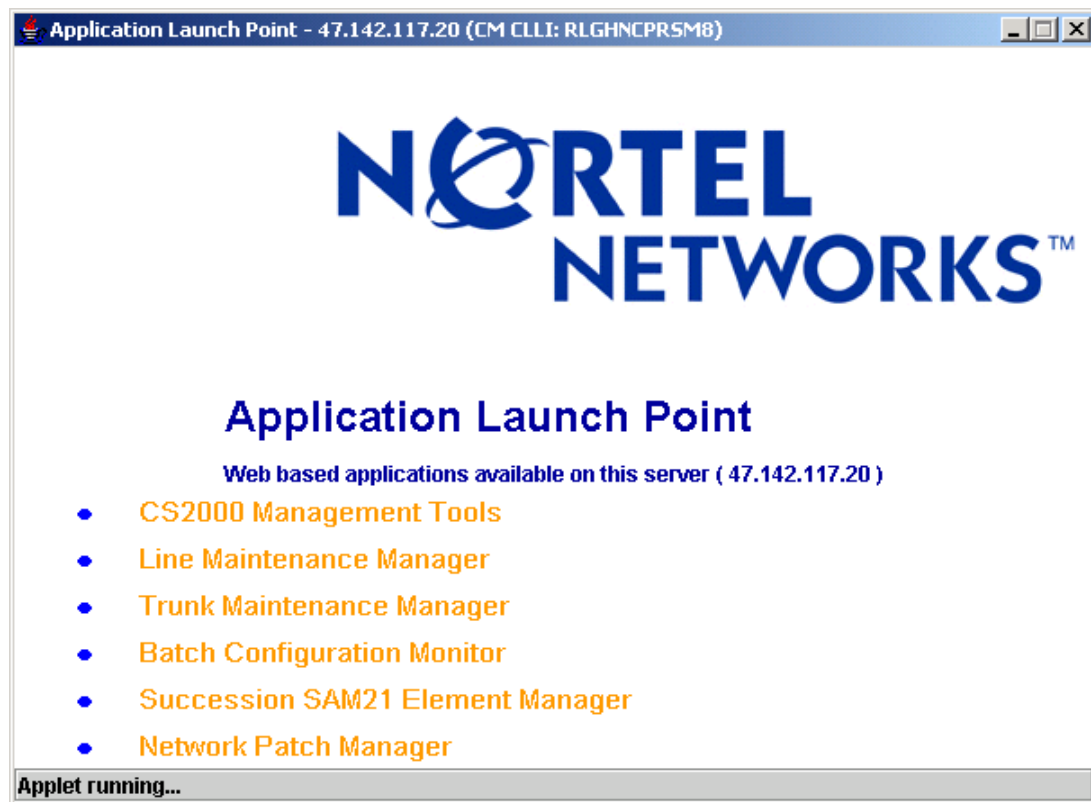


The Login window appears.

- 2 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



- 3 Click the link for the application you want to launch.  
The interface for the application you launched, is displayed.  
You have completed this procedure.

## Launching specific applications using a URL

### ATTENTION

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2\_05 and Java™ Web Start (JWS) version 1.2.0\_02 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in this procedure [Launching applications from a web browser on page 539](#).

### At your workstation

- 1 Launch your web browser.
- 2 In the Address field, enter one of the following URLs for the application you want to launch:

| Application                 | URL                                                  |
|-----------------------------|------------------------------------------------------|
| CS2000 Management Tools     | http://<host>:8080/launch/servlet/Launch?app=sesm    |
| Line Maintenance Manager    | http://<host>:8080/launch/servlet/Launch?app=lmm     |
| Trunk Maintenance Manager   | http://<host>/sesm/tmm.html                          |
| Batch Configuration Monitor | http://<host>/sesm/bpt.html                          |
| CS2000 SAM21 Manager        | http://<host>:8080/launch/servlet/Launch?app=sam21em |
| Network Patch Manager       | http://<host>:8080/launch/servlet/Launch?app=npm     |

Where

#### host

is the host name or IP address of the server where the application resides

The Login window appears.

- 3 Enter your user name and password, then click **Log In**.



The interface for the application you launched, is displayed.  
You have completed this procedure.

### Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and SAM21 Element Manager) connect to their corresponding server-side application through a Socks proxy.

**Note:** The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

If, when you launch a client application that connects through a Socks proxy, you receive an error message indicating that the Socks connection to the server has failed, the server is down and needs to be rebooted. Once the server has rebooted, you can relaunch the client application.

---

## Accessing the Network Patch Manager CLUI

---

### Application

Use this procedure to access the Network Patch Manager (NPM) command line user interface (CLUI).

**Note 1:** You can also access the NPM CLUI from the Integrated Element Management System (EMS) when the Integrated EMS is present in the office. Refer to the Integrated EMS Basics document, NN10329-111.

**Note 2:** The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 537](#).

### Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-based server” in the ATM/IP Security and Administration document, NN10402-600.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SSPFS-based server where NPM resides
- 2 When prompted, enter your user ID and password.
- 3 Start the NPM CLUI by typing  

```
$ npm
```

and pressing the Enter key.

- 4 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode: Enter 'npm' commands, help
or quit to exit.
```

```
npm>
```

You have completed this procedure.

---

## Starting the batch provisioning tool

---

### Application

Use this procedure to start the batch provisioning tool.

### Prerequisites

You must have a valid user ID and password.

### Action

Perform the following steps to complete this procedure.

#### ***At your workstation***

- 1 Log in to the server by typing  
    `> telnet <server>`  
    and pressing the Enter key.  
    where  
        **server**  
        is the IP address or host name of the CS 2000  
        Management Tools server
- 2 When prompted, enter your user ID and password.
- 3 Start the batch provisioning tool by typing  
    `$ bpt`  
    and pressing the Enter key.
- 4 When prompted, enter your username and password.



*Example response:*

Login in progress...

You are currently logged in as : rtps!

=====

Main Menu:

=====

- (1) Execute Batch File
- (2) Display Output
- (3) Display Logs
- (4) Delete Output or Log Files
- (h) Help

- (1) Exit

Selection: [1/2/3/4/h/x:1]

You have completed this procedure.

## Connecting to OSSGate

### Application

Use this procedure to connect to OSSGate. You can connect to OSSGate with password control turned on or off. When OSSGate password control is turned on, the password will not be echoed on the screen when logging in. To verify or change the status of password control, refer to procedure [Configuring OSSGate password control on page 419](#).

### Prerequisites

You must have a telnet client that supports line mode and can implicitly add a Carriage Return (CR) to any data coming from the OSSGate server.

### Action

Perform the following steps to complete this procedure.

#### **From a telnet client**

- 1 Connect to the OSSGate by typing

```
> telnet <server> <port_number>
```

where

**server**

is the IP address or host name of the remote host, which is the CS 2000 Management Tools server (non-secure connection) or the local host (secure connection)

**Note:** For a secure connection, port forwarding must be configured and enabled. Refer to the *OSSGate Users Guide*, NE10004-512 to configure port forwarding if required.

**port\_number**

is the port number (default 10023)

The login prompt will be slightly different depending on whether OSSGate password control is turned on.

- 2 Use the following table to determine your next step:

| If the login prompt is      | Do                     |
|-----------------------------|------------------------|
| Enter User Name             | step <a href="#">3</a> |
| Enter username and password | step <a href="#">5</a> |

- 3** When prompted, enter your user name.

Example

Enter User Name

> ossuser

- 4** When prompted, enter your password.

Example

Enter Password

> osspassword

You have completed this procedure.

- 5** When prompted, enter your username and password separated by a space, and press the Enter key.

Example

Enter username and password

> ossuser osspassword

You have completed this procedure.

---

## Changing modes within OSSGate

---

### Application

Use this procedure to change between the two modes that OSSGate supports: Command Interface (CI) and XML. The default mode is CI for Lines.

### Prerequisites

You must be logged in to OSSGate.

### Action

Perform the following steps to complete this procedure.

#### *From the OSSGate user interface*

- 1 Change to Control mode by pressing the Control key and the B key at the same time (Ctrl+B) .

> **^B**

and pressing the Enter key.

**Note:** For some terminal settings, the Ctrl+B character is not displayed on the screen.

- 2 At the prompt, enter the mode to change to by typing

? **mode <new\_mode>**

and pressing the Enter key.

where

**new\_mode**

is the mode (ci or xml) to change to

*Example*

> **mode xml**

The system responds with a confirmation of the mode change. The following example is for a mode change to XML.

Mode is XML.

You have completed this procedure.

---

## Stopping the SESM server application

---

### Application

Use this procedure to stop the Succession Element and Subelement Manager (SESM) server application on the CS 2000 Management Tools server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### **ATTENTION**

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

#### ***At your workstation***

- 1 Log in to the server by typing

> **telnet <server>**

and pressing the Enter key.

where

**server**

is the IP address or host name of the CS 2000 Management Tools server

**Note:** In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing

\$ **su - root**

and pressing the Enter key.

- 4 When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 5 Verify the status of the SESM server application by typing

```
servman query -status -group SESMSERVICE
```

| If SESMSERVICE is | Do                                |
|-------------------|-----------------------------------|
| running           | step <a href="#">6</a>            |
| not running       | you have completed this procedure |

- 6 Stop the SESM server application by typing

```
servstop SESMSERVICE
```

and pressing the Enter key.

- 7 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to stop.

- 8 Verify the SESM server application stopped by typing

```
servman query -status -group SESMSERVICE
```

and pressing the Enter key.

*Example response:*

```
Succession CS2K Management Tools is not running
You have completed this procedure.
```

---

## Stopping the SAM21 Manager server application

---

### Application

Use this procedure to stop the SAM21 Manager server application on the CS 2000 Management Tools server.

### Prerequisites

None

### Action

Perform the steps that follow to complete this procedure.

#### ATTENTION

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

#### *At your workstation*

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

#### **server**

is the IP address or host name of the CS 2000 Management Tools server

**Note:** In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 5 Verify the status of the SAM21 Manager server application by typing

```
servman query -status -group SAM21EM
```

| If SAM21EM is | Do                                |
|---------------|-----------------------------------|
| running       | step <a href="#">6</a>            |
| not running   | you have completed this procedure |

- 6 Stop the SAM21EM server application by typing

```
servstop SAM21EM
```

and pressing the Enter key.

- 7 Verify the SAM21EM server application stopped by typing

```
servman query -status -group SAM21EM
```

and pressing the Enter key.

*Example response:*

```
Executing: /opt/servman/bin/servquery -status -
group SAM21EM
```

```
Succession SAM21 Element Manager version:
SAM21EM_8_017_0
```

```
Current status of the Succession SAM21 Element
Manager:
```

```
SNMP Access Gateway is not running.
```

```
SAM21 Element Manager Server is not running.
```

You have completed this procedure.



---

## Stopping the NPM server application

---

### Application

Use this procedure to stop the Network Patch Manager (NPM) server application on a Succession Server Platform Foundation Software (SSPFS)-based server.

### Prerequisites

You need root user privileges to perform this procedure.

It is recommended that all users exit the NPM CLUI and GUI before stopping the NPM server application.

### Action

Perform the following steps to complete this procedure.

|                                                     |
|-----------------------------------------------------|
| <p style="text-align: center;"><b>ATTENTION</b></p> |
|-----------------------------------------------------|

|                                                                                           |
|-------------------------------------------------------------------------------------------|
| <p>In a two-server configuration, perform the steps that follow on the Active server.</p> |
|-------------------------------------------------------------------------------------------|

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SSPFS-based server where the NPM server application resides  
**Note:** In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

- 5 Verify the status of the NPM server application by typing

```
servman query -status -group NPM
```

and pressing the Enter key.

| If the NPM server application is | Do                                |
|----------------------------------|-----------------------------------|
| running                          | step <a href="#">6</a>            |
| not running                      | you have completed this procedure |

- 6 Stop the NPM server application by typing

```
servstop NPM
```

and pressing the Enter key.

- 7 Verify the NPM server application is no longer running by typing

```
servman query -status -group NPM
```

and pressing the Enter key.

You have completed this procedure.

---

## Stopping the APS server application

---

### Application

Use this procedure to stop the APS server application on the Server Platform Foundation Software (SPFS)-based server.

**Note:** The APS resides on the same server as the CS 2000 Management Tools software (CS2M).

### Prerequisites

None

### Action

Perform the steps that follow to complete this procedure.

|                                                     |
|-----------------------------------------------------|
| <p style="text-align: center;"><b>ATTENTION</b></p> |
|-----------------------------------------------------|

|                                                                                           |
|-------------------------------------------------------------------------------------------|
| <p>In a two-server configuration, perform the steps that follow on the Active server.</p> |
|-------------------------------------------------------------------------------------------|

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

  
and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SPFS-based server  
where the APS resides  
**Note:** In a two-server configuration, enter the physical IP  
address of the Active server (unit 0 or unit 1).
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

  
and pressing the Enter key.

- 4 When prompted, enter the root password.  
**Note:** In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.
- 5 Stop the APS server application by typing  
`# servstop APS`  
and pressing the Enter key.
- 6 Verify the APS server application stopped by typing  
`# servman query -status -group APS`  
and pressing the Enter key.  
You have completed this procedure.

---

## Disconnecting from OSSGate

---

### Application

Use this procedure to disconnect from OSSGate.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### *From the OSSGate user interface*

- 1 Change to Control mode by pressing the Control key and the B key at the same time (Ctrl+B).  
    > **^B**  
    and pressing the Enter key.  
        **Note:** For some terminal settings, the Ctrl+B character is not displayed on the screen.
- 2 Log out by typing  
    ? **logout**  
    and pressing the Enter key.  
    You are returned to the input ('>') prompt.
- 3 Change to Control mode by pressing the Control key and the B key (Ctrl+B) at the same time.  
    > **^B**  
    and pressing the Enter key.  
        **Note:** For some terminal settings, the Ctrl+B character is not displayed on the screen.
- 4 End the session by typing  
    ? **clearconv**  
    and pressing the Enter key.  
    You have completed this procedure.

---

## Starting and stopping the PM Poller

---

### Application

Use this procedure to start the PM poller on a network element or, stop the PM poller after you have collected the required data on the network element.

### Prerequisites

The SSPFS must be installed and running the (I)SN06 or later load.

### Action

Perform the following steps to complete this procedure.

|                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <p style="text-align: center;"><b>ATTENTION</b></p> <p>In a two-server configuration, perform the steps that follow on the Active server.</p> |
|-----------------------------------------------------------------------------------------------------------------------------------------------|

#### *At your workstation*

- 1 Log in to the SSPFS-based server by typing

**> telnet <server>**

and pressing the Enter key.

where

**server**

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

**Note:** In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing

**\$ su - root**

and pressing the Enter key.

- 4 When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 5 Change to the PM poller directory by typing

```
cd /opt/nortel/snmp-poller/bin
```

and pressing the Enter key.

- 6 Use the following table to determine your next step.

| If you want to      | Do                     |
|---------------------|------------------------|
| start the PM poller | step <a href="#">7</a> |
| stop the PM poller  | step <a href="#">9</a> |

- 7 Start the PM poller as follows:

- a Start the PM poller by typing

```
servstart SNMP_POLLER
```

and pressing the Enter key.

- b Verify the PM poller started by typing

```
servman query -status -group SNMP_POLLER
```

and pressing the Enter key.

*Example response:*

```
Executing: /opt/servman/bin/servquery -status
-group SNMP_POLLER.
pmfadm -c snmpp -n 5 -t 60
/opt/nortel/snmp-poller/bin/snmpp -c
/opt/nortel/snmp-poller/config/poller-config.xml
 retries: 0
 owner: root
 pids: 23853
The poller process is running.
```

- 8 Use the following table to determine your next step.

| If you want to              | Do                                |
|-----------------------------|-----------------------------------|
| leave the PM poller running | you have completed this procedure |
| stop the PM poller          | step <a href="#">9</a>            |

- 9 Stop the PM poller as follows:

- a Stop the PM poller by typing

```
servstop SNMP_POLLER
```

and pressing the Enter key.

*Example response*

```
SNMP_POLLER stopped
```

- b Verify the PM poller stopped by typing

```
servman query -status -group SNMP_POLLER
```

and pressing the Enter key.

*Example response*

```
Wed 19 Mar 2003 09:36:08 AM EDT: status poller
command.
```

```
pmfadm: "snmpp" No such <nametag> registered
```

The poller process is not running.

You have completed this procedure.



---

## Starting and stopping the QoS Collector Application

---

### Application

Use this procedure to start or stop the QoS Collector Application (QCA) on the Succession Server Platform Foundation Software (SSPFS)-based server.

**Note:** The QCA is installed on the same SSPFS-based server as the CS 2000 Management Tools software (CS2M), but a second instance of QCA may also be installed on a separate SSPFS-based server.

You need to stop and restart the QCA after you performed procedure “Configuring the QoS Collector Application” in the Configuration Management document.

**Note:** QCA is not applicable to AAL2 solutions.

### Prerequisites

None

### Action

#### *At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

| If using          | Do                     |
|-------------------|------------------------|
| telnet (unsecure) | step <a href="#">2</a> |
| ssh (secure)      | step <a href="#">3</a> |

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

> **telnet** <server>

and pressing the Enter key.

where

**server**

is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration

**b** When prompted, enter your user ID and password.

**c** Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

**d** When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step [4](#).

**3** Log in using ssh (secure) as follows:

**a** Log in to the server by typing

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

and pressing the Enter key.

where

**server**

is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration

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

**b** When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

- 4 Verify the status of QCA by typing  
**# servman query -status -group QCA**  
and pressing the Enter key.

*Example response when QCA is running*

A QCA instance is registered with PMFADN as Qca  
and running on the portNumber=20000

*Example response when QCA is not running*

A QCA instance is not registered with PMFADM as  
Qca

- 5 Use the following table to determine your next step.

| If you want to | Do                     |
|----------------|------------------------|
| start QCA      | step <a href="#">6</a> |
| stop QCA       | step <a href="#">7</a> |

- 6 Start QCA by typing  
**# servstart QCA**  
and pressing the Enter key.

*Example response*

Starting QCA through servstart  
QCA Started

Proceed to step [8](#).

- 7 Stop QCA by typing  
**# servstop QCA**  
and pressing the Enter key.

*Example response*

Stopping group using servstop  
Attempting to stop local QCA on port: 20000  
QCA stopped successfully  
QCA stopped

- 8 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

## Clearing the JWS cache on a client workstation

### Application

Use this procedure to clear the Java™ Web Start (JWS) cache on a client workstation.

The JWS cache on a client workstation needs to be cleared after an HTTPS certificate is installed on an existing Sun server that was not previously using a certificate. Clearing the cache allows you to properly launch the CS 2000 Management Tools client applications from your workstation.

### Prerequisites

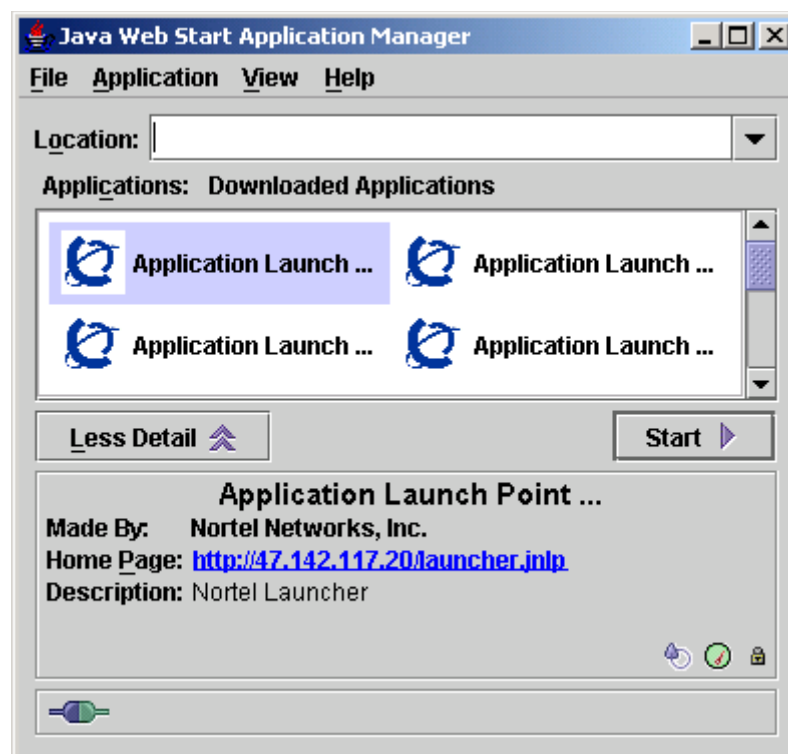
None

### Action

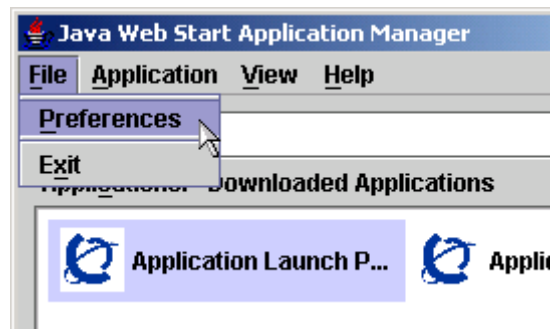
Perform the following steps to complete this procedure.

#### *At your workstation*

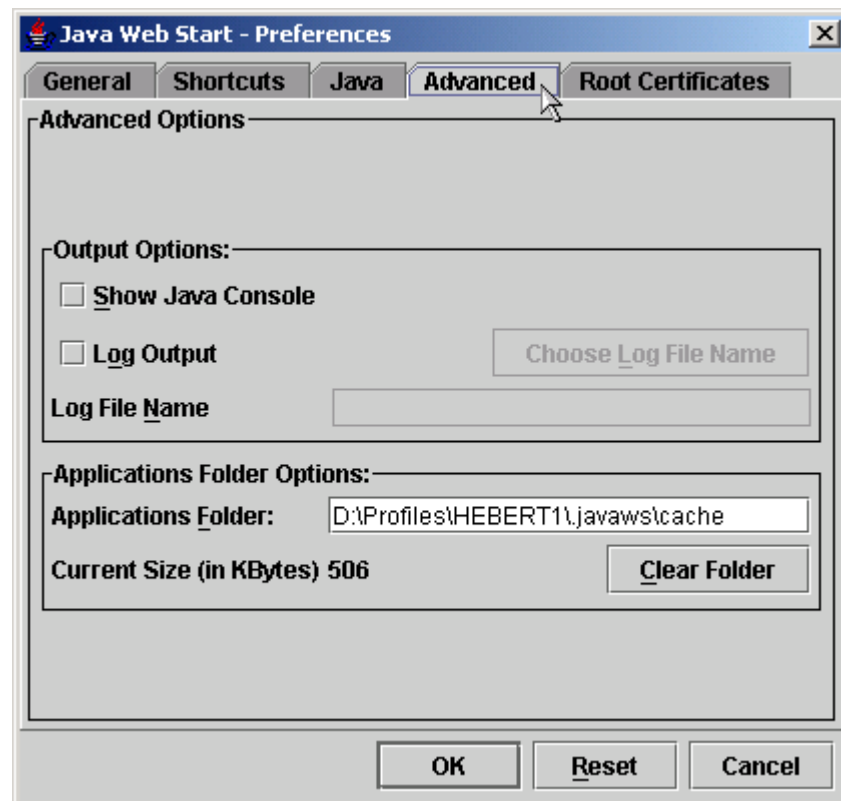
- 1 Access the Java Web Start Application Manager.



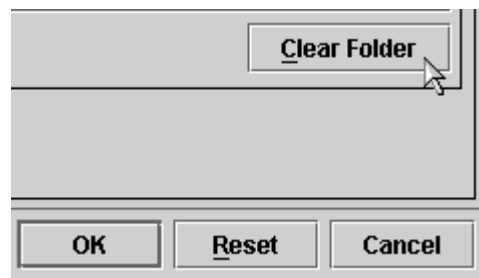
- 2 Click **File->Preferences** to access the Preferences window.



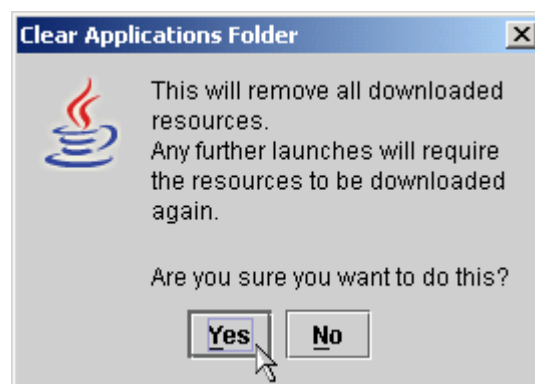
- 3 Click the **Advanced** tab to access the Advanced window.



- 4 Click **Clear Folder** to clear the cache.



- 5 Click **Yes** to confirm you want to clear the cache (remove all downloaded resources).



- 6 Click **OK** to close the Preferences window.
- 7 Exit the Java Web Start Application Manager.  
You have completed this procedure.

## Starting the OMPUSH server application

### Application

Use this procedure to start the OMPUSH server application.

**Note:** The OMPUSH server application is automatically started with SSPFS.

### Prerequisites

The Succession Server Platform Foundation Software (SSPFS) must be at release (I)SN06.2 or higher.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SSPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Determine the status of the OMPUSH server application by typing  

```
$ ompush_ctl -status
```

and pressing the Enter key.

| If the OMPUSH server application | Do                                |
|----------------------------------|-----------------------------------|
| is not running                   | step <a href="#">4</a>            |
| is running                       | you have completed this procedure |

- 4 Start the OMPUSH server application by typing

```
$ ompush_ctl -start
```

and pressing the Enter key.

*Example response:*

```
Tue May 22 19:13:38 2003: start ompush command.
The OMPUSH start command was sent.
```

You have completed this procedure.



---

## Stopping the OMPUSH server application

---

### Application

Use this procedure to stop the OMPUSH server application.

### Prerequisites

The Server Platform Foundation Software (SPFS) must be at release (I)SN06.2 or higher.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

  
and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Determine the status of the OMPUSH server application by typing  

```
$ ompush_ctl -status
```

  
and pressing the Enter key.

| If the OMPUSH server application | Do                                |
|----------------------------------|-----------------------------------|
| is running                       | step <a href="#">4</a>            |
| is not running                   | you have completed this procedure |

- 4 Stop the OMPUSH server application by typing

```
$ ompush_ctl -stop
```

and pressing the Enter key.

*Example response:*

```
Tue May 22 19:13:38 2003: start ompush command.
The OMPUSH stop command was sent.
```

You have completed this procedure.

---

## Cleaning up old data in the NPM database

---

### Application

Use this procedure to clean up the old data in the Network Patch Manager (NPM) database following an upgrade.

**ATTENTION**

This procedure includes stopping and starting the NPM, which has the NPM re-discover the patches on the system when the NPM is brought back into service. This can take several hours depending on office configuration. Therefore, ensure patching tasks are not planned or scheduled in the timeframe you want to perform this procedure.

**ATTENTION**

This procedure purges any user-defined reports, tasks, sets, plans and alarms, disables any enabled plans such as AUTOAPPLY and AUTORESTART, releases any patches or devices on hold, and unconfigures the Patch File Receipt System (PFRS). Therefore, you will need to re-define any user-defined reports, tasks, sets, plans, and alarms, re-enable any plans such as AUTOAPPLY and AUTORESTART, place any desired patches or devices on hold, and re-configure PFRS following this procedure.

### Prerequisites

You must have root user privileges to perform this procedure.

### Action

Perform the following steps to complete this procedure.

**At your workstation**

- 1 Generate and save a patchlist report using the NPM CLUI or GUI.

**Note:** The patchlist report may be useful in the event the apply time information is required at a later time.

| If using the | Do                     |
|--------------|------------------------|
| CLUI         | step <a href="#">2</a> |
| GUI          | step <a href="#">3</a> |

- 2 Using the NPM CLUI, generate and save a patchlist as follows:

- a Log in to the server by typing
 

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server**  
 is the IP address or host name of the SSPFS-based server on which you want to generate the report
- b When prompted, enter your user ID and password.
- c Change to the root user by typing
 

```
$ su -
```

 and pressing the Enter key.
- d When prompted, enter the password for the root user.
- e Change directory to /data/npm by typing
 

```
cd /data/npm
```

 and pressing the Enter key.
- f Determine if a tmp directory exists in the npm directory by typing
 

```
ls -l
```

 and pressing the Enter key.
- g Use the following table to determine your next step.

| If                     | Do                        |
|------------------------|---------------------------|
| a tmp directory exists | substep <a href="#">i</a> |
| otherwise              | substep <a href="#">h</a> |

- h** Create a tmp directory by typing  
`# mkdir tmp`  
and pressing the Enter key.
- i** Change directory to the tmp directory by typing  
`# cd tmp`  
and pressing the Enter key.
- j** Generate the patchlist report by typing  
`$ npm q patchlist output <filename>.list`  
and pressing the Enter key.  
where

**filename**

is the name you want to give to the patchlist report

**Example**

```
npm q patchlist output aug032004.list
```

**Example response**

```
Enter the NPM Succession user id and
password.
Login
```

- k** When prompted, enter the NPM user ID.

**Example response**

```
password
```

- l** When prompted, enter the NPM user password.

**Example response**

```
Redirecting output to: aug032004.list
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
Redirecting output to standard I/O
```

- m** Display the file by typing

```
$ ls
```

and pressing the Enter key.

Example response

```
aug032004.list
local.login
local.cshrc
local.profile
```

- n** If required, display the contents of the file by typing

```
$ cat <filename> |more
```

and pressing the Enter key.

where

**filename**

is the name you gave to the patchlist report file

**Example**

```
cat aug032004.list
```

Example response

```
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
```

- 3** Using the NPM GUI, generate and save a patchlist as follows:
- a** Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 537](#).
  - b** On the **Tasks** menu, click **Reports....**
  - c** Click the **Report List** tab to display the list of defined reports.
  - d** Click on **PATCHLIST**, and then click **Execute** to generate the PATCHLIST report.  
The **Reports Results** window is displayed.
  - e** Click **Save** to save the results of the PATCHLIST report and specify the filename and location to save the report.  
The **Save** window is displayed.

- f** Enter a name for the saved report in the **File name** field and then click **Save**.
  - g** Click **Close** to close the Reports Results window.
  - h** Click **Close** to close the Reports window.
  - i** On the Edit menu, Click **Preferences**.
  - j** Click on the **System Preferences** tab.  
Copy and paste the data on display including that in the Delete Patches from the Drop Box after Retrieval checkbox.
- 4** Log in to the server by typing  
`> telnet <server>`  
and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SSPFS-based server where the NPM resides
- 5** When prompted, enter your user ID and password.
- 6** Change to the root user by typing  
`$ su - root`  
and pressing the Enter key.
- 7** When prompted, enter the root password.
- 8** Stop the NPM server application by typing  
`# servstop NPM`  
and pressing the Enter key.

**9** Access the command line interface by typing

# **cli**

and pressing the Enter key.

*Example response*

Command Line Interface

1 - View

2 - Configuration

3 - Other

X - exit

select -

**10** Enter the number next to the “Configuration” option in the menu.*Example response*

Configuration

1 - NTP Configuration

2 - Apache Proxy Configuration

3 - DCE Configuration

4 - OAMP Application Configuration

5 - CORBA Configuration

6 - IP Configuration

7 - DNS Configuration

8 - Syslog Configuration

9 - Database Configuration

10 - NFS Configuration

11 - Bootp Configuration

12 - Restricted Shell Configuration

13 - Security Services Configuration

14 - Login Session

15 - Location Configuration

16 - Cluster Configuration

17 - Succession Element Configuration

18 - snmp\_poller (SNMP Poller Configuration)

X - exit

Select -



- 11** Enter the number next to the “Succession Element Configuration” option in the menu.

*Example response*

```
Succession Element Configuration
1 - NPM Application Configuration
2 - SAM21EM Application Configuration
3 - PSE Application Configuration
4 - OMPUSH Application Configuration
```

```
X - exit
```

```
select -
```

- 12** Enter the number next to the “NPM Application Configuration” option in the menu.

*Example response*

```
NPM Application Configuration
1 - CreateDB (Initialize or re-initialize the
 NPM database)
2 - ConfigureNpm (Configure the Network Patch
 Manager)
```

```
X - exit
```

```
select -
```

- 13** Enter the number next to the “CreateDB” option in the menu.

Allow to complete.

- 14** Exit each menu level of the command line interface to eventually return to the root level, by typing

```
select - x
```

and pressing the Enter key.

- 15** Start the NPM server application by typing

```
servstart NPM
```

and pressing the Enter key.

- 16** If any user-defined reports, tasks, sets, plans, or alarms existed prior to this procedure, re-define them using the corresponding procedure:
- for reports, use procedure “Defining reports using the NPM” in the Patching section of *Carrier Voice Over IP Network Upgrade*, NN10408-900
  - for tasks, use procedure “Saving a task using the NPM” in the Patching section of *Carrier Voice Over IP Network Upgrade*, NN10408-900
  - for sets, use procedure “Defining sets using the NPM” in the Patching section of *Carrier Voice Over IP Network Upgrade*, NN10408-900
  - for plans, use procedure “Defining a plan using the NPM” in the Patching section of *Carrier Voice Over IP Network Upgrade*, NN10408-900
  - for alarms, use procedure “Defining alarms using the NPM” in the *ATM/IP Solution-level Fault Management*, NN10408-900.
- 17** If any patches or devices were on hold prior to this procedure, place them back on hold using procedure “Setting field values using the NPM” in the Patching section of *Carrier Voice Over IP Network Upgrade*, NN10408-900.
- 18** If any plans such as AUTOAPPLY and AUTORESTART, were enabled prior to this procedure, re-enable them using procedure “Modifying a plan using the NPM” in the Patching section of *Carrier Voice Over IP Network Upgrade*, NN10408-900.
- 19** If PFRS was configured prior to this procedure, re-configure it using procedure “Configuring NPM for automatic patch file delivery” in the Patching section of *Carrier Voice Over IP Network Upgrade*, NN10408-900.

**Note:** If any users were logged in to the NPM GUI prior to this procedure, they must exit and re-launch the GUI. A re-connect to the NPM server from the GUI is not sufficient to clean up old data showing up in the GUI.

You have completed this procedure.

---

## Initializing the NPM database

---

### Application

Use this procedure to initialize the Network Patching Manager (NPM) database.

#### ATTENTION

This procedure purges any user-defined reports, tasks, sets, plans and alarms, disables any enabled plans such as AUTOAPPLY and AUTORESTART, releases any patches or devices on hold, and unconfigures the Patch File Receipt System (PFRS). Therefore, you will need to re-define any user-defined reports, tasks, sets, plans, and alarms, re-enable any plans such as AUTOAPPLY and AUTORESTART, place any desired patches or devices on hold, and re-configure PFRS following this procedure.

### Prerequisites

Only the root user can perform this procedure.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SPFS-based server where NPM resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

**5** Access the command line interface by typing

# **cli**

and pressing the Enter key.

*Example response*

Command Line Interface

1 - View

2 - Configuration

3 - Other

X - exit

select -

**6** Enter the number next to the “Configuration” option in the menu.*Example response*

Configuration

1 - NTP Configuration

2 - Apache Proxy Configuration

3 - DCE Configuration

4 - OAMP Application Configuration

5 - CORBA Configuration

6 - IP Configuration

7 - DNS Configuration

8 - Syslog Configuration

9 - Database Configuration

10 - NFS Configuration

11 - Bootp Configuration

12 - Restricted Shell Configuration

13 - Security Services Configuration

14 - Login Session

15 - Location Configuration

16 - Cluster Configuration

17 - Succession Element Configuration

18 - snmp\_poller (SNMP Poller Configuration)

X - exit

Select -

- 7** Enter the number next to the “Succession Element Configuration” option in the menu.

*Example response:*

```
Succession Element Configuration
1 - NPM Application Configuration
2 - SESM Application Configuration
3 - SAM21EM Application Configuration
4 - PSE Application Configuration
5 - RESMON Application Configuration
6 - OMPUSH Application Configuration
```

```
X - exit
```

```
select -
```

- 8** Enter the number next to the “NPM Application Configuration” option in the menu.

*Example response*

```
NPM Application Configuration
1 - CreateDB (Initialize or re-initialize the
 NPM database)
2 - ConfigureNpm (Configure the Network Patch
 Manager)
```

```
X - exit
```

```
select -
```

- 9** Enter the number next to the “CreateDB” option in the menu.

- 10** Exit each menu level of the command line interface to eventually return to the root level, by typing

```
select - x
```

and pressing the Enter key.

- 11** If any user-defined reports, tasks, sets, plans, or alarms existed prior to this procedure, re-define them using the corresponding procedure:

- for reports, refer to procedure “Defining reports using the NPM” in the Carrier Voice Over IP Network Upgrade document, NN10440-450
- for tasks, refer to procedure “Defining a task using the NPM” in the Carrier Voice Over IP Network Upgrade document, NN10440-450

- for sets, refer to procedure “Defining sets using the NPM” in the Carrier Voice Over IP Network Upgrade document, NN10440-450
  - for plans, refer to procedure “Defining a plan using the NPM” in the Carrier Voice Over IP Network Upgrade document, NN10440-450
  - for alarms, use procedure “Defining alarms using the NPM” in the ATM/IP solution-level Fault Management document, NN10408-900.
- 12** If any patches or devices were on hold prior to this procedure, place them back on hold using procedure “Setting field values using the NPM” in the Carrier Voice Over IP Network Upgrade document, NN10440-450.
- 13** If any plans such as AUTOAPPLY and AUTORESTART, were enabled prior to this procedure, re-enable them using procedure “Modifying a plan using the NPM” in the Carrier Voice Over IP Network Upgrade document, NN10440-450 .
- 14** If PFRS was configured prior to this procedure, re-configure it using procedure “Configuring the NPM for automatic patch file delivery” in the ATM/IP solution-level Configuration document, NN10409-500.

**Note:** If any users were logged in to the NPM GUI prior to this procedure, they must exit and re-launch the GUI. A re-connect to the NPM server from the GUI is not sufficient to clean up old data showing up in the GUI.

You have completed this procedure.

---

## Viewing patching information for the SPFS

---

### Application

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

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ***At your workstation***

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

#### *Example response*

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

X - exit

select -
```

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

*Example response*

Other

- 1 - Log Rotation
- 2 - capt\_files (Capture Various SSPFS Files/Logs For Debugging Purposes)
- 3 - sun\_explorer (Execute the Sun Explorer Data Gathering Tool)
- 4 - mount\_image (Mount A Generic Iso Image To The SSPFS Unit)
- 5 - umount\_image (Un-Mount A Generic Iso Image From the SSPFS Unit)
- 6 - disp\_sspfspatch (Display the patching status of the SSPFS unit)

X - exit

select -

- 7 Enter the number next to the "disp\_sspfspatch" option in the menu.

*Example response:*

===Executing "disp\_sspfspatch"

| SSPFS Patch | Installed | Applied |
|-------------|-----------|---------|
| =====       |           |         |
| SSPFS07MA   | Yes       | Yes     |
| SSPFS07MB   | Yes       | Yes     |

=="disp\_sspfspatch" completed successfully

**Note:** If no SSPFS patches are installed, the response will display "No SSPFS Patches Installed on This Unit".

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

select - **x**

and pressing the Enter key.

You have completed this procedure.



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

### Application

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

- [Simplex configuration \(one server\) on page 594](#)
- [High-availability configuration \(two servers\) on page 599](#)

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

The Succession Server Platform Foundation Software (SSPFS) creates file systems to best fit the needs of applications. However, it may be necessary to increase the size of a file system.

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

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

### SSPFS file systems

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

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

## Prerequisites

It is recommended that you back up your file systems and oracle data (if applicable) prior to performing this procedure. Refer to procedures [Performing a backup of oracle data on an SSPFS-based server on page 168](#) and [Performing a backup of file systems on an SSPFS-based server on page 174](#) if required.

## Action

Perform the following steps to complete this procedure.

### Simplex configuration (one server)

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

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

**a** Access the command line interface by typing

```
cli
```

and pressing the Enter key.

*Example response*

```
Command Line Interface
```

```
1 - View
```

```
2 - Configuration
```

```
3 - Other
```

```
X - exit
```

```
select -
```

**b** Enter the number next to the “View” option in the menu.

*Example response*

```
View
```

```
1 - sspfs_soft (Display Software
Installation Level Of SSPFS)
```

```
2 - chk_sspfs (Check SSPFS Processes)
```

```
3 - sw_conf (The software configuration of
the znc0s0jx)
```

```
4 - cpu_util (Overall CPU utilization)
```

```
5 - cpu_util_proc (CPU utilization by
process)
```

```
6 - port_util (I/O port utilization)
```

```
7 - disk_util (Filesystem utilization)
```

```
X - exit
```

```
select -
```

- c Enter the number next to the “disk\_util” option in the menu.

*Example response*

```

=== Executing "disk_util"

Filesystem kbytes used avail capacity Mounted on
/dev/md/dsk/d2 4129290 1892027 2195971 47% /
/proc 0 0 0 0% /proc
fd 0 0 0 0% /dev/fd
mnttab 0 0 0 0% /etc/mnttab
/dev/md/dsk/d8 2053605 155600 1836397 8% /var
swap 3505488 40 3505448 1% /var/run
swap 524288 448 523840 1% /tmp
/dev/md/dsk/d11 5161437 1428691 3681132 28% /opt
/dev/md/dsk/d23 2031999 34313 1936727 2% /PROU_data
/dev/md/dsk/d24 2031999 169042 1801998 9% /audio_files
/dev/md/dsk/d20 3080022 294615 2723807 10% /data
/dev/md/dsk/d25 949455 440344 452144 50% /user_audio_files
/dev/md/dsk/d21 3080022 275962 2742460 10% /opt/nortel
/dev/md/dsk/d22 12386331 10337214 1925254 85% /data/oradata
/dev/md/dsk/d26 122847 1041 109522 1% /data/qca

=== "disk_util" completed successfully

```

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

- 6 Note the file system you want to increase, as well as its current size (under column “Kbytes”).
- 7 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

8

#### ATTENTION

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

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

For example, to determine the size by which to increase the “qca” file system, subtract its current size, 122847k from the desired size, for example, 256000k. You would increase the size of the “qca” file system by 133153k, or 133MB.

- 9** Determine the amount of free disk space that can be allocated to file systems as follows:
- a** Determine the amount of free disk space on your system by typing  

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

and pressing the Enter key.
  - b** Divide the number of free blocks from step [a](#) by 2048 to obtain the number of free megabytes.
  - c** Subtract 9000 from the number of free megabytes from step [b](#) to obtain the number of free megabytes that can be allocated to existing file systems.

| If the value is    | Do                                     |
|--------------------|----------------------------------------|
| less than zero (0) | contact Nortel Networks for assistance |
| more than zero (0) | step <a href="#">d</a>                 |

- d** Use the following table to determine your next step.

| If                                                                                                                                                                                                                            | Do                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| the value you determined in step <a href="#">8</a> (size by which to increase the file system) is greater than the value you obtained in step <a href="#">9a</a> (amount of free disk space you can allocate to file systems) | contact Nortel Networks for assistance |
| the value you determined in step <a href="#">8</a> (size by which to increase the file system) is less than the value you obtained in step <a href="#">9a</a> (amount of free disk space you can allocate to file systems)    | step <a href="#">10</a>                |

## 10

**ATTENTION**

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

Increase the size of the file system by typing

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

Where

**mount\_point**

is the name of the file system you want to increase (noted in step [6](#))

**size**

is the size in megabytes (m) by which you want to increase the file system (determined in step [8](#))

**Example**

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

**Note:** The example above increases the “/data” file system by 512 megabytes (MB).

You have completed this procedure.

## High-availability configuration (two servers)

### ATTENTION

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

### At your workstation

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

| If using          | Do                     |
|-------------------|------------------------|
| telnet (unsecure) | step <a href="#">2</a> |
| ssh (secure)      | step <a href="#">6</a> |

- 2 Log in to the Inactive node by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the physical IP address of the Inactive node in the cluster  
**Note:** If you use the cluster IP address, you will log in to the Active node. Therefore, ensure you use the physical IP address of the Inactive node to log in.
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 5 When prompted, enter the root password.  
**Note:** Ensure you are on the Inactive server by typing `ubmstat`. If `ClusterIndicatorACT` is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorSTBY`, which indicates you are on the Inactive server.
- 6 Log in using ssh (secure) as follows:

- a Log in to the server by typing
- ```
> ssh -l root <server>
```
- and pressing the Enter key.

where

server

is the physical IP address of the inactive server

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

- b When prompted, enter the root password.

At the Inactive node

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

```
# ubmstat
```

and pressing the Enter key.

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

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

```
# udfstat
```

and pressing the Enter key.

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

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

- a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

Command Line Interface

- 1 - View
- 2 - Configuration
- 3 - Other

X - exit

select -

- b** Enter the number next to the "View" option in the menu.

Example response

View

- 1 - sspfs_soft (Display Software Installation Level Of SSPFS)
- 2 - chk_sspfs (Check SSPFS Processes)
- 3 - sw_conf (The software configuration of the znc0s0jx)
- 4 - cpu_util (Overall CPU utilization)
- 5 - cpu_util_proc (CPU utilization by process)
- 6 - port_util (I/O port utilization)
- 7 - disk_util (Filesystem utilization)

X - exit

select -

- c** Enter the number next to the "disk_util" option in the menu.

Example response

```
=== Executing "disk_util"
```

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/md/dsk/d2	4129290	1892027	2195971	47%	/
/proc	0	0	0	0%	/proc
fd	0	0	0	0%	/dev/fd
mnttab	0	0	0	0%	/etc/mnttab
/dev/md/dsk/d8	2053605	155600	1836397	8%	/var
swap	3505488	40	3505448	1%	/var/run
swap	524288	448	523840	1%	/tmp
/dev/md/dsk/d11	5161437	1428691	3681132	28%	/opt
/dev/md/dsk/d23	2031999	34313	1936727	2%	/PROU_data
/dev/md/dsk/d24	2031999	169042	1801998	9%	/audio_files
/dev/md/dsk/d20	3080022	294615	2723807	10%	/data
/dev/md/dsk/d25	949455	440344	452144	50%	/user_audio_files
/dev/md/dsk/d21	3080022	275962	2742460	10%	/opt/nortel
/dev/md/dsk/d22	12386331	10337214	1925254	85%	/data/oradata
/dev/md/dsk/d26	122847	1041	109522	1%	/data/qca

```
=== "disk_util" completed successfully
```

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

- 10 Note the file system you want to increase, as well as its current size (under column *Kbytes*).
- 11 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

12

ATTENTION

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

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

For example, to determine the size by which to increase the “qca” file system, subtract its current size, 122847k from the desired size, for example, 256000k. You would increase the size of the “qca” file system by 133153k, or 133MB.

- 13 Determine the amount of free disk space that can be allocated to file systems as follows:
 - a Determine the amount of free disk space on your system by typing

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

and pressing the Enter key.
 - b Divide the number of free blocks from step [a](#) by 2048 to obtain the number of free megabytes.

- c Subtract 9000 from the number of free megabytes from step [b](#) to obtain the number of free megabytes that can be allocated to existing file systems.

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

- d Use the following table to determine your next step.

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

14

ATTENTION

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

Increase the size of the desired file system by typing

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

Where

mount_point

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

size

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

Example

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

Note: The example above increases the “/data/qca” file system by 10 megabytes (MB).

- 15** Reboot the Inactive node by typing

```
# init 6
```

and pressing the Enter key.

- 16** Wait for the Inactive node to reboot, then log in again using its physical IP address.

- 17** Verify the status of file systems on the Inactive node by typing

```
# udfstat
```

and pressing the Enter key.

If the file systems are	Do
STANBY normal UP clean	step 18
not STANBY normal UP clean	contact your next level of support

- 18** Log in to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

is the physical IP address of the active node in the cluster

- 19** When prompted, enter your user ID and password.

- 20** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 21** When prompted, enter the root password.

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

ClusterIndicatorACT, which indicates you are on the Active server.

At the Active node

- 22** Stop the cluster by typing

StopCluster

and press the Enter key.

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

At the newly Active node

- 23** Clone the other node using procedure [Cloning the image of one node in a cluster to the other node on page 502](#) if required.

You have completed this procedure.

Verifying disk utilization on an SPFS-based server

Application

Use this procedure to verify disk utilization by the file systems on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

You must have root user privileges.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Log in to the server by typing
`> telnet <server>`
and pressing the Enter key.
where
server
is the IP address or host name of the SPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing
`$ su - root`
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Access the command line interface by typing
`# cli`
and pressing the Enter key.

Example response

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

X - exit

select -
```

- 6 Display the current disk capacity utilization as follows:
- a Enter the number next to the “View” option in the menu.

Example response

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

X - exit

select -
```

- b Enter the number next to the “disk_util” option in the menu.

Example response

```
=== Executing "disk_util"

Filesystem      kbytes  used  avail capacity  Mounted on
/dev/md/dsk/d2  4129290 1892027 2195971    47%    /
/proc           0         0         0     0%    /proc
fd              0         0         0     0%    /dev/fd
mnttab          0         0         0     0%    /etc/mnttab
/dev/md/dsk/d8  2053605 155600 1836397     8%    /var
swap            3505488   40 3505448     1%    /var/run
swap            524288   448 523840     1%    /tmp
/dev/md/dsk/d11 5161437 1428691 3681132    28%    /opt
/dev/md/dsk/d23 2031999   34313 1936727     2%    /PROU_data
/dev/md/dsk/d24 2031999 169042 1801998     9%    /audio_files
/dev/md/dsk/d20 3080022 294615 2723807    10%    /data
/dev/md/dsk/d25  949455 440344 452144    50%    /user_audio_files
/dev/md/dsk/d21 3080022 275962 2742460    10%    /opt/nortel
/dev/md/dsk/d22 12386331 10337214 1925254    85%    /data/oradata
/dev/md/dsk/d26  122847   1041 109522     1%    /data/qca

=== "disk_util" completed successfully
```

You have completed this procedure.

Installing or replacing an HTTPS certificate on an SSPFS-based server

Application

Use this procedure to install an HTTPS certificate on a Succession Server Platform Foundation Software (SSPFS)-based server. An HTTPS certificate enables secure transmission of communications, and is required from the SN07 release onward.

The steps to create a self-signed certificate are included in this procedure if you choose to use a self-signed certificate (see [Types of certificates](#)).

Types of certificates

Following, are the three types of security certificates that can be used. These certificates differ in the level of trust that needs to be assigned to a server.

- a certificate granted from a well known certificate authority (CA): used when the server is used in a public way, such as for e-commerce web sites
- a company-generated certificate: used when the server is used internally, and the operating company has its own internal CA
- a self-signed certificate created locally on the server: used when the server is used in a more restricted manner.

Note: When a server with a self-signed certificate is accessed, the browser presents the certificate and asks whether the certificate can be trusted. If the user answers “yes”, the server can be accessed. If the user answers “no”, nothing further will be received from the server.

Prerequisites

This procedure has the following prerequisites:

- The domain name service (DNS) must be enabled on the server to allow the security certificate to work, and must be enabled prior to the installation of the certificate. Refer to procedure “Configuring Domain Name Service” in the ATM/IP Solution-level Configuration Management document, NN10409-500.
- If purchasing a certificate from a third-party certificate authority (CA), such as VeriSign, obtain a PEM-encoded X.509 certificate, but without a passcode.

Note: The name of the certificate should match the host name of the server. Nortel Networks recommends the installation of a unique certificate for each host. A separate file contains the key, and should not have an associated password.

- Make sure all GUI screens are closed before you install the certificate.
- The RSA key for the HTTPS certificate must not have a password.
- The certificate must be created with the fully qualified domain name (FQDN) of the server on which the certificate will be installed.
- Sub-directories “ssl.crt” and “ssl.key” must already exist in the “/opt/apache/conf” directory.

Action

Use one of the methods below to install the certificate according to your office configuration:

- [Simplex configuration \(one server\) on page 609](#)
- [High-availability configuration \(two servers\) on page 614](#)

Simplex configuration (one server)

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

is the IP address or host name of the SSPFS-based server on which you want to install the HTTPS certificate

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

If you are	Do
using a self-signed certificate	step 5
not using a self-signed certificate	step 6

5 Create the self-signed certificate as follows:

a Access the “conf” directory by typing

```
# cd /opt/apache/conf
```

and pressing the Enter key.

b Generate the key file (server.key) by typing

```
# /opt/openssl/bin/openssl genrsa -rand  
/var/log/sspfslog 1024 > server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -rand and /var/log/sspfslog entries.

- c Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key  
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -key and server.key entries.

Example response:

```
You are about to be asked to enter information  
that will be incorporated into your  
certificate request.  
What you are about to enter is what is called  
a Distinguished Name or a DN.  
There are quite a few fields but you can leave  
some blank.  
For some fields there will be a default value.  
If you enter '.', the field will be left blank.  
-----
```

```
Country Name (2 letter code) [AU]:
```

- d When prompted, enter a two letter code for the country where the server is located.

Example response:

```
State or Province Name (full name)  
[Some-State]:
```

- e When prompted, enter the full name of the State or Province where the server is located.

Example response:

```
Locality Name (eg, city) []:
```

- f When prompted, enter the city where the server is located.

Example response:

```
Organization Name (eg, company) [Internet  
Widgits Pty Ltd]:
```

- g When prompted, enter the name of the company that owns the server.

Example response:

```
Organizational Unit Name (eg, section) []:
```

- h When prompted, enter the name of the department that owns the server.

Example response:

Common Name (eg, YOUR name []):

- i When prompted, enter the fully qualified domain name (FQDN) of the server.

Example response:

Email Address []:

- j When prompted, enter the email address of the organization that owns the server.

- 6 Place the certificate file (server.crt) you obtained in “/opt/apache/conf/ssl.crt”.

Note: If directory “ssl.crt” does not exist, you need to create it.

- 7 Place the key file (server.key) you obtained in “/opt/apache/conf/ssl.key”.

Note: If directory “ssl.key” does not exist, you need to create it.

- 8 Change the certificate’s owner and group by typing

```
# chown root:other  
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between “other” and the directory path.

- 9 Change the key file’s owner and group by typing

```
# chown root:other  
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between “other” and the directory path.

- 10 Set the certificate permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

- 11 Set the key file permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

- 12** Restart the WEBSERVER as follows:

 - a** Stop the WEBSERVER by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.
 - b** Start the WEBSERVER by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.
- 13** Restart the WEBSERVICES as follows:

 - a** Stop the WEBSERVICES by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.
 - b** Start the WEBSERVICES by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.
- 14** If you installed an HTTPS certificate on an existing SSPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure “Clearing the JWS cache on a client workstation” in the ATM/IP Solution-level Configuration Management document, NN10409-500.
- 15** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

High-availability configuration (two servers)

At your workstation

- 1 Log in to the active server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the active server on which you want to install the HTTPS certificate
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

If you are	Do
using a self-signed certificate	step 5
not using a self-signed certificate	step 6

- 5 Create the self-signed certificate as follows:
 - a Access the “conf” directory by typing

```
# cd /opt/apache/conf
```

and pressing the Enter key.
 - b Generate the key file (server.key) by typing

```
# /opt/openssl/bin/openssl genrsa -rand /var/log/sspfslog 1024 > server.key
```

and pressing the Enter key.
Note: Enter the command on one line with a space between the -rand and /var/log/sspfslog entries.

- c Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key  
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -key and server.key entries.

Example response:

```
You are about to be asked to enter information  
that will be incorporated into your  
certificate request.  
What you are about to enter is what is called  
a Distinguished Name or a DN.  
There are quite a few fields but you can leave  
some blank.  
For some fields there will be a default value.  
If you enter '.', the field will be left blank.  
-----
```

```
Country Name (2 letter code) [AU]:
```

- d When prompted, enter a two letter code for the country where the server is located.

Example response:

```
State or Province Name (full name)  
[Some-State]:
```

- e When prompted, enter the full name of the State or Province where the server is located.

Example response:

```
Locality Name (eg, city) []:
```

- f When prompted, enter the city where the server is located.

Example response:

```
Organization Name (eg, company) [Internet  
Widgits Pty Ltd]:
```

- g When prompted, enter the name of the company that owns the server.

Example response:

```
Organizational Unit Name (eg, section) []:
```

- h When prompted, enter the name of the department that owns the server.

Example response:

Common Name (eg, YOUR name []):

- i When prompted, enter the fully qualified domain name (FQDN) of the server.

Example response:

Email Address []:

- j When prompted, enter the email address of the organization that owns the server.

- 6 Place the certificate file (server.crt) you obtained in “/opt/apache/conf/ssl.crt”.

Note: If directory “ssl.crt” does not exist, you need to create it.

- 7 Place the key file (server.key) in “/opt/apache/conf/ssl.key”.

Note: If directory “ssl.key” does not exist, you need to create it.

- 8 Change the certificate’s owner and group by typing

```
# chown root:other  
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between “other” and the directory path.

- 9 Change the key file’s owner and group by typing

```
# chown root:other  
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between “other” and the directory path.

- 10 Set the certificate permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

- 11 Set the key file permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

- 12 Restart the WEBSERVER as follows:
 - a Stop the WEBSERVER by typing
servstop WEBSERVER
and pressing the Enter key.
 - b Start the WEBSERVER by typing
servstart WEBSERVER
and pressing the Enter key.
- 13 Restart the WEBSERVICES as follows:
 - a Stop the WEBSERVICES by typing
servstop WEBSERVICES
and pressing the Enter key.
 - b Start the WEBSERVICES by typing
servstart WEBSERVICES
and pressing the Enter key.
- 14 Clone the image of the node with the HTTPS certificate onto the other node using procedure [Cloning the image of one node in a cluster to the other node on page 502](#).
- 15 If you installed an HTTPS certificate on an existing SSPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure “Clearing the JWS cache on a client workstation” in the ATM/IP Solution-level Configuration Management document, NN10409-500.
- 16 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Preparing a DVD-RW for use

Application

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At the server

- 1 Insert the DVD into the drive.

Note: Only rewriteable media can be erased. Verify that the DVD you are attempting to erase is a DVD-RW before inserting it into the drive.

At your workstation

- 2 Log in to the server by typing
 > **telnet** <server>
 and pressing the Enter key.
 where
 server
 is the IP address or hostname of the SSPFS-based server
- 3 When prompted, enter your user ID and password.
- 4 Use the following table to determine your next step.

If the DVD is	Do
new	step 5
used	step 6

- 5 Verify the DVD is ready for use by typing

```
$ cdrw -l
```

and pressing the Enter key

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

- 6 Erase the contents of the DVD by typing

```
$ cdrw -b all
```

and pressing the Enter key

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

- 7 Reinsert the DVD into the drive.

- 8 Verify the DVD is ready for use by typing

```
$ cdrw -l
```

and pressing the Enter key

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

- 9 Eject the DVD from the drive as follows:

- a** Ensure you are at the root directory level by typing

```
$ cd /
```

and pressing the Enter key.

b Eject the DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

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

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

Then, press the eject button located on the front of the DVD drive.

c Remove the DVD from the drive.

10 Obtain another DVD and repeat the process starting with step [4](#).

11 Proceed to use the DVD.

You have completed this procedure.

Changing the PMGRdaemon password

This procedure enables you to change the Windows Administrator password and the 'Logon' password for the PMGRdaemon service.

ATTENTION

When changing the administrator password for the machine you must also change the 'Logon' password for the PMGRdaemon service.

At the Windows desktop interface

- 1 Right click the "My Computer" icon on the desktop.
- 2 Select "Manage" from the pop-up menu. The Computer Management window opens.
- 3 Under "System Tools", expand the "Local Users and Groups" folder.
- 4 Open the "Users" folder.
- 5 In the right panel of the Computer Management window, right click the "Administrator" icon.
- 6 Select "Set Password" from the pop-up menu. The Set Password window opens.
- 7 In the Set Password window, enter the new password in the "New password" dialog box.
- 8 Enter the new password in the "Confirm password" dialog box.
- 9 Click "OK". The Set Password window closes.
- 10 From the Computer Management window, expand the "Services and Applications" folder.
- 11 Open the "Services" folder.
- 12 In the right panel of the Computer Management window, right click the "PMGRdaemon service" icon and select "Properties".
- 13 When the PMGRdaemon Properties dialog box opens, select the logon tab.
- 14 Make sure the user is set to '.\Administrator'.
- 15 Enter the new password.
- 16 Confirm the new password.

Note: You must log off and back on to the system once you change the passwords.

- 17** Close all windows and log off and back on to the system.
- 18** You have completed this procedure.

ORCA BTX8 and BTX12 TGCP gateway administration overview

The Open Reliable Communication Architecture (ORCA) Broadband Telephony Exchange (BTX) products are VoIP media gateways that provide interworking between a PacketCable managed IP network and the PSTN. You can install and manage an ORCA gateway using the configuration software that is provided with the product (NueraView).

NueraView consists of two integrated products, Nuera Configurator and HP OpenView Network Node Manager. NueraView enables you to:

- set up an ORCA BTX application with the components required to provide network management functions through HP OpenView
- monitor all the ORCA gateways in a network
- recognize fault conditions and isolate the problem to a particular subsystem or network component
- generate performance reports
- define threshold-crossing alerts to detect degrading network performance

For instructions on how to manage the ORCA BTX8 and BTX21 TGCP gateways, refer to vendor-supplied documentation.

How to trace a call on a CS 2000

On a CS 2000, you can trace established intra-office and interoffice calls involving

- TDM circuit-switched technology
- dynamic packet trunks (DPTs) that use SIP-T signaling

Note: Not for DPTs that use BICC signaling.

To trace a call, use the SIPTRACE command. You can use this command in any level of the MAP user interface

You can use the SIPTRACE command to trace E911 calls and other calls as well.

Syntax of the SIPTRACE command

For a TDM call, the syntax of the SIPTRACE command is as follows:

SIPTRACE T <TDM-trunk-group> <TDM-trunk-member>

where

<TDM-trunk-group> is the common language location identifier (CLLI) of the TDM trunk group.

<TDM-trunk-member> is an integer in the range 0 to 9999

For a call on a DPT, the syntax of the command is as follows:

SIPTRACE D '<DPT-SIPT-callid>'

where

<DPT-SIPT-callid> is the DPT SIP-T call ID

Note: The DPT SIP-T call ID must be enclosed in single quotation marks, as shown above.

System response

The system response to the SIPTRACE command is as follows:

<input> is currently connected to <output>

Whenever you use a SIP-T callid as input for a SIPTRACE command, the system checks for a possible second trunk termination within the

same call server domain. Similarly, if the system finds that a SIP-T callid is the output of a SIPTRACE command, the system checks for a possible second trunk termination within the same call server domain.

For more information, see the following examples.

TDM to line interworking in the CS 2000

In this example, the input is a TDM trunk member. The system response indicates that it is connected to a line.

TDM to line interworking in the CS 2000

```
CI> SIPTRACE T ETSIV1LPA 2

TDM trunk ETSIV1LPA 2 is currently connected to LINE
1158206005
```

SIP-T DPT to line interworking in the CS 2000

In this example, the input is a SIP-T DPT callid. The system response indicates that it is connected to a line. The call scenario is as follows: Line 1158206005 --> SIP-T --> Line 1158206007.

SIP-T DPT to line interworking in the CS 2000

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K4SIP1LOOPFR3 callid
0026.4030-10-16-49-02.67@CS2K4_84 is currently connected
to LINE 1158206007
SIP-T DPT KSIP1LOOPFR3 callid
0026.4030-10-16-49-02.67@CS2K4_84 is currently connected
to LINE 1158206005
```

TDM to TDM interworking in the CS 2000

In this example, the input is a TDM trunk member. The system response indicates that it is connected to another TDM trunk member.

TDM to TDM interworking in the CS 2000

```
CI> SIPTRACE T ETSIV1LPB 2

TDM trunk ETSIV1LPB 2 is currently connected to TDM
trunk UKISUPLPA 10
```

TDM to SIP-T DPT interworking in CS 2000

In this example, the input is a TDM trunk member. The system response indicates that it is connected to a SIP-T DPT callid.

The call scenario is as follows:

Line 115820607 --> TDM ETSILPA 2

TDM ETSILPB 2 --> SIP-T --> Line 1158206008.

TDM to SIP-T DPT interworking in CS 2000

```
CI> SIPTRACE T ETSIV1LPB 2
```

```
TDM trunk ETSIV1LPB 2 is currently connected to  
SIP-T DPT K4SIP1LOOPFR3 callid  
0026.4030-10-16-49-02.67@CS2K4_84  
SIP-T DPT K4SIP1LOOPFR3 callid  
0026.4030-10-16-49-02.67@CS2K4_84 is currently connected to  
LINE 1158206008
```

SIP-T DPT to TDM interworking in CS 2000

In this example, the input is a SIP-T DPT callid. The system response indicates that it is connected to a TDM trunk member.

The call scenario is as follows:

Inter-call Server posted SIP-T --> TDM ETSILPA 2

TDM ETSILPB 2 --> SIP-T --> Line 1158206008.

SIP-T DPT to TDM interworking in CS 2000

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'
```

```
SIP-T DPT K1SIP1V1 callid  
0026.4030-10-16-49-02.67@CS2K4_84 is currently  
connected to TDM trunk ETSIV1LPA 2  
SIP-T DPT K1SIP1V1 callid 0026.4030-10-16-49-02.67@CS2K4_84  
not associated with any active call
```

Note: In this case, the SIPTRACE command cannot determine the other agent for an inter-call-server SIP-T DPT because another call server is involved. Therefore, the output shows that the SIPTRACE command execution in this call server could not determine the connected agent for the SIP-T leg belonging to another call-server domain. To determine the complete path of the call, the SIPTRACE command must be executed in successive call servers also.

Output TDM trunk member identified as a C7ISL member

In this example, the input is a TDM trunk member. The system response indicates that it is connected to a TDM trunk member that is

found to be a member of a C7ISL (ISUP signaling loopback) facility. In this case, the response displays the final agent of the call.

Output TDM trunk member identified as a C7ISL member

```
CI> SIPTRACE T ETSIV1LPB 2

TDM trunk ETSIV1LPB 2 is currently connected to TDM
trunk (C7ISL) ETSIV1LPA 3
TDM trunk (C7ISL) UKISUPLPA 4 is currently connected
to LINE 1158206005
```

Input TDM trunk member identified as a C7ISL member

In this example, the input is a TDM trunk member that is a member of a C7ISL (ISUP signaling loopback) facility. The system response indicates that it is connected to a TDM trunk member.

Input TDM trunk member identified as a C7ISL member

```
CI> SIPTRACE T ETSIV1LPB 2

TDM trunk (C7ISL) ETSIV1LPB 2 is currently connected to
TDM trunk UKISUPLPA 8
```

SIP-T looparound

In this case the system encounters a SIP-T callid as the output of the SIPTRACE command execution. The system then checks for a possible second trunk termination within the same call server domain.

The call scenario is as follows:

Line 1158206005 --> SIP-T --> SIP-T (posted) --> Line 1158206007.

SIP-T looparound

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K1SIP1UK3 callid
0026.4030-10-16-49-02.67@Cs2K4_84 is currently
connected to SIP-T DPT K1SIP1V1 callid
0026.4030-10-16-49-02.95@CS2K4_84
SIP-T DPT K2SIP1CZ1 callid
00026.4030-10-16-49-02.95@CS2K4_84 is currently
connected to LINE 1158206005
SIP-T DPT K1SIP1UK3 callid
0026.4030-10-16-49-02.67@CS2K4_84 is currently
connected to LINE 1158206007
```

Note: If the output of the SIPTRACE command involves a SIP-T DPT callid, we cannot predict the sequence in which the output

agents will be displayed in the output. The output sequence depends on the sequence in which the SIP-T GWC returns the DPT terminal IDs.