ATM/IP Solution-level Security and Administration

ATTENTION
This document addresses all Nortel Networks Succession solutions. Some statements may not apply to your solution.

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.

(I)SN07 features (Sheet 1 of 3)

Feature descriptions
CS 2000 feature **A00002585 -- TMM development for PTS trunk (PT-IP)** This feature extends TMM functionality to support the following: • PTS trunk maintenance will be supported by TMM. All maintenance commands related to ISUP trunk and PRI trunk will be supported for PTS trunk. • Post by carriers name - in addition to selecting a trunk gateway, the user can select a specific carrier name, post trunks and perform all maintenance operations supported by Maintenance by Gateway Name for ISUP, PRI, and PTS trunks from GUI and OSSGate. • General TMM robustness enhancements

(I)SN07 features (Sheet 2 of 3)

Feature descriptions

A00004422 -- E911 DPT SIP-T call trace (All solutions)

This feature provides the ability to identify which SIP-T DPT trunks and members (originating and terminating) are associated with a live call trace within the Succession network.

GWC feature

A00003575 -- GWC Security productization (IAC, Intl IAC)

IP Security (IPSec) capability is available in (I)SN07 for the following GWC line profiles:

- SMALL_LINENA
- SMALL_LINEINTL

A00003576 -- TGCP security (IAC, Intl IAC)

IP Security (IPSec) capability is available in (I)SN07 for the following GWC trunking profiles:

- TRUNKNA
- TRUNKINTL

The feature enables the IPSec provisioning panel on the CS 2000 GWC Manager GUI.

SSPFS feature

A00003613 -- NSDM configuration parameters (PT-IP)

This feature will add three configuration parameters to the existing SSPFS configuration, which will be configured via the existing cli tool. New menu options for each of these parameters will be added to the SSPFS cli tool.

- CM Internet Protocol (IP) address. This is the address by which the CM can be reached. This address should be reachable by the SSPFS through VLANs, which are defined in the network topology.
- Login greeting: a string that is displayed to remote Telnet users before they attempt to log in.
- System location: a string defining the physical location of the SSPFS server.

Centrex IP feature

(I)SN07 features (Sheet 3 of 3)

Feature descriptions
A00003717 -- CICM OSMINE readiness - flowthrough provisioning (Intl IAW) This feature provides the Centrex IP terminal flow-through provisioning. Flowthrough provisioning provides the capability for OSSGate clients to add, modify and delete Centrex IP terminal features stored in the CICM. This feature provides a means to provision Centrex IP terminals in the Succession network from a single interface. Customers access flow-through functionality via the OSSGate application when logged into Lines Provisioning. Prior to this activity, when provisioning new Centrex IP Client Manager (CICM) line terminations, it was necessary to provision the CICM datafill via the CICM Element Manager GUI and provision the Gateway Controller (GWC) and XA-Core datafill via the SESM OSSGate SERVORD+ interface. Flow-through provisioning reduces the need to perform both provisioning steps and provides an alternative to the CICM EM GUI interface which will facilitate terminal provisioning by third-party OSS applications. **A00005986 -- CICM EM integration with PAM+ proxy (Intl IAW)** This feature allows user authentication on the CICM element manager to be provided by the pluggable authentication module (PAM) on the SSPFS platform. **Traffic Office Position System (TOPS) feature** **A00005160 -- OSSAIN XA-CORE data messaging capacity enhancements (All solutions)** This feature enables OSSAIN data messaging to use XA-Core Ethernet interfaces such as the HIOP and the new HCMIC card. Prior to this activity, all OSSAIN messaging used the EIU (Ethernet Interface Unit). **MG 9000 feature** **A00005646 -- IPSEC SUPPORT FOR MG9K (UA-AAL1, UA-IP)** This feature implements IPSec for MG9000 Element Manager to MG9000 Line Gateway OAMP communications. The craftsperson will be able to independently manage IPSec parameters for all OAM&P communications to and from MG9000 network elements. This feature will enable/disable/modify IPSec on the OAM&P messaging channel from the MG9000 EM to an MG9000.

Overview of Security Architecture

The network security architecture for the IAC solution uses Internet Protocol Security (IPSec) to protect the traffic between the Gateway Controller (GWC) and other 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.

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) - for SAs between GWC and a Cable Modem Termination System (CMTS) or third-party Trunk Gateway Control Protocol (TGCP) gateways

  IKE creates an authenticated secure communication channel between the GWC and a gateway. 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 - for SAs between GWC and a Multimedia Terminal Adapter (MTA) line gateway

  Kerberos with Public Key support (using the PKINIT extension to the Kerberos IETF standard) is used to exchange keys and authenticate an MTA to a GWC. MTA authentication process with the GWC requires a PacketCable Key Distribution Center (KDC) server, which grants authentication tickets to the MTA. These tickets are used to authenticate an MTA to a GWC, 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 only used on the GWC and 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 GWC with the flexibility of accepting secure and non-secure messages, so IPSec can be activated on the GWC 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.

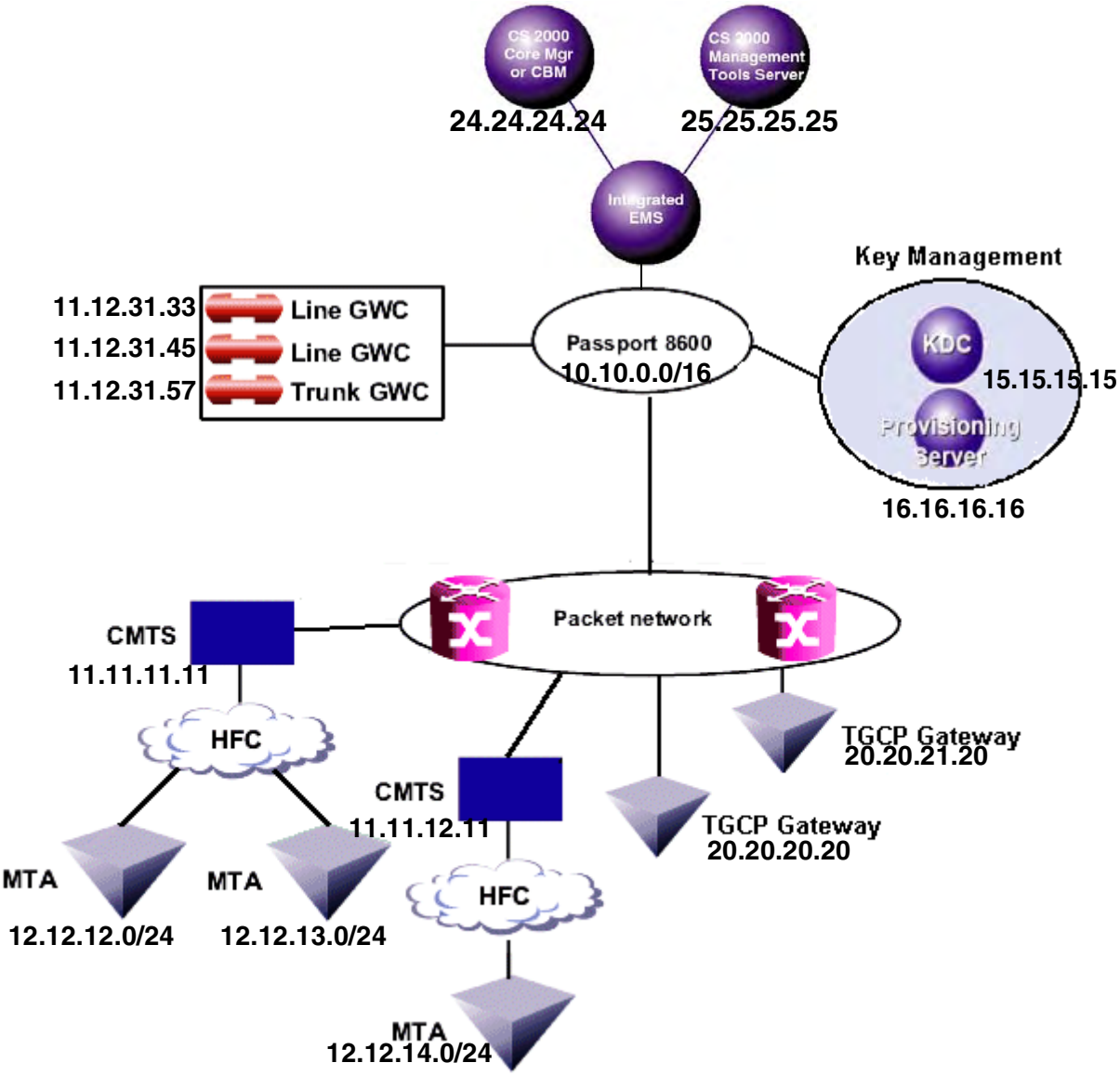
Configuring the network with security

Purpose of this procedure

This procedure provides a high-level overview of the steps necessary to configure IP Security (IPSec) in the IAC solution. 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.

When to use this procedure

Use this procedure to create the initial IPSec policy table after the network has been upgraded to SN07.

Prerequisites

The network must be upgraded to SN07.

IPSec has not been configured on any components.

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

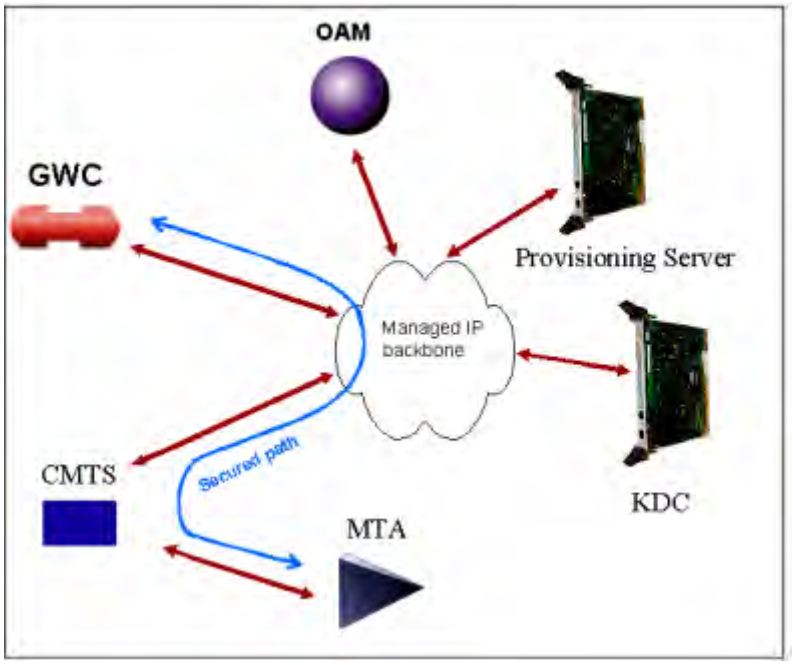
Action

Enabling IPSec in the network

1. 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.
2. 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.
3. Configure a Security policy for all network elements which require security.
4. To configure the MTA to Line GWC path for security, perform the following steps.

MTA to GWC path



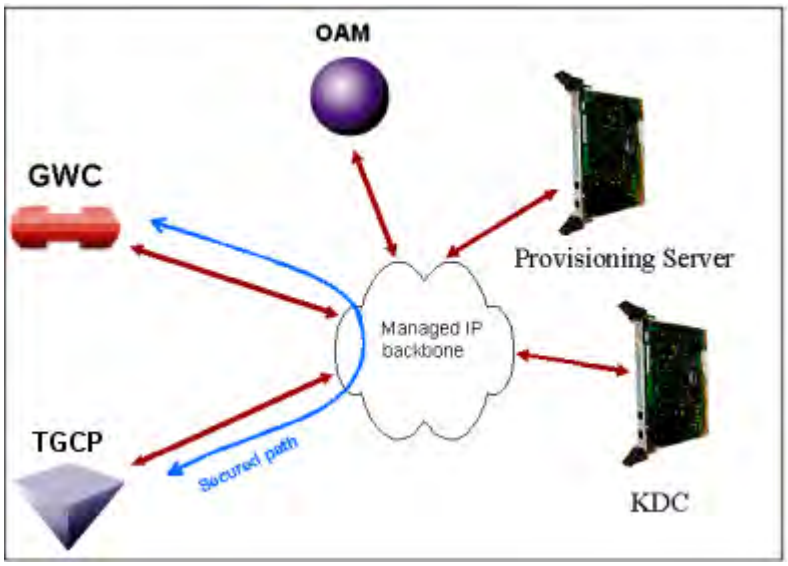
a Configure the GWC with Kerberos using the procedure "Configure Kerberos Key Management" located in *GWC Security and Administration*, NN10213-611.

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.

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

TGCP to GWC path

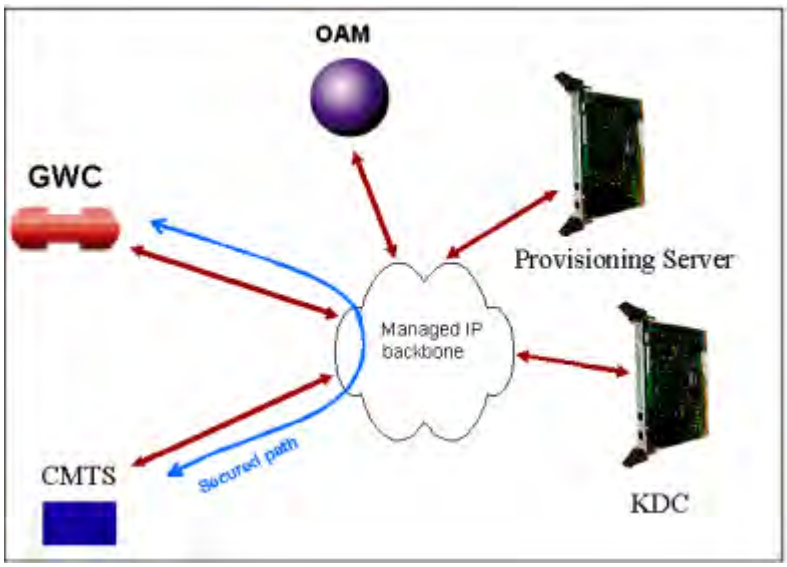


a Activate IPSec with Flex Policies using the procedure "Activate or de-activate IPSec using FLEX policy" located in *GWC Security and Administration*, NN10213-611.

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

6 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.

7 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 the IAC solution. This procedure does not disable security on any third-party devices, such as the Nuera Gateway, MTA, or CMTS. 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. 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.
2. 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 should be made during the backup and restore window.

ATTENTION

All related devices in the solution need to be backed up 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 should be backed up in the same window.

Correspondingly all related devices should 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	21
Call Agent	Call Agent backup	33
SAM21	none (See Note 1)	
GWC	none (See Note 1)	

Service data backup components

Component	Procedure (s)	Page
Session Server	Perform a database restore to a Session Server unit	148
CS 2000 CS LAN	Saving the Passport 8600 boot configuration file	31
UAS	Backing up UAS configuration files	36
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	 39 41 45 49 51 54
APS	Backing up the APS-specific Oracle database and application files	57
USP	Administration: OAM&P Workstation Backup	60
Real-time Transport Protocol (RTP) Media Portal	RTP Media Portal Basics, NN10367-111	
CICM	CICM Security and Administration, NN10252-611	
CORE NETWORK		
Passport devices	Basic service data backup	75
GATEWAYS		
MG 9000	none (See Note 1)	
MG 4000	none (See Note 2)	
IW SPM	none (See Note 2)	
NETWORK MANAGEMENT		

Service data backup components

Component	Procedure (s)	Page
CS 2000 Management Tools	Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater Performing a full backup of file systems - (I)SN06.2 or greater	63 70
MG 9000 Manager	Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater Performing a full backup of file systems - (I)SN06.2 or greater	63 70
Integrated Element Management System	Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater Performing a full backup of file systems - (I)SN06.2 or greater	63 70
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 should be performed after hardware changes, software updates or patches, or major reconfigurations. Fileset backup should also 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	85
USP	Administration: Backup	87
GATEWAYS		
Passport devices	Basic service data backup	75
NETWORK MANAGEMENT		
CS 2000 Core Manager	Creating system image backup tapes (S-tapes) manually Configuring SBA backup volumes on the core	89 102
USP Manager	Administration: Creating Disaster Recovery Floppy Disks	84

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

Component backup frequency

Component	Backup Frequency
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
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.

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:

>ITOCCI

and press the Enter key.

Example of a MAP response

```
ITOC User Interface is now active.

ITOCCI:
```

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	Do
ALR	step 6
not ALR	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

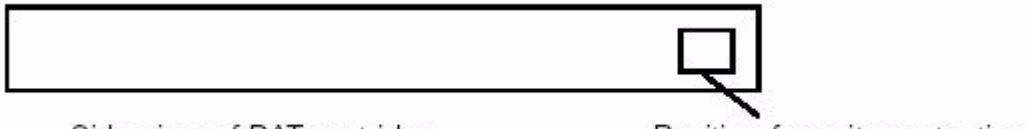
WARNING
Static electricity damage
Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP) when you handle the tape and packlet. The use of the wrist strap protects the packlets against damage caused by electrostatic discharge (ESD).

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 Networks. 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 17
not successful	step 24

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 18
not successful	step 24

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:
```

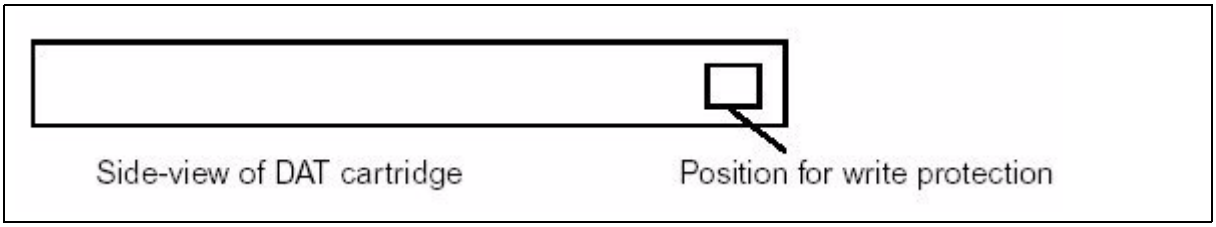
At the shelf

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.

Saving the Passport 8600 boot configuration file

The Passport 8600 boot configuration can be saved to a file via 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 Passport 8000 Series Switch Using the Command Line Interface Release 3.2,” 313194-A.

Note: You must be directly connected to the switch to initiate a Boot Monitor session. You can only connect via a Telnet connection 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.

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 IMGSCHED.

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:
>ITOCCI
ITOC User Interface is now active.
ITOCCI:
>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 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 the CS 2000 Management Tools document NN10106-511, entitled “CS 2000 Management Tools Configuration Management.”

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: OAM&P Workstation Backup

You can perform two types of backup on your OAM&P 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 OAM&P 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 OAM&P 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 OAM&P workstation.

Note: Nortel Networks recommends that you perform a full system backup once a week and modified (differential) backups once a day.

Performing a Manual Backup

Nortel Networks recommends that you perform a manual backup of your OAM&P workstation after initial installation.

To perform a manual backup of the system configuration for your OAM&P workstation, perform the following steps:

At the OAM&P workstation

1. Reboot the workstation.
2. Insert a tape to which the workstation will save your data.
3. 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.
4. Select Open an existing backup job.

5 Click OK.

6 Select Automatic Full Backup.

7 Click Open.

8 If you want to schedule a regular backup, click Schedule.

a If you clicked Schedule, a popup window appears. Select the time and frequency of the regular backup.

9 Click Start. The backup procedure begins.

Note:

This procedure takes approximately 10-15 minutes.

This procedure is complete.

Configuring for Automatic Backup

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 OAM&P 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 OAM&P 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 OAM&P workstation must remain on with Windows active, and a tape must be in the tape drive.

Verifying 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 OAM&P workstation.

Viewing 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 OAM&P workstation.

Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater

Application

Use this procedure to perform a data backup on a Succession Server Platform Foundation Software (SSPFS)-based server (t1400 or Netra 240) running the (I)SN06.2 or greater release of the SSPFS.

Note: For systems running the (I)SN05 or (I)SN06 release of the SSPFS, use procedure Performing a full backup of Oracle data on a Sun server - pre-(I)SN06.2 on page 67 in this document.

The server may be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (EMS)

  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 Billing Manager (CBM)

  Note: If the server is hosting the Core Billing Manager (CBM), it is not required to perform a data backup.

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
- you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data (t1400 only)
- you need one or more blank DVD-RW of 4.7 GB to store the data (Netra 240 only) - please note that the backup utility limits the storage to 2 GB per DVD-RW

Note: To re-use a DVD-RW, refer to procedure Erasing the contents of a CD/DVD on a Sun server on page 430 in this document.

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 may cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

Action

Perform the following steps to complete this procedure.

At the server

1 Insert the blank tape or DVD-RW into the drive.

At your workstation

2 Telnet 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 are performing the backup

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 9
a DVD-RW	step 10

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 11
a DVD-RW	step 12

11 Verify the backup on 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- root/other  1291264 2003-10-01
15:58 oracle.dmp
-rw-rw-rw- root/other     8192 2003-10-01
15:58 critdata.cpio
```

b Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

12 Verify the backup on DVD-RW was successful as follows:

a List the content of the DVD-RW by typing

```
# tar tvf /cdrom/*bkdata*/*.tar
```

and pressing the Enter key.

Example response:

```
-rw-rw-rw- root/other  1291264 2003-10-01
15:58 oracle.dmp
-rw-rw-rw- root/other     8192 2003-10-01
15:58 critdata.cpio
```

b Remove the DVD-RW from the drive, label it, and store it in a safe place.

13 You have completed this procedure.

Performing a full backup of Oracle data on a Sun server - pre-(I)SN06.2

Application

Use this procedure to perform a full backup of application data in the Oracle database on a Sun server (t1400) running the (I)SN05 or (I)SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the (I)SN06.2 or greater release of the SSPFS, use procedure Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater on page 63 in this document .

ATTENTION
It is recommended that provisioning activities be put on hold during the time of the Oracle backup.

Prerequisites

This procedure has the following prerequisites:

- the Oracle database must be in-service
- you need a blank 4mm DDS-3 (Digital Data Storage) tape of 125m and 12GB to store the data

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 may cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the blank tape into the tape drive.

At your workstation

2 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Sun server on which you are performing a full backup of Oracle data

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 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

7 Change to the Oracle user by typing

```
# su - oracle
```

and pressing the Enter key.

Note: You may be required to enter a password for the Oracle user.

8 Backup the Oracle data by typing

```
$ /opt/nortel/sspfs/bks/bkfullora
```

and pressing the Enter key.

9 Quit the Oracle user by typing

```
$ exit
```

and pressing the Enter key.

10 List the content of the tape to ensure the backup was successful by typing

```
# tar tvf /dev/rmt/0
```

and pressing the Enter key.

Example response:

```
-rw-r--r-100/100 8296448 Jun 11 18:08 2003
/var/tmp/bkexpora_2003061118_co.dmp
```

11 Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

12 You have completed this procedure.

Performing a full backup of file systems - (I)SN06.2 or greater

Application

Use this procedure to perform a full backup of the file systems on a Sun server (t1400 or Netra 240) running the (I)SN06.2 or greater release of the Succession Server Platform Foundation Software (SSPFS).

Note: For system running the (I)SN05 or (I)SN06 release of the SSPFS, use procedure Performing a full backup of file systems - pre-(I)SN06.2 on page 73 in this document.

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 data backup on an SSPFS-based server: (I)SN06.2 or greater on page 63 in this document, if required)

  Note: The data backup is not required prior to this procedure for the Core Billing Manager (CBM) product family.

- you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data (T1400 only)
- you need one or more blank DVD-RW of 4.7 GB to store the data (Netra 240 only) - please note that the backup utility limits the storage to 2 GB per DVD-RW

  Note: To re-use a DVD-RW, refer to procedure Erasing the contents of a CD/DVD on a Sun server on page 430 in this document.

Action

At the Sun server

1 Insert a blank tape or DVD-RW into the drive.

At your workstation

2 Telnet to the Sun 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

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 6
a DVD-RW	step 7

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-RW, you may be prompted to insert another blank DVD.

If you are using	Do
a tape	step 8
a DVD-RW	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.

9 Verify the backup to DVD was successful as follows:

a List the content of the DVD by typing

```
# gtar -tvMf /cdrom/*bkfullsys*/*.tar
```

and pressing the Enter key.

b Remove the DVD from the drive, label it, and store it in a safe place.

10 You have completed this procedure.

Performing a full backup of file systems - pre-(I)SN06.2

Application

Use this procedure to perform a full backup of the file systems on a Sun server (t1400) running the (I)SN05 or (I)SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the (I)SN06.2 or greater release of the SSPFS, use procedure Performing a full backup of file systems - (I)SN06.2 or greater on page 70 in this document.

Prerequisites

This procedure has the following prerequisites:

- the Oracle database must be in-service
- you need a blank 4mm DDS-3 (Digital Data Storage) tape of 125m and 12GB to store the data

Action

At the Sun server

1 Insert a blank tape into the tape drive.

At your workstation

2 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 on which you are performing the backup

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 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.

8 List the content of the tape to ensure the backup was successful by typing

```
# ufsrestore tfs /dev/rmt/0 1 (for /)
# ufsrestore tfs /dev/rmt/0 2 (for /var)
# ufsrestore tfs /dev/rmt/0 3 (for /data)
# ufsrestore tfs /dev/rmt/0 4 (for /opt)
# ufsrestore tfs /dev/rmt/0 5 (for /opt/nortel)
```

and pressing the Enter key.

9 Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

10 You have completed this procedure.

Basic service data backup

This section describes using Passport Service Data Backup and Restore to perform a basic back up of service data.

Passport 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. Passport Backup also copies the special files that are found under the directory /provisioning/netsentry.

Passport 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 Passport 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, Passport/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 Passport/SNMP Devices Backup and Restore root directory.

where:

devtype

is the device type (PASSPORT, PP4400, or PP4460).

devname

is the device name.

timestamp

has the format yyyymmddhhmmss

datatset

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 Passport Backup and Restore window. From the Preside 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 Passport Backup and Restore window. From the Preside 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 Passport Backup and Restore window. From the Preside 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 Passport Backup and Restore window. From the Preside 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 Passport Backup and Restore window. From the Preside 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 Passport Backup and Restore window. From the Preside 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 Passport Backup and Restore window. From the Preside 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.

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.

Create a backup of the GWC load file

Purpose of this procedure

This procedure is used to log onto the CS 2000 Core Manager (SDM) 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 will overwrite 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 will likely 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" found in the Gateway

Controller Configuration Management NTP, 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 The procedure is complete.

Note: To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure.

Administration: Backup

If you change the external IP address of an RTC system node in 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 OAM&P 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

To do a backup operation, perform the following steps:

At the OAM&P workstation

1 Open the Backup Active RTC window by clicking Administration in the main menu and clicking Backup in the Administration window.

2 Enter a description of the data snapshot in the Description box. You can enter up to 32 characters.

3 Click Backup to create the data snapshot. An hourglass appears while the current system configuration is saved. This can take several minutes, depending on system activity.

The Backup Status box indicates when the data snapshot has been successfully saved on the active RTC system node. The data snapshot is named for the date and time of its creation.

4 Click Close to close the Backup Active RTC window and return to the Administration window.

5 At the Administration window, click File Manager. The File Manager window appears.

6 Select the disk drive in your alternate boot server to which you want to copy the data snapshot from the Source list.

7 Select the active RTC system node from the Destination list.

8 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.

9 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 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.

10 When the files transferred, click Close to return to the Administration window.

11 Open the Alternate Boot Server (ABS) Configuration Manager window by clicking ABS Config on the Administration window.

12 From the menu bar, select File --> Login.

13 Enter your password in the Password window and click OK.

14 From the menu bar, select File --> ABS Configuration.

15 Select the system name from the Site Name list.

16 Select the data snapshot from the Alternate Boot Data Snapshot list.

17 Click OK.

18 From the menu bar, select File --> Logout.

Creating system image backup tapes (S-tapes) manually

Purpose

Use this procedure to create a system backup image manually.

Application

Use this procedure to 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
- CS 2000 Core Manager software

ATTENTION
This procedure must be performed ONLY from a local console by a trained AIX system administrator with root user privileges.

ATTENTION
All volume groups on the CS 2000 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 CS 2000 Core Manager
- changes to the configuration of disks or logical volumes
- installation of a new version of CS 2000 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 Networks.

The brands approved by Nortel Networks are: Hewlett Packard (HP), Maxell, Verbatim, Imation.

The tape lengths approved by Nortel Networks are:

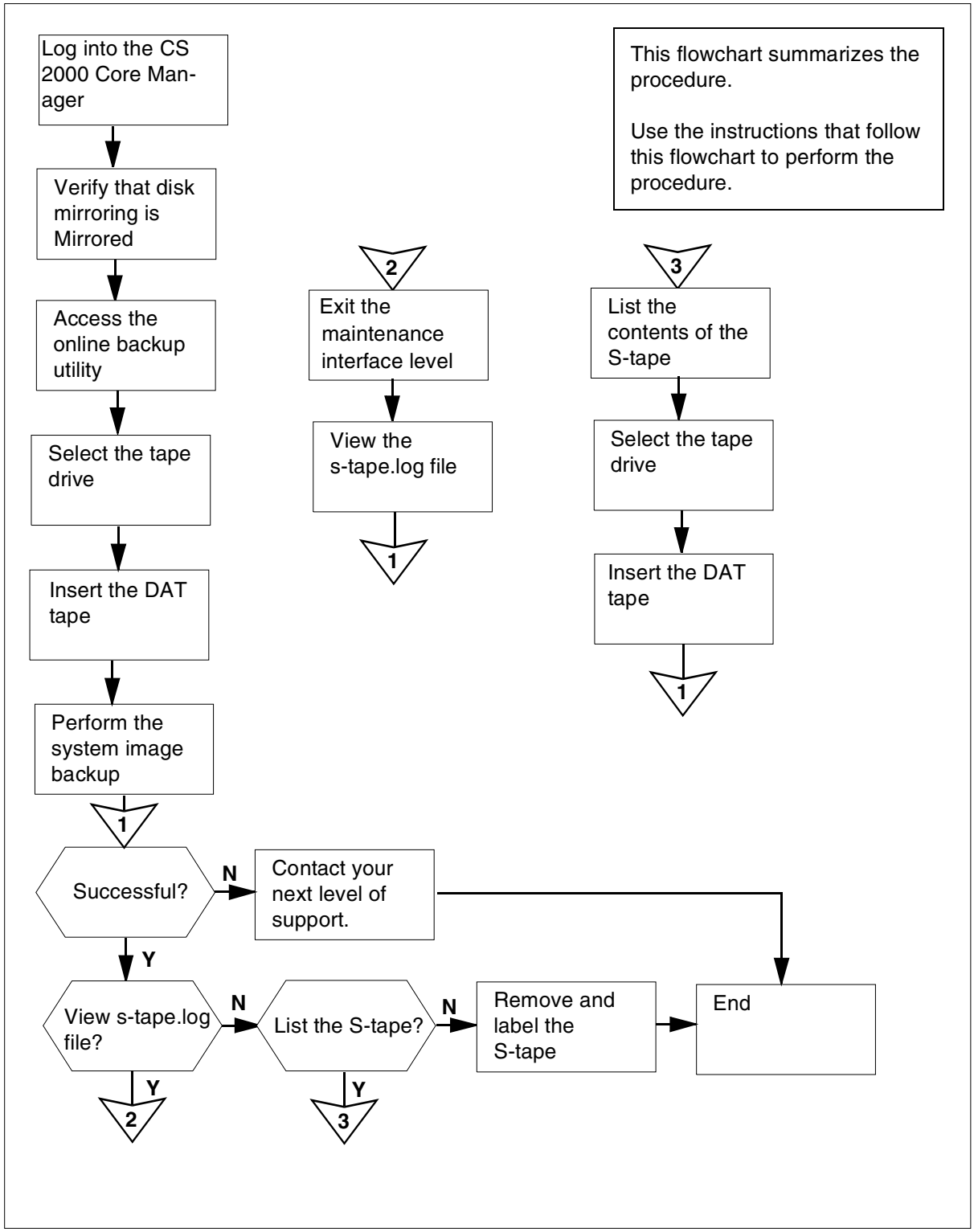
- 90-meter (90M)
- 125-meter (125M)
- 120-meter (120M)

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.

Action

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)



Creating system image backup tapes (S-tapes)

At the local VT100 console

1 Log into the CS 2000 Core Manager as the root user.

2 Access the maintenance interface:

 # sdmmtc

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 3
are not “Mirrored”	contact next level of support

3 Access the administration (Admin) menu level of the RMI:

> admin

4 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.

5 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.

6 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:

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 CS 2000 Core Manager

7

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 CS 2000 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 90 section.

At the local console

8 When you are certain you are using the correct tape, enter:

> y

9 Read the system message to determine if there is enough room on the temporary directory for the system image backup to proceed.

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 13
not enough disk space	step 10

Note: If there is not enough room on the temporary directory, an error message appears.

10 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.

11 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.

12 Read the system message.

If the backup	Do
is successfully completed	step 13
fails	contact your next level of support

13 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.
A log file /tmp/s-tape.log has been created.

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 )
==>
```

14 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 27
protect and label the tape	step 15

If you eject the tape, the screen displays “Tape ejected.” below the information displayed in step 13. 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)
```

15 Place the write-protected tab of the S-tape in the open position, to prevent accidental erasure.

16 When you are ready for the system to return to the System Image Backup and Restore Main Menu, enter

> y

17 Determine if the backup is successful.

The system informs you if the system image backup is successful, as shown in the response in step 13. You may also wish to view the s-tape.log file or list the files on the S-tape.

If	Do
you wish to view the s-tape.log file	step 18
you wish to list the S-tape	step 27
the backup is successful	step 35
the backup fails	contact your next level of support

18 Exit the System Image Backup and Restore Main Menu:

> 0

19 Exit the RMI:

> quit all

20 Access the s-tape.log file:

 # cd /tmp

21 Scroll through the file:

 # more s-tape.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
```

22 Determine if you wish to list the S-tape.

If you	Do
wish to list the S-tape	step 23
do not wish to list the S-tape	step 39

23 Return to the login directory:

 # cd

24 Access the RMI:

 # sdmmtc

25 Access the administration (Admin) menu level of the RMI:

> admin

26 Access the System Image Backup and Restore Menu:

> backup

27 From the System Image Backup and Restore Menu, select List Contents of the System Image Tape (S-tape):

> 3

28 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.

29 Select the tape drive:

> n

where

<n>
is the l (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:

30 After you select the tape drive, you are prompted to insert the S-tape into the tape drive that you selected in step 29.

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 CS 2000 Core Manager

31 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

32 When you are ready to continue this procedure, enter:

> y

33 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 )
```

34 Return to the System Image Backup and Restore Menu:

> y

At the CS 2000 Core Manager

35 If you have not already done so, remove the S-tape from the tape drive by pressing the eject button on the tape drive.

36 Label the tape according to your office procedures, and store it in a safe location.

37 If you ejected an SBA tape, reinsert the tape.

At the local VT100 terminal

38 Exit the System Image Backup and Restore Menu,:

> 0

Note: If you wish to exit the RMI, enter QUIT ALL.

39 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 and 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.

Calculate disk space to contain backup volumes

At your system

1 Write down the dms_disk_space value from the procedure SBA installation and configuration (answer 28) in North American ATM/IP Solution-level Accounting, NN10412-800 and International ATM/IP Solution-leve Accounting NN10400-800, 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 105
IOP	Configuring IOP disk drive backup volumes on page 109
SLM	Configuring SLM disk drive backup volumes on page 112
3PC	Configuring 3PC disk drive backup volumes on page 115

Configuring DDU disk drive backup volumes

At the MAP

1 Post the billing stream:

```
> mapci;mtc;appl;sdmbil;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 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 103 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
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 steps 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 103, 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 steps 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 steps 19 through 23 once you receive confirmation that the files are successfully created. Performing the procedure, Configuring SBA backup volumes on a billing stream in North American ATM/IP Solution-level Accounting, NN10412-800 and International ATM/IP Solution-leve 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;sdmbil;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 103. 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 103, 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 ftfs

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 steps 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 steps 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 and International ATM/IP Solution-leve 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;sdmbil;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 103. 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 103 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 steps 7 to 14 until all volumes have been created.

16 Configure the billing stream of the logical volumes you created in steps 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 and International ATM/IP Solution-leve 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;sdmbil;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 103. 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 103 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 ftfs

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 steps 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 steps 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 and 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.

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	Booting the XA-Core from a Reset Terminal	120
SAM21	SAM21 Shelf Controller reload or restart	143
GWC	Restart or reboot a GWC card	144
Session Server	Perform a database restore to a Session Server unit	148
CS 2000 CS LAN	Resetting the Passport 8600 using a saved configuration file	150
UAS	Restoring UAS configuration files Restoring audio files to a UAS node	151 155
MS 2000 Series	Restoring audio files to a Media Server 2000 Series node	156
APS	Restoring the APS-specific Oracle database and application files	157
USP	Administration: Restore Operations	160
Real-time Transport Protocol (RTP) Media Portal	RTP Media Portal Basics, NN10367-111	
CICM	CICM Security and Administration, NN10252-611	
CORE NETWORK		
Passport 15000	Basic service data restore	172
GATEWAYS		
MG 9000	none (See Note 1)	

Component restoration procedures

Component	Procedure (s)	Page
MG 4000	none (See Note 1)	
IW SPM	none (See Note 1)	
NETWORK MANAGEMENT		
CS 2000 Core Manager	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	177 187 196
CS 2000 Management Tools	Performing a data restore on a Sun server - (I)SN06.2 or greater Performing a full system restore on a Sun server - SN06.2 or greater	199 205
MG 9000 Manager	Performing a data restore on a Sun server - (I)SN06.2 or greater Performing a full system restore on a Sun server - SN06.2 or greater	199 205
Preside MDM	none (See Note 2)	
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" 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.

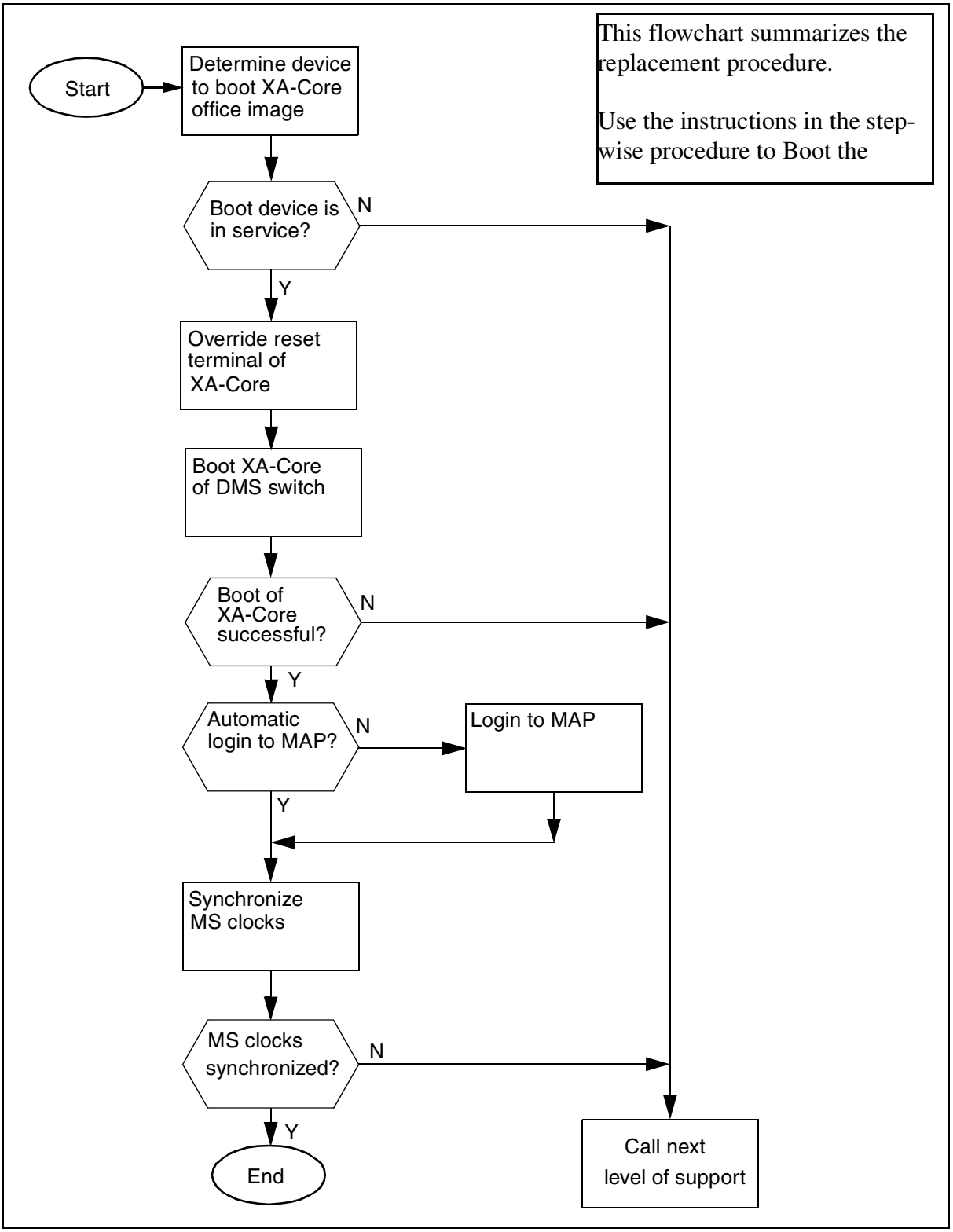
CAUTION
Extended service interruption
Log-in procedures can vary depending on your office configuration.

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.

Call Agent restore

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 Networks 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:
>ITOCCI
ITOC User Interface is now active.
ITOCCI:
>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.

Backup 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

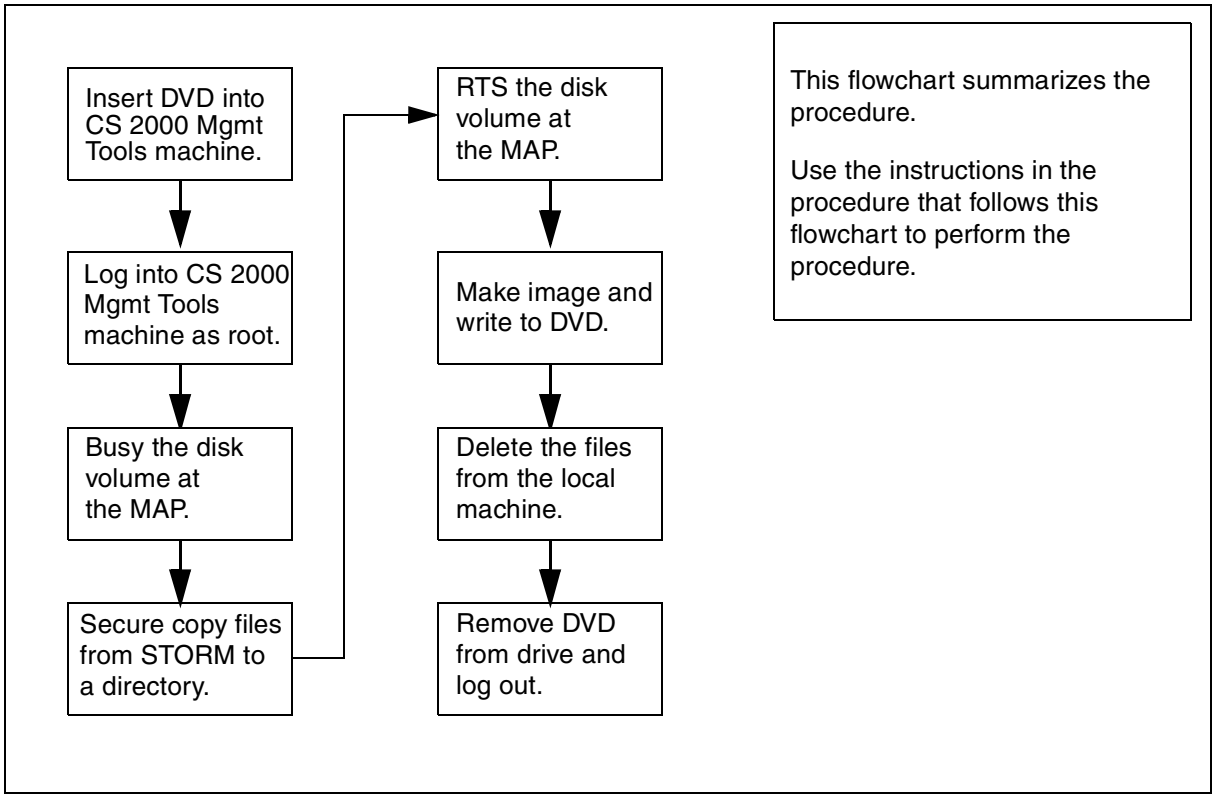
The UNIX commands mkisofs and cdrw are used. For information about these commands, type **man mkisofs** or **man cdrw** at a terminal prompt.

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 how to backup 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,rsize=4096...
10.40.44.239:/nfsserv/3pc/mtc/tape1 on /TAPE1 type nfs (rw,rsize=409...
10.40.44.238:/nfsserv/3pc/cs/sd00 on /3PC/sd00 type nfs (rw,rsize=409...
10.40.44.239:/nfsserv/3pc/cs/sd01 on /3PC/sd01 type nfs (rw,rsize=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,rsize=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 Networks.

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	Listfile the volume that the image is in: **> DISKUT; LF <vol_name>**
volume	Listvols the volume with the megabyte option: **> DISKUT; LV SD00TEMP MB** Subtract FREE MBYTES from TOTAL MBYTES to determine the approximate size of the volume: **400 - 340 = 60 MB**

```
  > LF SD00ADUMP0
 File information for volume SD00ADUMP0:
 {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
--------------------------------------------------------------------------

   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
```

The approximate size of the image in megabytes is NUM OF RECORDS IN FILE / 1000:

220288 / 1000 = 220 MB

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 ADUMP0

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  144121 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 -asl /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.*

List contents of the ISO 9660 image

```
# lofiadm -a /data/dvdimage.iso /dev/lofi/1
# mount -F hsfs /dev/lofi/1 /mnt
# ls -asl /mnt
total 431996
   4 dr-xr-xr-x   2 root   sys        2048 Apr 20 09:48 .
   2 drwxr-xr-x  33 root   root       1024 Apr 20 11:16 ..
431990 -rw-r--r-- 1 maint  maint  221178840 Apr 20 09:47 IMG_TO_BACKUP.img1
```

18 Determine the name of the DVD-RW device:

 # cdrw -l

All optical disk devices are printed.

Determine the DVD-RW device name

```
# cdrw -l
Looking for CD devices...
    Node             Connected Device             Device type
----------------------+--------------------------------+-----------------
 cdrom0                | TOSHIBA  DVD-ROM SD-R6012 1033 | CD Reader/Writer
```

Note: *If the command responds with "`No CD writers found or no media in the drive`," and the CS 2000 Management Tools server is a cluster then verify that the DVD-RW is placed in the active unit. The active unit is identified by a lit USER LED on the face of the unit.*

19 Optionally simulate (-S flag) recording the image to verify that the ISO 9660 image can be recorded on the DVD-RW. This step requires approximately 10 minutes:

 # cdrw -d <dvd_dev> -S -i /data/dvdimage.iso

Example
 # cdrw -d cdrom0 -S -i /data/dvdimage.iso

The CDROM tray ejects after this simulation. ***Close the CDROM tray and continue this procedure to write the DVD-RW****.*

20 Record the image. This step requires approximately 10 minutes:

 # cdrw -d <dvd_dev> -i /data/dvdimage.iso

Example
 # cdrw -d cdrom0 -i /data/dvdimage.iso

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.

Restore from 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 Networks support personnel.

Interval

Perform this procedure when required by your office.

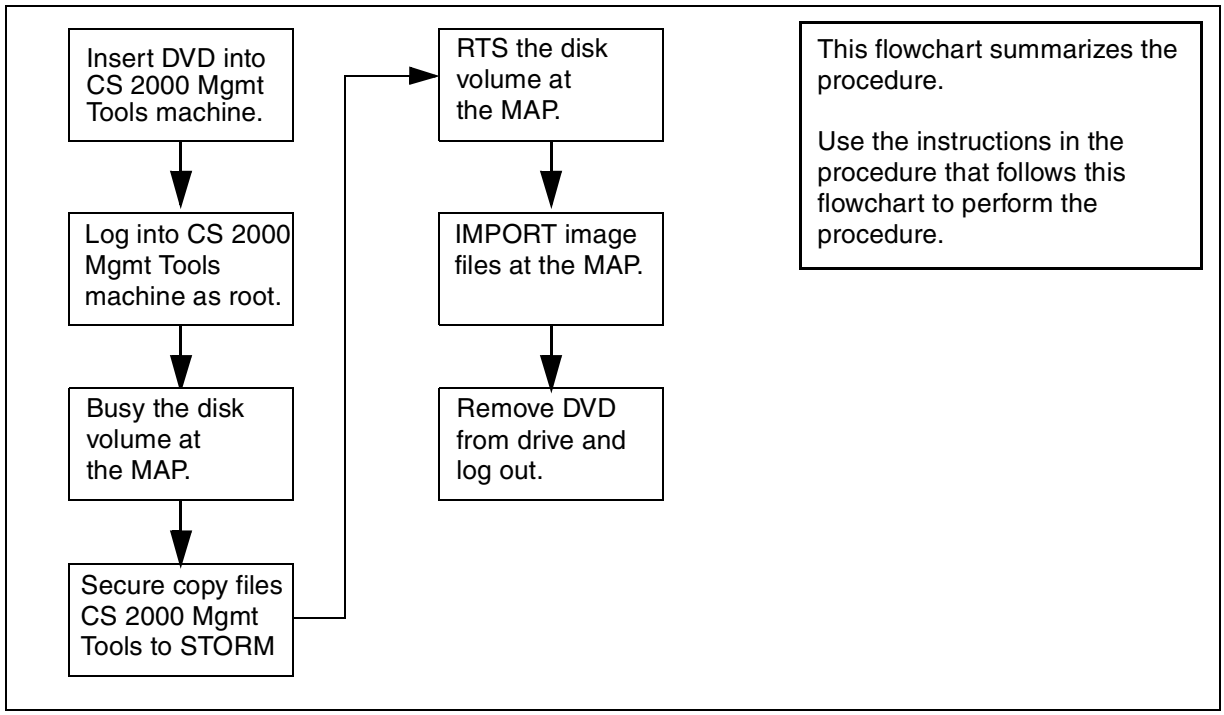
Common procedures

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 how to restore 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.

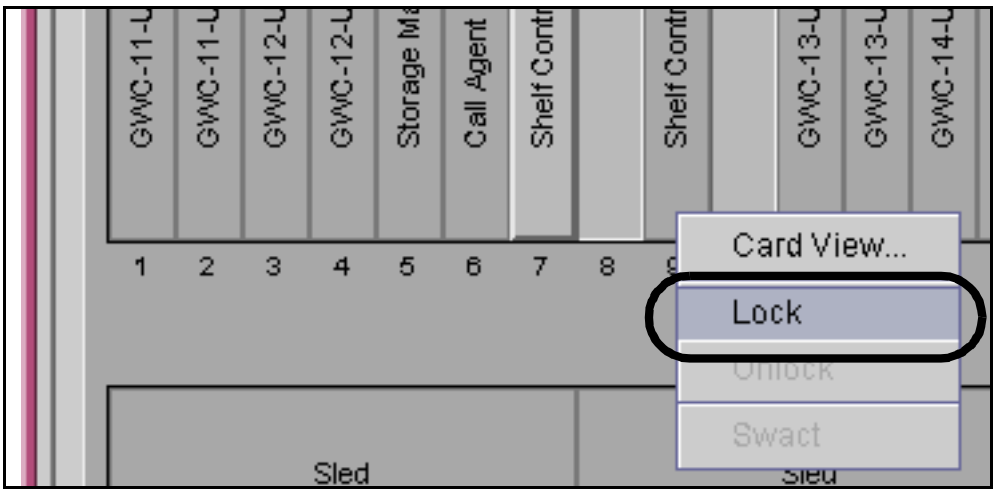
12 Store the DVD-RW per office procedure.

13 This procedure is complete.

SAM21 Shelf Controller reload or restart

At the CS 2000 SAM21 Manager client

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 SAM21 Shelf Controller to indicate that it is in simplex (alarm 2C on the other SAM21 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 (SDM) or Core and Billing Manager (CBM).

To restart software applications only, refer to procedure Restart GWC card services .

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 (SDM) or CBM.

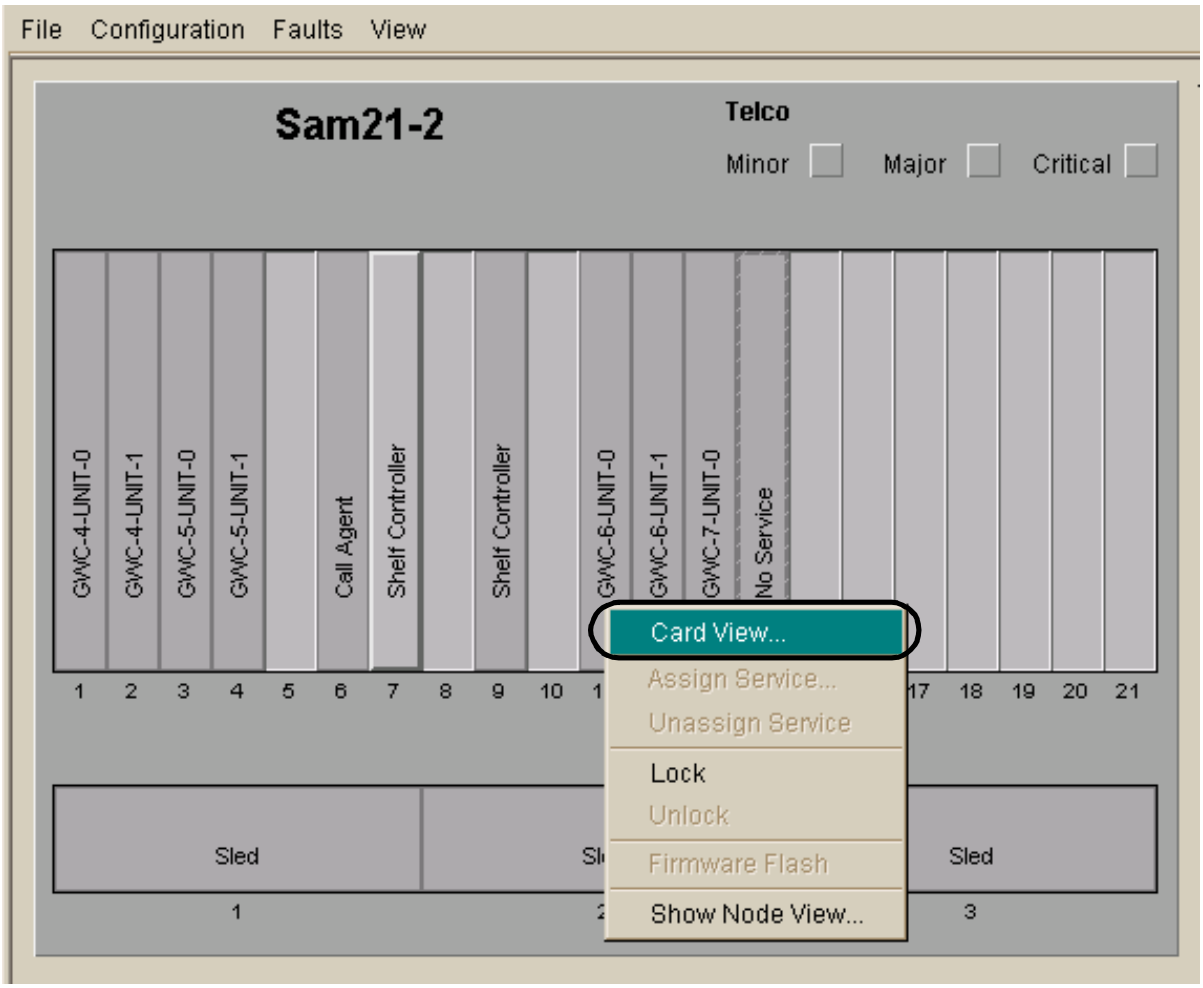
Prerequisites

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.

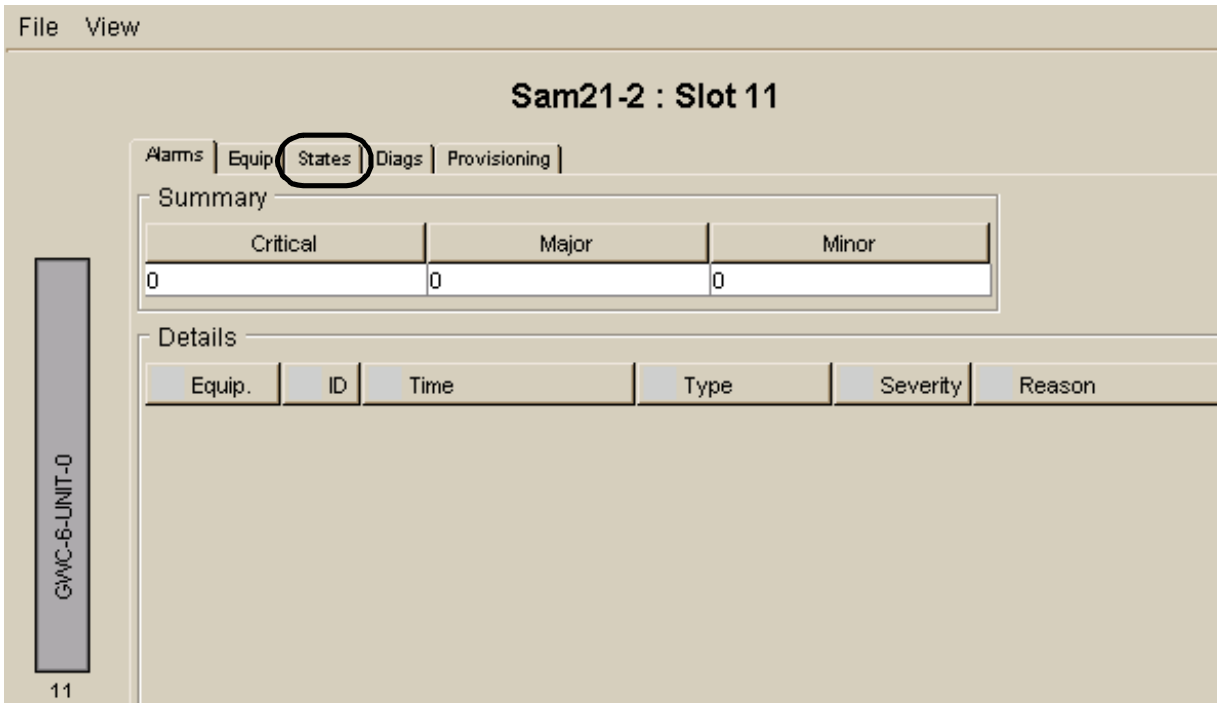
Action

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.

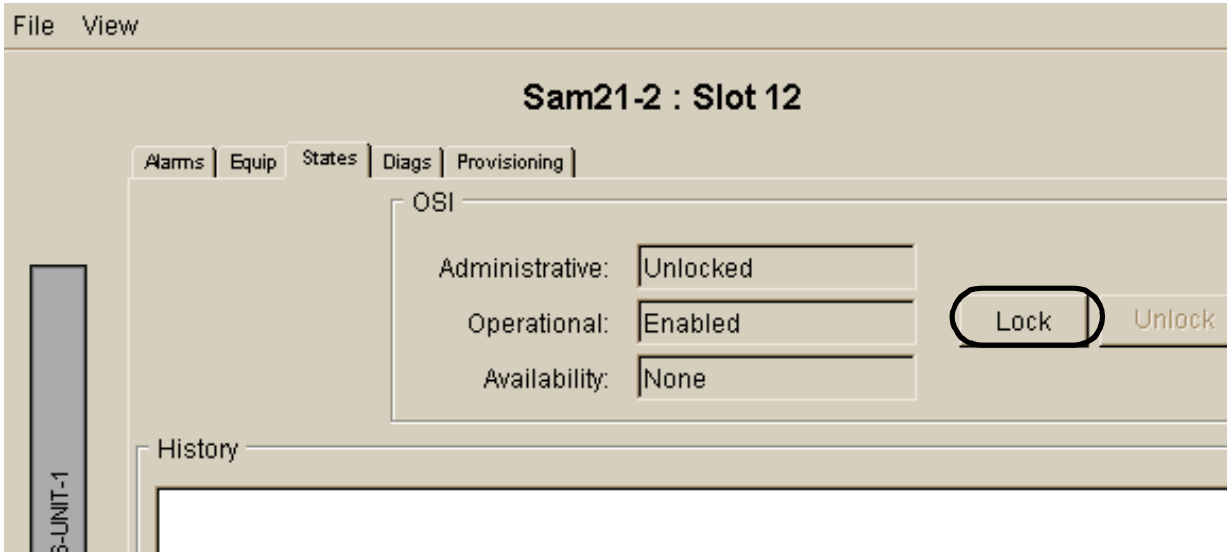


2 At the Card View, select the **States** tab.

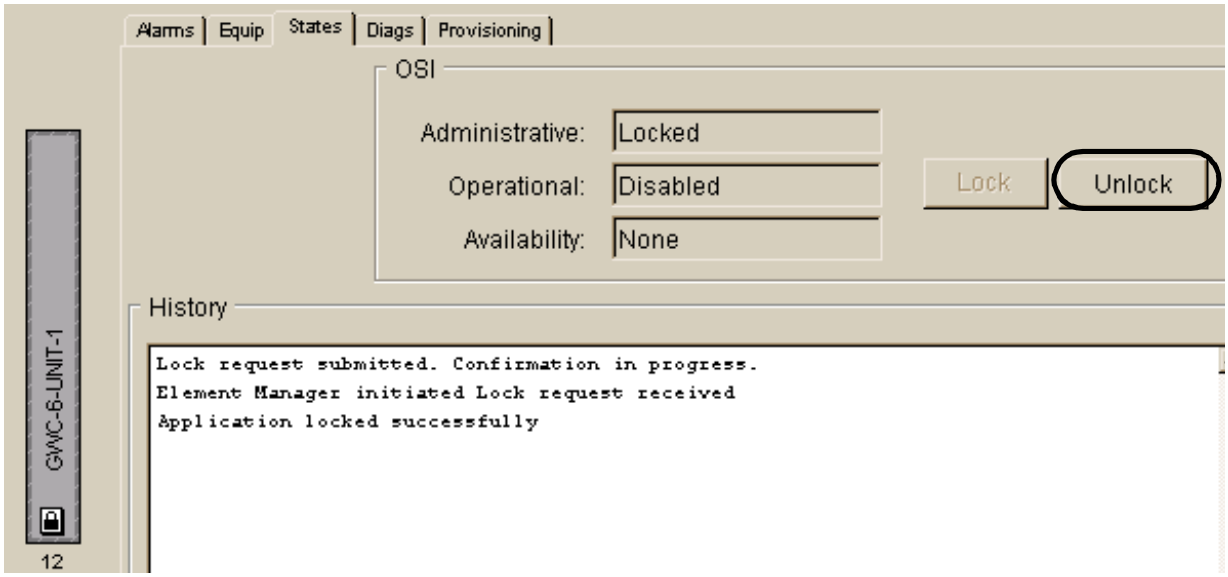


3 Click the **Lock** button to lock the card.

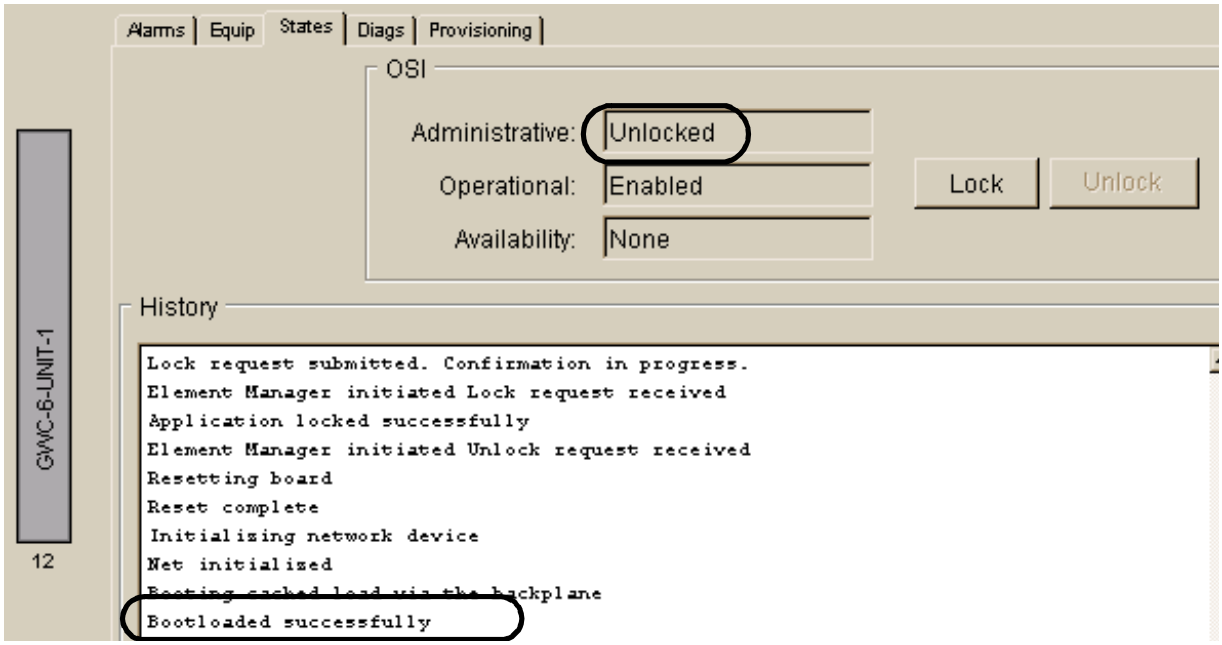
Note: The card must be busy (disabled) before you can lock it. Refer to the procedure “Disable (Busy) GWC card services” in the Gateway Controller Security and Administration NTP, NN10213-611.



4 Wait until the Administrative state of the card is Locked and the History window indicates “Application locked successfully”. Then, click the **Unlock** button.



5 Monitor the reboot process. Wait until the Administrative state of the card is “Unlocked” and the History window indicates “Bootloaded successfully”.



6 This procedure is complete.

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 either the active or inactive 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 the high level upgrade activity Perform an emergency maintenance release rollback activity found in the Session Server Upgrades NTP, NN10349-461.

Limitations and Restrictions

CAUTION

Performing a restore of the SIP Gateway 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 Session Server unit.

Action

At a Session Server command line interface

1 Open a secure shell to the Session Server unit you are restoring a backup copy of the database to by typing

```
> ssh -l <userid> <SS_IP_address>
```

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Session Server

SS_IP_address
is the IP address of either Session Server 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 Passport 8600 using a saved configuration file

The Passport 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 Passport 8000 Series Switch Using the Command Line Interface Release 3.2,” 313194-A.

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

Resetting the Passport 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.

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\mainsa.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.con (for ATM only)
- mainsa.conf (for all configurations)
- atmhard.con (for ATM only)
- snmpd.cnf (for all configurations)
- hosts (for all configurations)
- atmSvcProfile.con (for ATM only)
- atmhardloop.con (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 ATM/IP Configuration document, 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	Do
you are restoring from tape	step 4
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, reseat the RTC system nodes, and then restore power. Your stored data snapshot is now the running data snapshot.

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.

The following sections contain procedures to restore data snapshots stored on your alternate boot server or on the RTC system nodes.

Restoring a Data Snapshot from your Alternate Boot Server

WARNING

Wear wrist straps, and use standard anti-static precautions.

To restore a system configuration from a data snapshot stored on your alternate boot server, perform the following steps:

At the OAM&P workstation

1 To open the File Manager window, click Administration on the main menu and click File Manager.

Note: To have access to the file manager function, you must be working from the OAM&P workstation that is configured as an alternate boot server.

2 Select the disk drive in your alternate boot server where the data snapshot is stored from the Source field.

3 Select the RTC system node in slot 12 from the Destination list.

4 View the contents of the Snapshot field in the Destination portion of the window. If the data snapshot to be restored is not listed in the field, proceed to step 5. If the data snapshot to be restored is listed in the field, proceed to step 7.

5 In the Snapshot field in the Source portion of the window, 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 provisioning and maintenance window for the RTC system node in slot 12. To do this, return to the main menu, click the System Mgmt button to open the System Configuration window, click the icon for the control CAM shelf in the system to open the shelf_name window, and click the icon for the RTC system node in slot 12.

8 Click Edit. The Edit button changes to Unedit button and the fields in the Provisioning portion of the window become editable.

9 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.

10 Click Apply 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.

11 If this RTC system node is the inactive RTC system node, perform the following steps. Otherwise, proceed to step 12.

a If the RTC system node is locked, proceed to step 11b. Otherwise, click Lock and proceed to step 11b.

b If the RTC system node is off-line, proceed to step 12. Otherwise, click Offline and proceed to step 12.

12 Repeat steps 3–11 for the RTC system node in slot 15.

13 Make note of which RTC system node is the active RTC system node. This information will be required later in the procedure.

14 Deactivate the linksets for your system, as appropriate. To do this, perform the following steps:

a To open the SS7 MTP Linkset Administration window, click Network Mgmt on the main menu, click MTP on the Network Management window, and click Linksets on the SS7 MTP window.

b Locate the linkset you want to deactivate.

All provisioned linksets are listed in the Linkset Records field. Click a linkset from the list. All data relating to this linkset automatically appears.

If you are unsure of the linkset name or far end point code, you must scroll through the entire list.

If you know the linkset name, you can easily find the linkset by clicking on the Find by Name radio button, entering the linkset name in the Linkset field, and clicking on the Apply button.

If you know the far end point code, you can easily find the linkset by clicking on the Find by PC radio button, entering the far end point code in the Far End PC field, and clicking on the Apply button.

c Click the Deactivate button to deactivate the displayed linkset. All links in a linkset are deactivated by this command.

d Repeat steps 14b and 14c for each linkset that you want to deactivate prior to performing a COR operation.

15 Change the path state of the ASP paths to Down, as appropriate. To do this, perform the following steps:

a To open the Application Server Process Path Administration window, click Network Mgmt on the main menu, click IPS7 on the Network Management window, and click ASP Paths on the IPS7 window.

b Locate the path whose state you wish to change. All provisioned paths are displayed in the Application Server Process Path Records list, near the bottom of the window. Click a path from the list. All data relating to this path automatically appears.

If you are unsure of the PID or ASP Name information, scroll through the list until you find the PID or ASP Name you want.

c Click Down to change the state of the path to Down.

d Repeat steps 15b and 15c for each ASP path that you want to bring down prior to performing a COR operation.

16 Click Exit on the main menu to close the GUI.

17 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 18. If you do want to update the alternate boot data snapshot, perform the following steps:

a Double-click the Universal Signaling Point icon on your desktop to display the Login window.

b To open the Modify Site window, click Configure to open the Site Configuration window and click Modify Site.

c Select your system from the Site Name list.

d Select the boot data snapshot that you want to use as an alternate boot data snapshot from the Alt. Boot Data Snapshot list.

e Click OK to save the change. The system displays a pop-up confirmation window.

f Click OK to close the popup confirmation window. The system displays a message in a popup window to ask you if you want to modify the BOOTP tab window.

g Click No to close the popup window.

h Click Close to close the Site Configuration window.

18 To perform a COR on your system, use the following steps:

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 18a 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.

Note: 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.

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 18d 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.

19 Double-click Universal Signaling Point on your desktop to restart the GUI as soon as one of the RTC system nodes is enabled. This is indicated when an LED turns green on the front panel of the shelf below either slot 12 or 15.

Note: Nortel Networks recommends that you do not make any provisioning changes until the data in the shelf_name window indicates that both RTC system nodes are enabled or that one RTC system node is enabled and the other is off-line.

20 Log into your system. To do this, select your system from the Site list, enter your user name in the User ID field, enter your password in the Password field, and click Connect. The system displays the main menu.

21 To open the RTC system node provisioning and maintenance window for the RTC system node in slot 12, click the System Mgmt button to open the System Configuration window, click the

control CAM shelf to open the shelf_name window, and click the RTC system node in slot 12.

22 Verify that the description of the data snapshot listed in the Running Data Snapshot field is the same as the description of the data snapshot you just attempted to restore.

23 If the data snapshot descriptions match, proceed to step 24. 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.

24 To update the system time settings in the Set Date/Time window, click Administration on the main menu to open the Administration window, and click Set Date/Time.

25 The system time settings will be incorrect by as many minutes as the system took to perform the COR. Adjust the settings in the Time portion of the window appropriately.

26 Click OK to save the new system time settings.

Restoring a Data Snapshot from an RTC System Node

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.

Typically, when you are restoring a system configuration, the data snapshot is located on the disk drive for your alternate boot server. However, it might be necessary to restore a system configuration saved in a data snapshot that is not stored on the disk drive in your alternate boot server.

To restore a system configuration using a data snapshot stored on an RTC system node, perform the following steps:

At the OAM&P workstation

1 To open the File Manager window, click Administration on the main menu and click File Manager.

Note: To have access to the file manager function, you must be working from the OAM&P workstation that is configured as an alternate boot server.

2 Select the RTC system node in which the data snapshot you want to restore is located from the Destination list.

3 Select the disk drive in your alternate boot server where the data snapshot will be stored from the Source list.

4 Initiate a copy operation by clicking the suitcase icon. An hourglass displays while the snapshot is being copied. The fields in the Source portion of the window will be updated with the information for the copied snapshot when the copy operation is complete.

Note: The data snapshots are large and can take several minutes to copy from an RTC system node to your alternate boot server, depending on system activity.

5 Select the other RTC system node from the Destination field.

6 View the contents of the Snapshot field in the Destination portion of the window. If the data snapshot to be restored is not listed in the field, proceed to step 7. If the data snapshot to be restored is listed in the field, proceed to step 9.

7 In the Snapshot field in the Source portion of the window, select the data snapshot to be restored.

8 Initiate a copy operation by clicking the printer 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.

9 To open the RTC system node provisioning and maintenance window for the RTC system node in slot 12, click the System Mgmt button on the main menu, click the control CAM shelf to open the shelf_name window, and click the RTC system node in slot 12.

10 Click Edit. The Edit button changes to Unedit and the fields in the Provisioning portion of the window become editable.

11 Change the boot data snapshot for the RTC system node. To do this, click 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.

12 Click Apply 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 to indicate 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 change the boot data snapshot back to match the running boot data snapshot.

13 If this RTC system node is the inactive RTC system node, perform the following steps. Otherwise, proceed to step 14.

a If the RTC system node is locked, proceed to step 13b. Otherwise, click Lock and proceed to step 13b.

b If the RTC system node is off-line, proceed to step 14. Otherwise, click Offline and proceed to step 14.

14 Repeat steps 9–13 for the RTC system node in slot 15.

15 Make note of which RTC system node is the active RTC system node. This information will be required later in the procedure.

16 Deactivate the linksets for your system, as appropriate. To do this, perform the following steps:

a To open the SS7 MTP Linkset Administration window, click Network Mgmt on the main menu, click MTP on the Network Management window, and click Linksets on the SS7 MTP window.

b Locate the linkset you want to deactivate.

All provisioned linksets are listed in the Linkset Records field. Click a linkset from the list. All data relating to this linkset automatically appears.

If you are unsure of the linkset name or far end point code, you must scroll through the entire list.

If you know the linkset name, you can easily find the linkset by clicking Find by Name, entering the linkset name in the Linkset field, and clicking Apply.

If you know the far end point code, you can easily find the linkset by clicking Find by PC, entering the far end point code in the Far End PC field, and clicking Apply.

c Click the Deactivate button to deactivate the displayed linkset. All links in a linkset are deactivated by this command.

d Repeat steps 16b and 16c for each linkset that you want to deactivate prior to performing a COR operation.

17 To change the path state of the ASP paths to Down, as appropriate, perform the following steps:

a To open the Application Server Process Path Administration window, click Network Mgmt on the main menu, click IPS7 on the Network Management window, and click ASP Paths on the IPS7 window.

b Locate the path whose state you wish to change. All provisioned paths are displayed in the Application Server Process Path Records list, near the bottom of the window. Click a path from the list. All data relating to this path automatically appears.

If you are unsure of the PID or ASP Name information, scroll through the list until you find the PID or ASP Name you want.

c Click Down to change the state of the path to Down.

d Repeat steps 17b and 17c for each ASP path that you want to bring down prior to performing a COR operation.

18 Click Exit to exit the GUI.

19 You may want to change the alternate boot data snapshot if the system configuration stored in the data snapshot file is significantly 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 20.

If you do want to update the alternate boot data snapshot, perform the following steps:

a Double-click the Universal Signaling Point icon on your desktop to display the Login window.

b To open the Modify Site window, click Configure to open the Site Configuration window and click Modify Site.

c Select your system from the Site Name list.

d Select the boot data snapshot that you want to use as an alternate boot data snapshot from the Alt. Boot Data Snapshot list.

e Click OK to save the change. A popup confirmation window appears.

f Click OK to close the popup confirmation window. The system displays a popup window with a message that asks you if you want to modify the BOOTP tab window.

g Click No to close the popup window.

h Click Close to close the Site Configuration window.

20 To perform a COR on your system, use the following steps:

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 20a 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 20d 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.

21 Double-click the Universal Signaling Point icon on your desktop to restart the GUI as soon as one of the RTC system nodes is enabled.

This is indicated when an LED turns green on the front panel of the shelf below either slot 12 or 15.

Note: Nortel Networks recommends that you do not make any provisioning changes until the data in the shelf_name window indicates that both RTC system nodes are enabled or that one RTC system node is enabled and the other is off-line.

22 To log in to your system, perform the following steps:

a Select your system from the Site list.

b Enter your user name in the User ID field.

c Enter your password in the Password field.

d Click the Connect button. The main menu appears.

23 To open the RTC system node provisioning and maintenance window for the RTC system node in slot 12, click System Mgmt on the main menu, click the control CAM shelf to open the shelf_name window, and click slot 12.

24 Verify that the description of the data snapshot listed in the Running Data Snapshot field is the same as the description of the data snapshot you just attempted to restore.

25 If the data snapshot descriptions match, proceed to step 26. If the snapshot descriptions do not match, return to step 1 and attempt the procedure again. If the procedure has failed twice in a row, contact your next level of support.

26 To update the system time settings in the Set Date/Time window, click Administration on the main menu to open the Administration window, and click Set Date/Time.

27 The system time settings will be off for as many minutes as the system took to perform the COR. Adjust the settings in the Time portion of the window appropriately.

28 Click OK to save the new system time settings.

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.

To perform a restore operation from a backup tape, perform the following steps:

At the OAM&P 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.

Basic service data restore

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.

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).

Application

ATTENTION
You must be a trained AIX system administrator who has root user privileges to the core manager to perform this procedure.

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.

You must be a root user at a local VT100 console to perform this procedure.

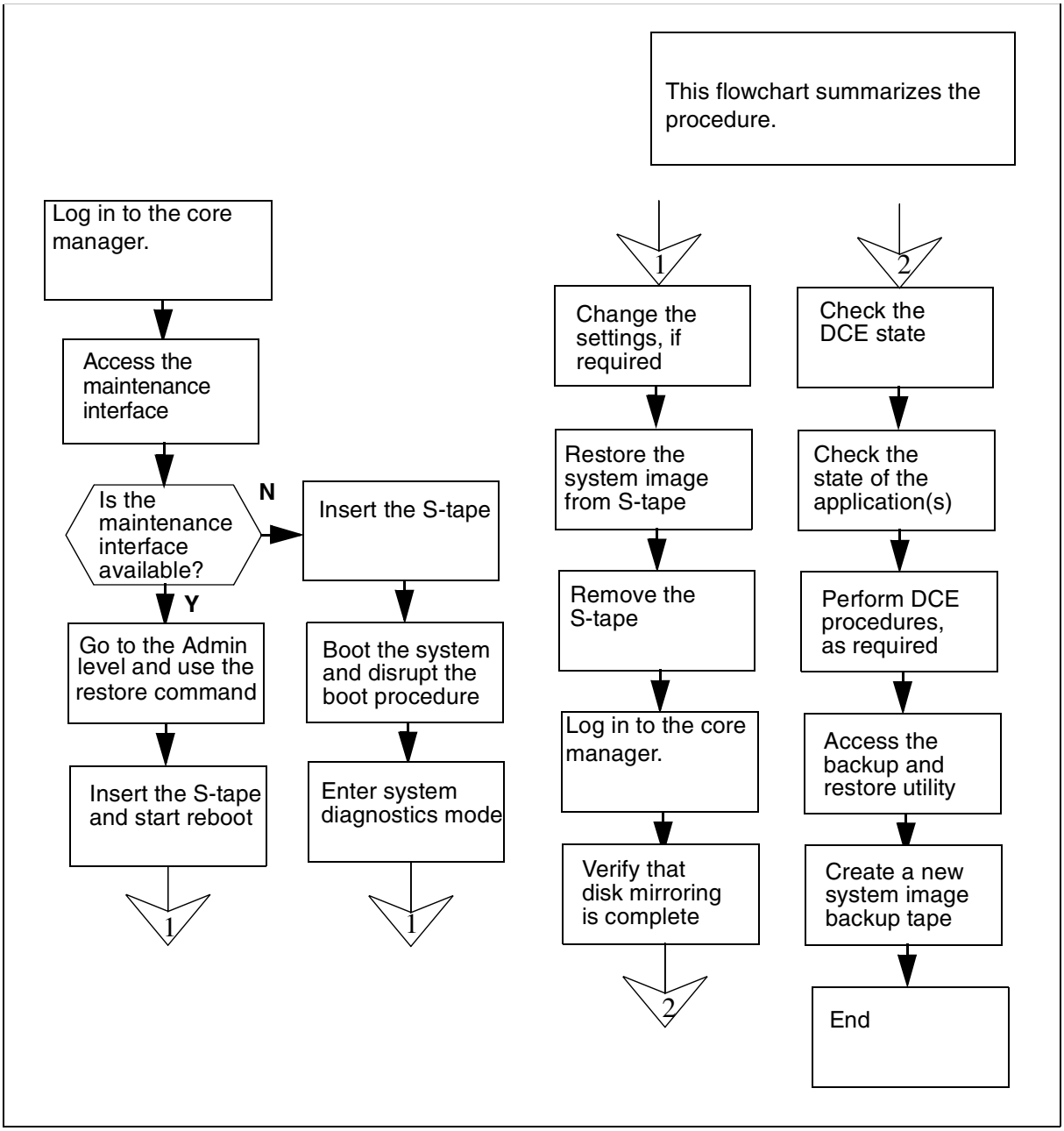
Interval

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



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 root user.

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
                                      31200 0660
   3    0  IO         0     $00   N  SEAGATE
ST12400N
                                      ST32430
0660
   1    50 IO         5     $01   Y  ARCHIVE
Python
                                      28388-XXX
5.45
   6    0  IO         0     $00   N  SEAGATE
ST11200N
                                      ST31230
0660
   8    0  IO         0     $00   N  SEAGATE
ST12400N
                                      ST32430
0660
   6    50 IO         5     $01   Y  ARCHIVE
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
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 root user. 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 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.

42 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).

Application

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 who has root user privileges to access the core manager.

ATTENTION
All volume groups on the CS 2000 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.

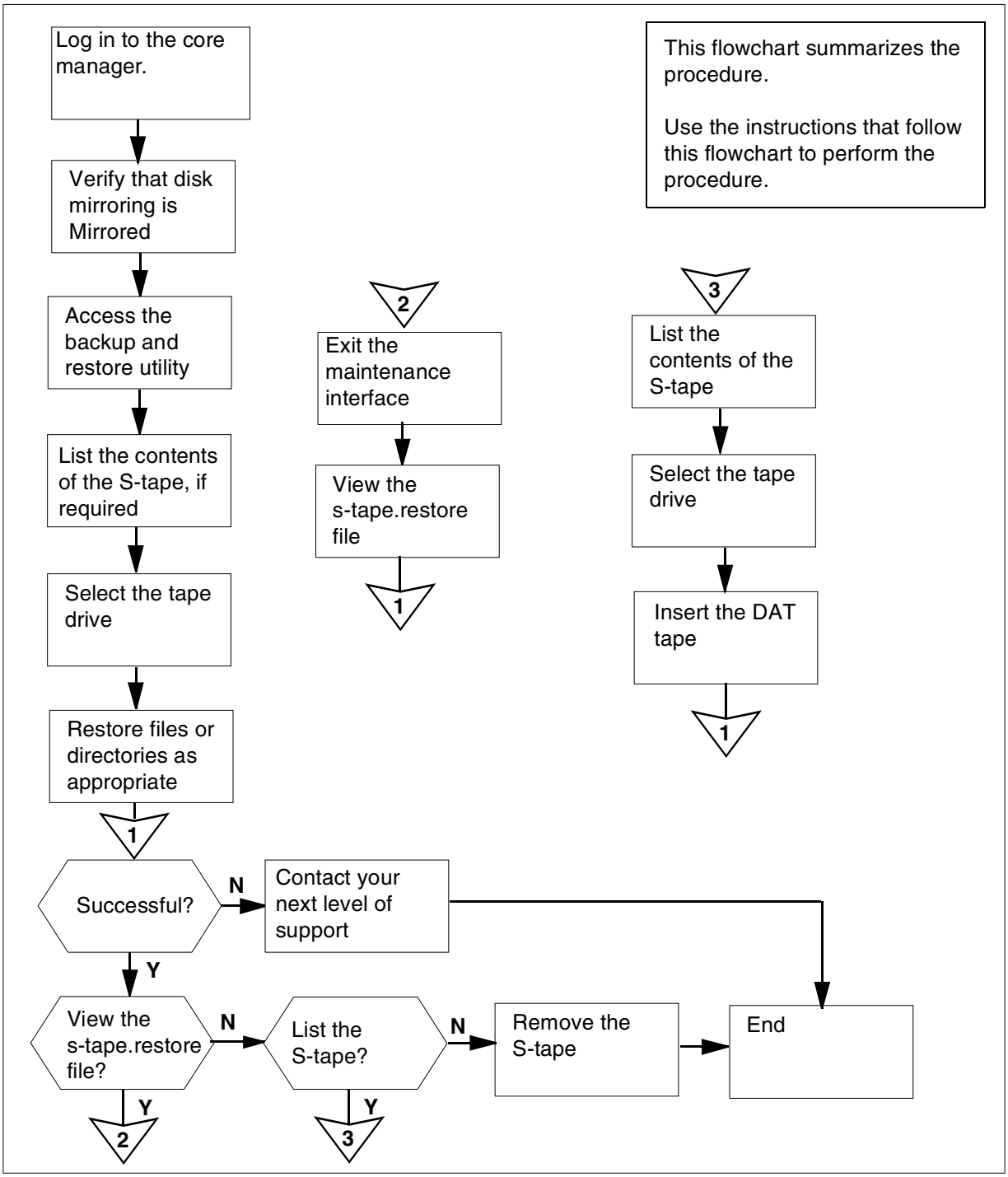
ATTENTION
If your system includes the SuperNode Billing Application (SBA), use tape drive DAT0 to perform this procedure.

This procedure can be performed by the root user from a local or remote terminal.

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)



Partial restore from the system image tape (S-tape)

At the local or remote console

1 Log into the core manager as the root user.

2 Access the maintenance interface:

```
# sdmmtc
```

3 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 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
- I 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

Purpose

Use this procedure to recover backup files from lost backup volumes. The procedure swaps back old volumes as the primary backup volumes.

Application

You need to recover backup files from lost backup volumes if the SBA cannot track backed up files when the SWACT and RESTART processes occur when you perform procedure “Configuring SBA backup volumes” in the CS 2000 Core Manager Accounting document.

Prerequisites

Before starting the procedure, you need

- the names of the swapped out volumes
- to have performed “Configuring SBA backup volumes on the core” in the CS 2000 Core Manager Accounting document, and the SBA has 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:

```
> mapci;mtc;appl;sdmbil;post <stream_name>
```

where

<stream_name> is the name of the billing stream.

2 Quit back to the appl;sdmbil level:

```
> quit
```

3 Confirm that the names of the billing stream's existing backup volumes are the swapped in volumes you created earlier:

```
> 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.

4 Read the notes you made when you performed the procedure, "Configuring SBA backup volumes on the core" in the CS 2000 Core Manager Accounting document, to confirm that the backup volumes that you listed in step 3 are the backup volumes you created with that procedure.

If the backup volume names are	Do
the backup volume names configured when you performed the procedure	continue with step 5
not the backup volume names configured when you performed the procedure	determine if someone else re-configured the backup volumes before you continue with step 5

5 Access the billing level:

```
> mapci;appl;sdmbil
```

6 Configure the billing stream of the logical volumes you created when you performed the procedure, "Configuring SBA backup volumes on the core" in the CS 2000 Core Manager Accounting document:

```
> addvol <stream_name> <volume1> ... <volume5>
```

where:

<stream_name>
is the name of the billing stream

<volume1> ... <volume5>
is the volume name. Up to five volumes (with each entry separated by a space) can be added at one time.

Example
To add five volumes, the command is:

addvol AMA S00DAMA S01DAMA S02DAMA S03DAMA S04DAMA

Repeat this step until all of the volumes have been added to the stream, and then proceed to step 7.

7 Exit back to the command prompt:

```
> quit all
```

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 core manager.

Note 2: You must provide, to all operating company personnel who work on the core, the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware that any restarts or switch of activity (SwAct) that occur before the billing stream returns to normal mode can cause a serious loss of billing records.

The mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

8 You have completed this procedure.

Performing a data restore on a Sun server - (I)SN06.2 or greater

Application

Use this procedure to restore data from a backup tape or DVD-RW on a Sun server (t1400 or Netra 240) running the (I)SN06.2 or greater release of the Succession Server Platform Foundation Software (SSPFS).

Note 1: For systems running the (I)SN05 or (I)SN06 release of the SSPFS, use procedure Restoring application data to the Oracle database (pre-(I)SN06.2) in this document.

Note 2: The data restore is not required for the Core Billing Manager (CBM) product family.

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater
- you need the tape or the DVD-RW on which the data was backed up

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the backup tape or DVD-RW into the drive.

At your workstation

2 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 If required, stop the server applications that run 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
MG 9000 Manager and mid-tier server applications	the MG9000 Security and Administration document, NN10162-611, if required
Integrated EMS server application	the Integrated EMS Security and Administration document, NN10336-611, if required

7 Restore the database by typing

```
$ /opt/nortel/sspfs/bks/rsdata
```

and pressing the Enter key.

8 Remove the backup tape or the DVD-RW from the drive, and store it in a safe place.

9 Verify that the database is restored properly.

10 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
MG 9000 Manager and mid-tier server applications	the MG9000 Security and Administration document, NN10162-611, if required
Integrated EMS server application	the Integrated EMS Security and Administration document, NN10336-611, if required

11 You have completed this procedure.

Restoring application data to the Oracle database (pre-(I)SN06.2)

Application

Use this procedure to restore the application data to the Oracle database from a backup tape on a Sun server (t1400) running the (I)SN05 or (I)SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For system running the (I)SN06.2 or greater release of the SSPFS, use Performing a data restore on a Sun server - (I)SN06.2 or greater on page 199 in this document.

Prerequisites

You need the tape on which the data was backed up.

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the backup tape into the drive.

At your workstation

2 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 Stop the server applications that run on the server.

For	Refer to
SESM, SAM21EM and NPM server applications	Stopping the SESM server application on page 380 Stopping the SAM21 Manager server application on page 382 Stopping the NPM server application on page 384
MG 9000 Manager and mid-tier server applications	the MG9000 Security and Administration document, NN10162-611, if required

7 Change to the Oracle user by typing

```
# su - oracle
```

and pressing the Enter key.

8 Perform the restore command by typing

```
$ /opt/nortel/sspfs/bks/rsimpora
```

and pressing the Enter key.

9 Quit the Oracle user by typing

```
$ exit
```

and pressing the Enter key.

10 Remove the tape from the drive and store it in a safe place.

11 Start the server applications that run on the server.

For	Refer to
SESM, SAM21EM and NPM server applications	Starting the SESM server application on page 353 Starting the SAM21 Manager server application on page 356 Starting the NPM server application on page 358
MG 9000 Manager and mid-tier server applications	the MG9000 Security and Administration document, NN10162-611, if required

12 You have completed this procedure.

Performing a full system restore on a Sun server - SN06.2 or greater

Application

Use this procedure to perform a full system restore from a backup tape or DVD-RW on a Sun server (t1400 or Netra 240) running the SN06.2 or greater release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the SN05 or SN06 release of the SSPFS, use procedures Restoring root file systems - pre-(I)SN06.2 on page 208 and Restoring non-root file systems - pre-(I)SN06.2 on page 211 in this document.

Use one of the methods below according to your office configuration.

- Simplex configuration (one server) on page 205
- High-availability configuration (two servers) on page 206

Note: Only the Simplex configuration (one server) is applicable to perform a full system restore from tape on a t1400 server.

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS SN06.2 or greater
- you need the backup tape or DVD-RW

Action

Perform the following steps to complete this procedure.

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 SSPFS CD disk#1 into the CD/DVD drive.

4 At the OK prompt, restore the system by typing

```
OK boot cdrom - restore
```

and pressing the Enter key.

5 When prompted, accept the software license restrictions by typing

ok

and pressing the Enter key.

The system reboots.

6 When prompted, insert the backup tape or Volume 1 of the backup DVD-RW into the drive.

The restore process can run for several minutes and may prompt you for additional Volumes that were generated during the full system backup to DVD-RW.

7 Restore the data. Refer to procedure Performing a data restore on a Sun server - (I)SN06.2 or greater.

Note: The data restore is not required for the Core Billing Manager (CBM) product family.

8 Once the data restore is complete, reboot the system by typing

init 6

and pressing the Enter key.

9 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 Bring the system to the OK prompt by typing

init 0

and pressing the Enter key.

5 Insert SSPFS CD disk#1 into the CD/DVD 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.

8 When prompted, insert Volume 1 of the backup DVD-RW into the drive.

The restore process can run for several minutes and may prompt you for additional Volumes that were generated during the full system backup to DVD-RW.

9 Restore the data. Refer to procedure Performing a data restore on a Sun server - (I)SN06.2 or greater.

Note: The data restore is not required for the Core Billing Manager (CBM) product family.

10 Once the data restore is complete, reboot the system by typing

init 6

and press the Enter key.

11 Re-image the inactive node using the active node's image. Refer to procedure "Cloning the image of one node in a cluster to the other node" in the ATM/IP Security and Administration document, NN10402-600, if required.

12 You have completed this procedure.

Restoring root file systems - pre-(I)SN06.2

Application

Use this procedure to restore the root file systems from tape on a Sun server (t1400) running the (I)SN05 or (I)SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the (I)SN06.2 or greater release of the SSPFS, use procedure Performing a full system restore on a Sun server - SN06.2 or greater on page 205 in this document

Prerequisites

You need the tape on which the data was backed up.

Action

Perform the following steps to complete this procedure.

At the server console

1. Log in to the server through the console using the root user ID and password.
2. Insert the backup tape into the drive.
3. Insert SSPFS CD disk#1 into the CD-ROM drive.
4. Enter the following commands:

   ```
   # metadetach d2 d1
   # metaroot /dev/dsk/c0t0d0s1
   # init 6
   ```

5. When prompted, log on as root.
6. Enter the following commands:

   ```
   # metaclear -r d2
   # metaclear d1
   # init 0
   ```

7. At the ok prompt, boot the system from the CD-ROM by typing

   ```
   ok boot cdrom -s
   ```

   and pressing the Enter key.

8 Enter the following commands:

```
# mount /dev/dsk/c0t0d0s1 /a
# cp /a/etc/system /a/etc/system.unmirror
# cp /a/etc/vfstab/ /a/etc/vfstab.unmirror
# cd /a
# ufsrestore rfs /dev/rmt/0 1
```

Note: The system can take between 20 and 45 min. to process the above command.

```
# rm restoresymtable
# cd /
# cp /a/etc/system.unmirror /a/etc/system
# cp /a/etc/vfstab.unmirror /a/etc/vfstab
# umount /a
# fsck /dev/rdsk/c0t0d0s1
# installboot /usr/platform/`uname -i` /lib/fs/ufs/bootblk /dev/rdsk/c0t0d0s1
```

Note: The above command is entered on one line. There is no space between "`-i`" and "`/lib/fs/ufs/bootblk`". Use the back quote on the same key as the Tilda (~) for *uname -i.*

```
# init 6
```

9 When prompted, log on as root.

Note: The root password required is the restored root password and not the default root password.

10 Enter the following commands:

```
# metainit -f d0 1 1 c0t0d0s1
# metainit d1 1 1 c0t1d0s1
# metainit d2 -m d0
# metaroot d2
# lockfs -fa
# init 6
```

11 When prompted, log on as root.

12 Enter the following commands:

```
# metattach d2 d1
# init 6
```

13 When prompted, log on as root.

14 Remove the tape from the drive and store it in a safe place.

15 Eject the SSPFS CD disk#1 from the CD-ROM drive by entering the following commands:

```
# cd /
# eject cdrom
```

16 You have completed this procedure.

Restoring non-root file systems - pre-(I)SN06.2

Application

Use this procedure to restore all of the non-root file systems from tape on a Sun server (t1400) running the (I)SN05 or (I)SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the (I)SN06.2 or greater release of the SSPFS, use procedure Performing a full system restore on a Sun server - SN06.2 or greater on page 205 in this document.

Prerequisites

You need the tape on which the data was backed up, and you need root user privileges.

Action

Perform the following steps to complete this procedure.

At the server console

1. Log in to the server through the console (port A) using the root user ID and password.
2. Boot the system to the OK prompt by typing

   ```
   # shutdown -i 0 -y
   ```

   and pressing the Enter key.
3. Insert the backup tape into the drive.
4. At the OK prompt, boot the system in single-user mode by typing

   ```
   OK> boot -s
   ```

   and pressing the Enter key.
5. When the system prompts you to either enter the root password or press Control-D, enter your root password to continue the maintenance process.

6 Enter the following command:

```
# ufsrestore tfs /dev/rmt/0 1 | grep audio_files
```

If	Do
the response to the command is similar to `321287 ./audio_files`	substep a
the command produces no output	substep b

a Enter the following series of commands:

```
# cd /audio_files
# ufsrestore rfs /dev/rmt/0 2
# rm restoresymtable

# cd /data
# ufsrestore rfs /dev/rmt/0 3
# rm restoresymtable

# cd /opt
# ufsrestore rfs /dev/rmt/0 4
# rm restoresymtable

# cd /opt/nortel
# ufsrestore rfs /dev/rmt/0 5
# rm restoresymtable

# cd /PROV_data
# ufsrestore rfs /dev/rmt/0 6
# rm restoresymtable

# cd /user_audio_files
# ufsrestore rfs /dev/rmt/0 7
# rm restoresymtable

# cd /var
# ufsrestore rfs /dev/rmt/0 8
# rm restoresymtable
```

Note: The restore time for each filesystem is dependent on the size of the filesystem. Restore can take 60 minutes or more to complete after which the prompt returns. Do not press Ctrl-C as this will interrupt the restore process.

Proceed to step 7

b Enter the following series of commands:

```
# cd /data
# ufsrestore rfs /dev/rmt/0 2
# rm restoresymtable

# cd /opt
# ufsrestore rfs /dev/rmt/0 3
# rm restoresymtable

# cd /opt/nortel
# ufsrestore rfs /dev/rmt/0 4
# rm restoresymtable

# cd /var
# ufsrestore rfs /dev/rmt/0 5
# rm restoresymtable
```

Note: The restore time for each filesystem is dependent on the size of the filesystem. Restore can take 60 minutes or more to complete after which the prompt returns. Do not press Ctrl-C as this will interrupt the restore process.

7 Enter the following command:

```
# init 6
```

8 Remove the tape from the drive and store it in a safe place.

9 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.
- Group-based authorization controls which operations a user is authorized to perform.

Integrated Element Management System (Integrated EMS)

The Integrated EMS acts as a proxy to the central security administration system. 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. Refer to Centralized security administration overview.

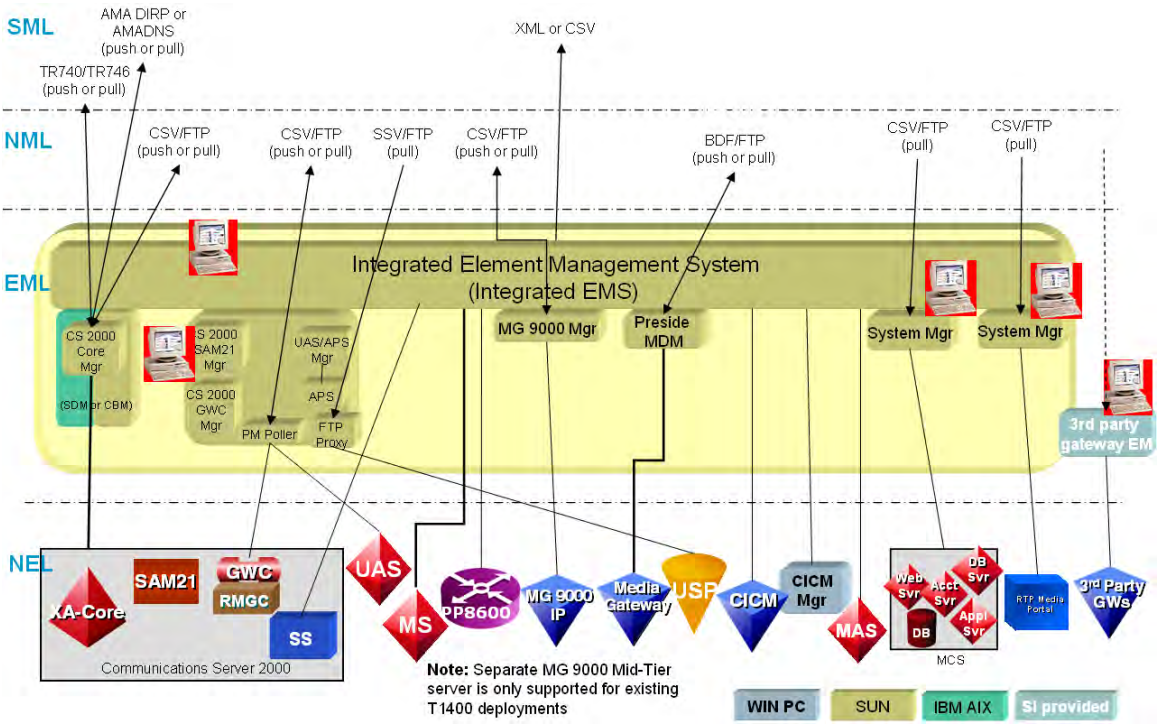
Line gateways

Line gateways are third-party network elements. Security mechanisms for these are vendor-specific. For details, refer to the vendor's documentation.

Security operations architecture

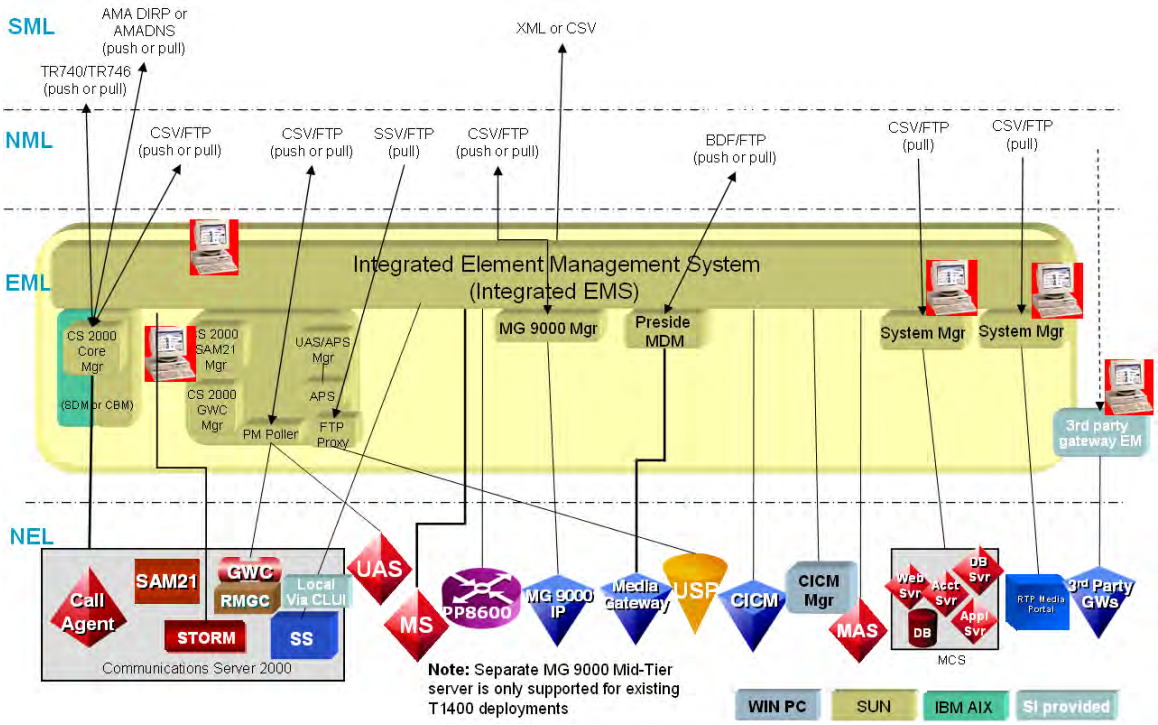
The following figure illustrates the security operations architecture for CS 2000 Server.

Security architecture for the CS 2000 Server (IP solutions)



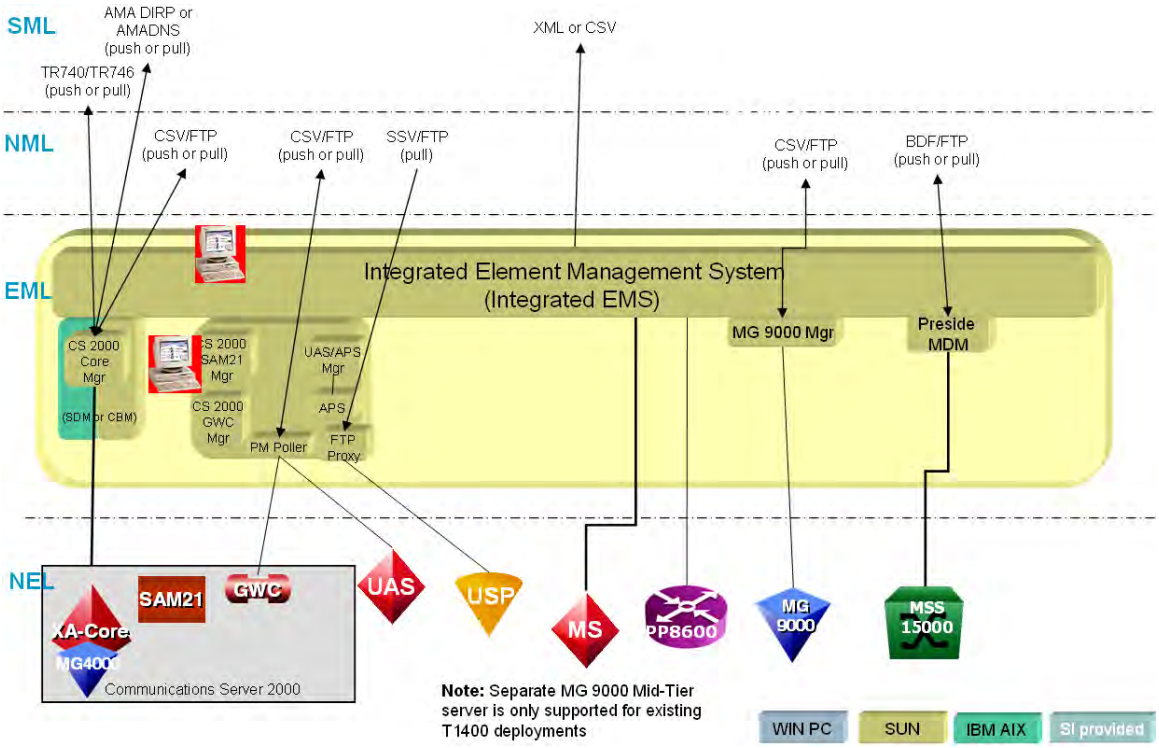
The following figure illustrates the security operations architecture for CS 2000 Server - Compact.

Security architecture for the CS 2000 Server - Compact (IP solutions)



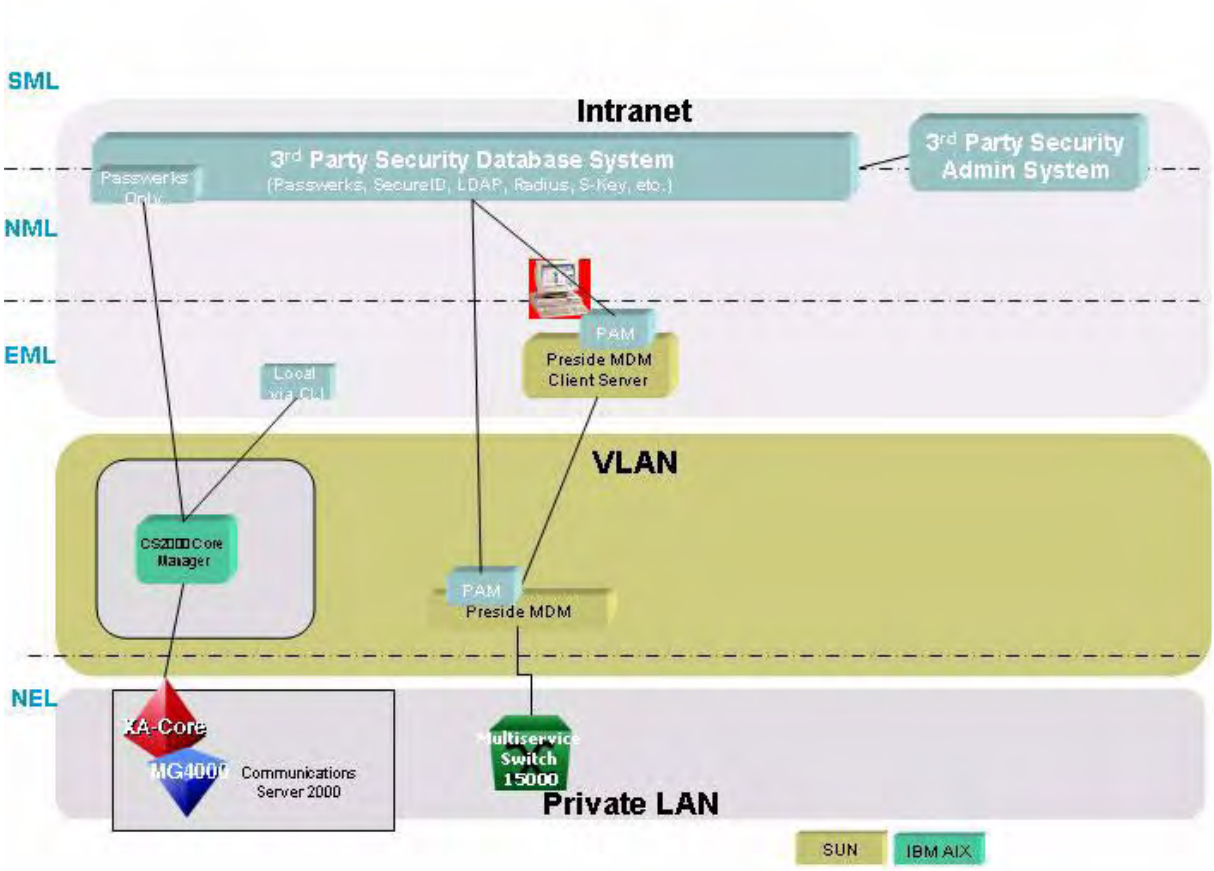
The following figure illustrates the security operations architecture for CS 2000 Server (UA-AAL1).

Security architecture for the CS 2000 Server (UA-AAL1)



The following figure illustrates the security operations architecture for CS 2000 Server (PT-AAL1).

Security architecture for the CS 2000 Server (PT-AAL1)



PT-XA Core or PT-SN70 solutions

If your switch is equipped with a CS 2000 Core Manager, then it can provide security and administration management for the DMS-related and SPM-related equipment on the PT-XA Core or PT-SN70 switch. However, if your switch is not equipped with a CS 2000 Core Manager, the XA-Core (or SN70EM) and MAP provide security and administration management. Please refer to the previous section for details about secure file transfer.

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	USP Security and Administration
NN10160-611	USPc (compact) Security and Administration
NN10161-611	Universal Audio Server Security and Administration
NN10162-611	MG 9000 Security and Administration
NN10163-611	Spectrum Peripheral Module Security and Administration
NN10164-611	MG 4000 Security and Administration
NN10165-611	Interworking Spectrum Peripheral Module (ATM) Security and Administration
NN10166-611	Interworking Spectrum Peripheral Module (IP) Security and Administration
NN10167-611	Dynamic Packet Trunking Spectrum Peripheral Module (IP) Security and Administration
NN10168-611	Dynamic Packet Trunking Spectrum Peripheral Module (ATM) Security and Administration
NN10170-611	CS 2000 Core Manager Security and Administration
NN10171-611	Communication Server 2000 Security and Administration
NN10174-611	Succession Communication Server 3000 Security and Administration
NN10175-611	Call Agent Security and Administration
NN10176-611	STORM Security and Administration

Nortel Networks Network Security and System Administration technical publications

NTP serial number	Title
NN10177-611	SAM21 Shelf Controller Security and Administration
NN10213-611	Gateway Controller Security and Administration
NN10252-611	CICM Security and Administration
NN10180-611	Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP
NN10275-909	Succession Fault Management Logs Reference
NN10337-611	MS 2000 Series Security and Administration
NN10346-611	Session Server Security and Administration
NN10336-611	Integrated EMS Security and Administration
NN10367-111	RTP Media Portal Basics

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.

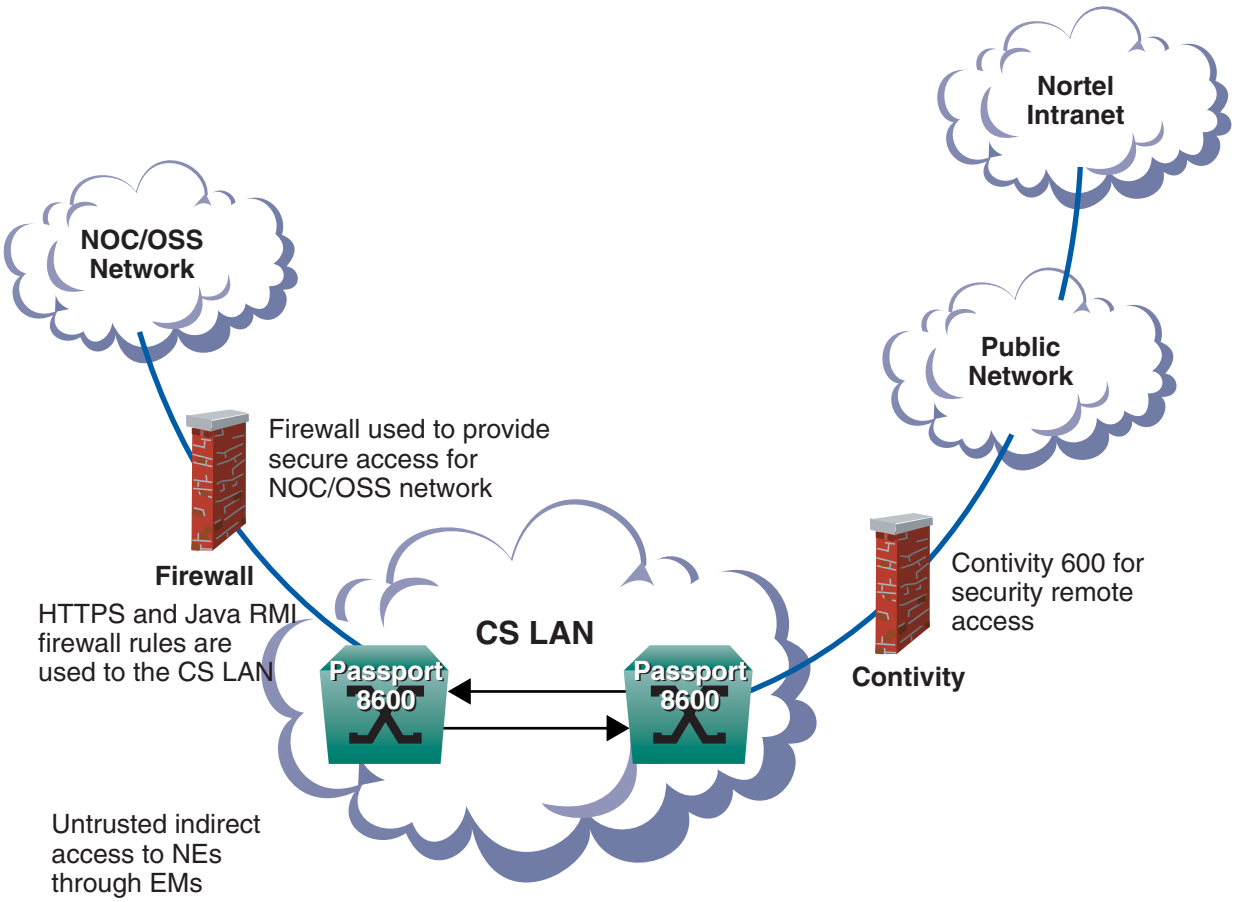
For details, please refer to the following:

- Nortel Networks engineering guidelines for your solution
- Technical Publications

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-Passport 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
- Preside MDM server
- MG 9000 Server (for UA-AAL1 only)
- MG 9000 Mid Tier (for UA-AAL1 only)
- Integrated EMS

The components that are configured in the Bearer subnet are:

- UAS
- Media gateways
- IW-SPM
- MG 9000 (UA-AAL1 only)

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 Succession 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 the 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.

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 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 Succession 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 Succession 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 Succession 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.

Succession 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. Refer to the procedure for Configuring Domain Name Service in ATM/IP Solution-level Configuration Management, NN10276-500 for more information. 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 Succession 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**: line services, line cards, v5.2 services, small line gateways (port level)
- **trk**: trunks, trunk-based services, v5.2 services, small trunking gateways (port level), carrier, carrier-based services
- **mg**: small and large gateways, including UAS, CICM, and PVG
- **mgc**: CS 3000, CS 2000, USP, GWC, CS 2000 SAM21, MCS 5200, 3PC, Storm
- **ems**: 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)	lnadm	trkadm	mgadm	mgcadm	emsadm
Read/Write (rw)	lnrw	trkrw	mgrw	mgcrw	emsrw
Read Only (ro)	lnro	trkro	mgro	mgcro	emsro
Subscriber Provisioning (sprov)	lnsprov	trksprov	mgsprov	mgcsprov	emssprov
Maintenance (mtc)	lnmtc	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 may perform security administration activities.

For details about managing user accounts, refer to your Succession networks component documentation (see Technical Publications).

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	*CS 2000 Core Manager Security and Administration*
NN10180-611	*Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP*
NN10275-909	*Succession Fault Management Logs Reference Volumes 1-3*

PAM-based user authentication

Overview

Succession 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.

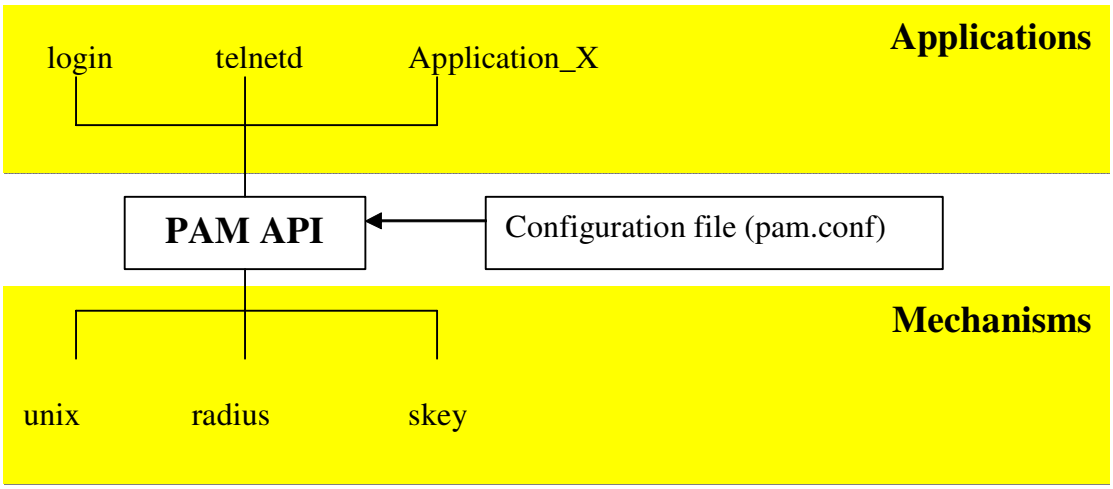
Succession solutions' use of PAM provides unified user login interfaces for the following client applications:

- 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

Succession user authentication services can use a single centralized third party server which provides authentication services to Succession management systems via a pluggable authentication module (PAM) on the Integrated EMS platform.

In (I)SN07, the CICM element manager is integrated into the Succession 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 Succession account managed on a centralized authentication database which interfaces to Succession 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 Succession 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 Succession 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
Passport 8600 Java Device Manager - Device Manager: Local database - Platform access: RADIUS or local database	Local database
Preside 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 authentication, administration, and authorization for most components in the solution. For more details on supported components, see *Integrated EMS Security and Administration*, NN10336-611.

Integrated EMS provides security architecture based on a Pluggable Authentication Module (PAM) and Name Services Switch (NSS).

This architecture provides the following features:

- central administration of user accounts
- 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 method	Documentation reference
USP	HTTPS	USP Security and Administration, NN10159-611
Passport 8600	Radius	Configuring and Managing Security, 314724-B
SSPFS CS 2000 Management Tools Audio Provisioning Server (APS) Network Patch Manager (NPM) MG 9000 Manager	PAM	ATM/IP Solution-level Security and Administration, NN10402-600
Integrated EMS	HTTPS	Integrated EMS Security and Administration, NN10336-611
CICM Manager	HTTPS	CICM Configuration Management, NN10240-511

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	PP8600 Command Line
SSPFS CS 2000 Management Tools Audio Provisioning Server (APS) Network Patch Manager (NPM) MG 9000 Manager	CS 2000 Management Tools

Integrated EMS single sign-on launch points

Network element/EMS platform/application	Integrated EMS launch point
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
APS	APS Manager APS Application
NPM	NPM NPM Command Line
QOS	QOS Command Line
SSPFS	SSPFS 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 command-line Unix interface on the Integrated EMS server. For details, see Configuring a third-party Pluggable Authentication Module.

If NSSwitch services are configured on a third party system, it is important to note that this security solution supports only the NSSwitch group and password databases. Although other database types may be defined in NSSwitch, they are not used by the central security feature.

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.

Hardware requirements

The following table lists details of port usage.

	Port details
Security server	
Radius server	1812 (UDP/Radius authentication)
Apache/Tomcat Apache/Tomcat (SSL)	80:8080 443/8443
SunONE IS	58080, 58081 (TCP for Radius and HTTPS proxies) 58888, 7000 (TCP/logging)
SunONE web services	389 (UDP/LDAP/DS) 2413 (TCP/LDAP)
SSPFS client	
Pam-radius daemon	dynamically allocated port from available ports for programs (range 5,000 - 65,535)

Limitations and restrictions

The following are limitations and restrictions:

- the following devices do not support centralized security administration in (I)SN07: Succession Core and Billing Manager (CBM), Preside MDM, Media Gateway 7400/15000, Multiservice Switch 15000
- the maximum number of provisionable central security users is 1000
- if you set the status of a newly created user to "disable" in the User Profile dialog box, the Integrated EMS Security administration tool can take up to 24 hours to disable command line access to the Integrated EMS server. You can disable an account immediately by setting the user's shell to /bin/false. To set the user's shell to /bin/false, log in to the Integrated EMS server as root and type the command usermod -s /bin/false <username>.
- due to update time intervals, it may take up to 30 minutes after an account or password expires for the expiry to be displayed in the Integrated EMS Security Administration window
- 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 that are supported are pam_dce and pam_ldap
- password aging notification is not supported on any centralized security devices or on the security server in (I)SN07
- on a client SSPFS machine, updates to user profile and group information that are performed on the security server are applied when a user exits all SSPFS client sessions on the client machine and logs back into the client machine
- on SSPFS devices, you must set up SSPFS platform access to enable user platform access to the device
- Succession Centrex IP Client Manager Element Manager (CICM) 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
- telnet access to the Integrated EMS server is restricted to local accounts only
- a certificate must be installed on the Integrated EMS server to ensure that the system operates correctly
- 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/password. Such a conflict may severely impact system operation. The following table lists Sun Solaris system accounts and user IDs.
- the total number of groups that a user can belong to cannot exceed sixteen. The sixteen groups include groups created in Integrated EMS and groups created at the SSPFS/Solaris level.

- the user name cannot be longer than 8 characters.
- the group name cannot be longer than 8 characters.

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, mtssg:50015, FIELD:50016, oracle:50017, patch:50018

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. Refer to procedure Changing the authentication mechanism between UNIX and DCE on page 333 in this document.

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and Succession 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. This 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 a Sun 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 279 in this document
- configuring a central security client, which refers to all the SSPFS-based servers that host the OAM&P applications - refer to procedure Configuring a central security client on page 288 in this document

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 319 in this document.

User accounts

It is recommended to migrate all user accounts on the CS 2000 Management Tools server to the Integrated EMS central security server with the following exceptions:

- accounts that are required to provide emergency access to a device
- super-user accounts, for example, root user
- accounts on which system processes run

The steps to migrate existing user accounts that are to be centrally managed, are included in procedures Configuring the Integrated EMS central security server in the network on page 279 and Configuring a central security client on page 288 in this document. To add new users that are to be centrally managed, refer to the Integrated EMS Security and Administration document, NN10336-611.

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. For more details, refer to procedure Setting up local user accounts on an SSPFS-based server on page 258 in this document.

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 271 in this document.

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.

Tools and utilities

Security and administration procedures are performed on the Sun 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

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 SSPFS-based server on page 254 Changing the APS Oracle account password on page 256 Setting up local user accounts on an SSPFS-based server on page 258

Local user accounts and passwords procedures

Procedure
Changing a user password on an SSPFS-based server on page 269
Changing an expired root password on an SSPFS-based server on page 271
Deleting local user accounts from an SSPFS-based server on page 272
Setting the Oracle Listener password on an SSPFS-based server on page 274
Changing the Oracle Listener password on an SSPFS-based server on page 276

Note: For details about managing user accounts on network components, refer to your Succession networks component documentation (see Technical Publications on page 219).

ATTENTION
Local user accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up local users, removing local users, and changing local passwords, must be performed on both servers.

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 279
Configuring a central security client on page 288
Configuring a third-party Pluggable Authentication Module on page 299

Centralized security configuration procedures

Procedure
Configuring the security server SunONE component on page 310
Reverting the client server to its previous configuration on page 315
Configuring the Single Sign-On token on page 319

Security

The following table lists the procedures available for security.

Security procedures

Procedure
Changing the authentication mechanism between UNIX and DCE on page 333
Setting secure FTP proxy on page 338

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 341
Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater on page 63
Performing a full backup of file systems - (I)SN06.2 or greater on page 70
Performing a data restore on a Sun server - (I)SN06.2 or greater on page 199
Performing a full system restore on a Sun server - SN06.2 or greater on page 205
Cloning the image of one node in a cluster to the other node on page 345

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 353
Starting the SAM21 Manager server application on page 356
Starting the NPM server application on page 358
Starting the APS server application on page 360
Launching CS 2000 Management Tools client applications on page 361
Accessing the Network Patch Manager CLUI on page 374
Starting the batch provisioning tool on page 376
Connect to OSSGate on page 378
Changing modes within OSSGate on page 379
Stopping the SESM server application on page 380
Stopping the SAM21 Manager server application on page 382
Stopping the NPM server application on page 384
Stopping the APS server application on page 386
Disconnect from OSSGate on page 388
Starting and stopping the PM Poller on page 389
Starting and stopping the QoS Collector Application on page 392
Starting the OMPUSH server application on page 397
Stopping the OMPUSH server application on page 399
Initializing the NPM database on page 401

Administration

The following table lists the procedures available for administration.

Administration procedures

Procedure
Cloning the image of one node in a cluster to the other node on page 345
Viewing patching information for the SSPFS on page 404
Increasing the size of a file system on an SSPFS-based server on page 406
Verifying disk utilization on an SSPFS-based server on page 418
Installing an HTTPS certificate on an SSPFS-based server on page 420
Erasing the contents of a CD/DVD on a Sun server on page 430
Clearing the JWS cache on a client workstation on page 423

Changing the Oracle user password on an SSPFS-based server

Application

Use this procedure to change the default Oracle passwords on a Succession Server Platform Foundation Software (SSPFS)-based server.

Note: Refer to procedure Changing the APS Oracle account password on page 256 in this document, to change the default password.

Prerequisites

None

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 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 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.

9 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 CS 2000 Management Tool

1 Open an xterm window and log in using the “root” login and password.

2 When the APS is installed, the Oracle account password is “lionpwd”. If you are unsure whether the password has been changed, obtain the current password by entering the following command:

`/usr/ntdb/uas/scripts/getNTDBpasswd.ksh`

The system displays the current Oracle account password.

3 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 either the default password, “lionpwd” or the password that you displayed in step 2.

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.

4 The following prompt displays.

```
The APS dbserver software should be restarted to
use the new password.

Do you want to do this now? (Y/N)
```

Enter Y to restart the APS dbserver software.

5 You can now check the password change you have made by entering the following command:

`/usr/ntdb/uas/scripts/getNTDBpasswd.ksh`

The system displays the current Oracle account password.

6 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 (see User groups on page 258).

ATTENTION

If upgrading from a release prior to (I)SN06, existing users must be assigned to primary group “succssn” for login access, and to one or more Secondary user groups on page 258 to specify the operations the user is authorized to perform (see step 13 of this procedure).

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.

User groups

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	mgcmtc	mgmtc	emsmtc
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 table below.

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 table below.

Operation	User role mapping
adm (administration)	Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, sprov, mtc, and ro user operations.
rw (read/write)	Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do sprov, mtc, and ro user operations.
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.

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 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

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

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Query a GWC					x
Query an MG					x
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
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	mgcmtc	mgcsprov	mgcro
Query NAT					x
Query media proxy					x
Change associated NAT		x			

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Get tuple					x
Get tuple range					x
Get CM CLLI					x
Add tuple		x			
Replace tuple		x			
Delete tuple		x			
List all tuples	x				
Suspend application	x				
Restore application	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 CM CLLI			x		
Set Auto Refresh					x

ADSL provisioning operations

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

Line provisioning operations

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

Line maintenance operations

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

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, delete, modify V5.2 interface		x					x			
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
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, audit, restart, and image from the NPM GUI or CLUI	x				
Software image from MG 9000 Manager GUI		x			

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 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 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 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 <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 258) and any other user groups you noted in step 12 to which the user already belonged (include 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.

14 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 not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

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 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 password for a specific user by typing

```
# passwd <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.

8 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 not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

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.

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.
5. You have completed this procedure.

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.

ATTENTION

User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

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 SSPFS-based server

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

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

6 You have completed this procedure.

Setting the Oracle Listener password on an SSPFS-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 “**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 SSPFS-based server on page 276 in this document.

ATTENTION
User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

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 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 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
```

8 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 SSPFS installation. This procedure provides the steps to change the Oracle Listener password on a Succession Server Platform Foundation Software (SSPFS)-based server.

ATTENTION

User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

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 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 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/listen
er.ora
Old Parameter File
/opt/oracle/product/8.1.7/network/admin/listen
er.bak
The command completed successfully
```

13 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 should 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.

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 is already installed on the server - refer to procedure Installing an HTTPS certificate on an SSPFS-based server on page 420 in this document
- the SunONE component is already configured to run in secure mode - refer to procedure Configuring the security server SunONE component on page 310 in this document

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 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.

a 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

b Note the user groups the user currently belongs to.

c Delete the user accounts you want to centrally manage, from the Unix files on the server.

Note: In a two-server configuration, delete the user accounts on both servers (inactive and active).

Delete a 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 want to centrally manage.

d 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.

e If the central administration system is the Integrated EMS, assign the user account group information in Unix.

Note: In a two-server configuration, assign the user account group information on both servers (inactive and active).

Assign one or more user groups to a user 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 below) - include a comma between groups, but no space

Secondary user groups

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

userid
is a variable for the user name

Note 1: Do NOT set the Unix password for the user account.

Note 2: The total number of groups that a user can belong to cannot exceed sixteen. The sixteen groups include groups created in Integrated EMS and groups created in SSPFS/Solaris.

6 Complete PAM configuration as follows:

At installation, the Integrated EMS replaces the existing PAM configuration file (pam.conf) with a new PAM configuration file that uses the Integrated EMS security application. If the pam.conf file had any special edits, you must re-edit the file to add those special edits.

You can use the Integrated EMS PAM, which is pre-bundled with the Integrated EMS load, or you can use your own third-party PAM. The Distributed Computing Environment (DCE) and the Lightweight Directory Access Protocol (LDAP) PAMs are the third-party PAMs that are supported. Refer to procedure Configuring a third-party Pluggable Authentication Module on page 299 in this document, if required.

7 Once PAM configuration is complete, add PAM Radius (Remote Access Dialup User Service) clients to the Radius server as follows:

Note: Clients cannot authenticate through the security server if the client IP is not added through the Radius Client Configuration command line interface (CLI).

In a two-server configuration, perform the steps that follow on both servers (inactive and active).

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 Integrated EMS security server

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.

e 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 -
```

f 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 -
```

g 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
 7 - RADSVR Application Configuration
 8 - S1IS Application Configuration

 x - exit

select -
```

h Enter the number next to the “RADSVR Application Configuration” option in the menu.

Example response

```
RADSVR Application Configuration
 1 - LIST_CLIENTS (List all of the existing
     Radius clients)
 2 - DELETE_CLIENTS (Delete a Radius client)
 3 - ADD_CLIENTS (Add clients to the Radius
     server)

 x - exit

select -
```

i Enter the number next to the “ADD_CLIENTS” option in the menu.

Example response

```
===Executing “ADD_CLIENTS”

Enter radius client IP or subnet to ADD (“end
to terminate):
```

j When prompted, enter the radius client IP or subnet you want to add.

Example response

```
Enter radius client shared secret:
```

k When prompted, enter the radius client shared secret.

Example response

```
Enter radius client type:
```

l When prompted, enter the radius client type (for example, IEMS).

Example response

```
Adding Radius server client: 12.45.33.74
Enter radius client IP or subnet to ADD ("end"
to terminate)
```

m When prompted, enter the IP address or subnet of the radius client you want to add.

Note: For a two-server configuration, you must enter the two physical IP addresses of the cluster as well as the virtual IP address of the SSPFS-based host. For a one-server configuration, enter the virtual IP address of the SSPFS-based host.

n Complete the add process by typing

`end`

and pressing the Enter key.

Example response

```
Reload Radius server dynamic configuration
files...
Radius server dynamic configuration reload
successful.

==="ADD_CLIENTS" completed successfully
```

- 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 You have completed this procedure.

Configuring a central security client

Application

Use this procedure to configure a central security client to use the Integrated Element Management System (Integrated EMS) central security server. A central security client is an SSPFS-based server that hosts the Operations, Administration, Maintenance, Performance (OAM&P) applications, such as the Media Gateway (MG) 9000 Manager, CS 2000 Management Tools, and CS 2000 SAM21 Manager.

ATTENTION

You can revert to the previous configuration of the client server using procedure Reverting the client server to its previous configuration on page 315 in this document.

In the event you want to re-configure the central security client to use a new Integrated EMS server IP, perform steps 2 and 3 of this procedure.

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the Integrated EMS 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 279 in this document)

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 Integrated EMS, follow the procedures in the third party documentation.

a 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.

b If the central administration system is the Integrated EMS, assign the user account group information in Unix.

Telnet to the Integrated EMS central security 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

c When prompted, enter your user ID and password.

d Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

e When prompted, enter the root password.

f Assign the user account group information in Unix.

Note: In a two-server configuration, assign the user account group information on both servers (inactive and active).

Assign one or more user groups to a user 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 below) - include a comma between groups, but no space

Secondary user groups

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

userid
is a variable for the user name

Note: Do NOT set the Unix password for the user account.

g Delete the user accounts you just added to the Integrated EMS central security server.

Note: In a two-server configuration, delete the user accounts on both servers (inactive and active).

Telnet 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

h When prompted, enter the user ID and password for an account that was migrated to the Integrated EMS central security server.

i Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

j When prompted, enter the root password.

k 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.

2 Configure the Integrated EMS security server location 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 “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
0.0.0.0):
```

f When prompted, enter the virtual IP address of the Integrated EMS server.

Example response

```
IEMS IP: 45.12.23.56

Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

g Accept the IP address you just entered by typing

ok

and pressing the Enter key.

Example response

```
=== “iems_ip” completed successfully
```

h 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 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)

 x - exit

select -
```

c Enter the number next to the “pam_radius” option in the menu.

Example response

```
===Executing “pam_radius”

Saving original PAM configuration

Updating PAM Configuration to use IEMS
Security Server
IEMS Security Server IP: 45.12.23.56

Enter “ok” to continue
Enter anything else to exit
```

d Accept the PAM configuration update by typing

ok

and pressing the Enter key.

Example response

```
Enter the Shared Secret
```

e When prompted, enter the security server shared secret.

f Accept the shared secret you just entered by typing

ok

and pressing the Enter key.

g When prompted, enter the Radius Client timeout, or press the Enter key to accept the default value if one is specified.

Example response

```
Radius Client Timeout: 12

Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

h When prompted, accept the update by typing

ok

and pressing the Enter key.

Example response

```
Configuring pam-radius
Starting pam-radius
===”pam_radius” completed successfully
```

The system replaces the existing PAM configuration file (pam.conf) with a new PAM configuration file that uses the Integrated EMS security server.

i 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.

j If the pam.conf file had any special edits, you must re-edit the file to add those special edits.

4 Set up SSPFS platform access for users that are centrally managed as follows:

Note: 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 step if users are to be granted platform access.

In a two-server configuration, perform the steps that follow on both servers (active and inactive).

a Telnet to the Integrated EMS central security 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

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.

e Set up the user's shell and home directory by typing

```
# usermod -s /bin/sh -d
/export/home/<username> <username>
```

and pressing the Enter key.

where

username
is the user's ID

Note: The above command is entered on one line.

f Determine the user's user ID (UID) by typing

```
# id <username>
```

and pressing the Enter key.

where

username
is the user's ID

Note: A user's UID is autogenerated when the user's account is created.

g Telnet 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

h When prompted, enter the user's ID and password.

i Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

j When prompted, enter the root password.

k Set up the user's UID on the SSPFS-based server by typing

```
# useradd -u <uid> <username>
```

and pressing the Enter key.

where

uid
is the user's UID you obtained in step 4f.

username
is the user's ID

l 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 ID

m 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 ID

n Log out of the SSPFS-based server by typing

```
# exit
```

and pressing the Enter key.

5 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 300
- LIghtweight Directory Access Protocol (LDAP) PAM on page 305

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

Action

Perform the following steps to complete this procedure.

Distributed Computing Environment (DCE) PAM

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 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 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 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 in the pam.conf" file as indicated:

- change "login auth" to " login auth sufficient /usr/lib/security/$ISA//pam_dce.so.1"
- change "other auth" to " other auth sufficient /usr/lib/security/$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 in the pam.conf" file as indicated:

- change "login account" to " login account sufficient /usr/lib/security/$ISA//pam_dce.so.1"
- change "other account" to " other account sufficient /usr/lib/security/$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 in the 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"

d Add pam_dce with sufficient setting as the first entry in the pam.conf" file as indicated:

- change "other password" to " other password sufficient /usr/lib/security/$ISA//pam_dce.so.1"
- change "sesm password" to " sesm password sufficient /usr/lib/security/$ISA//pam_dce.so.1 try_first_pass"
- change "secclient password" to " secclient password sufficient /usr/lib/security/$ISA//pam_dce.so.1"

e Remove the "other password" entry for iems in the "etc/pam.conf" file.

10 Add the users and permissions to the Integrated EMS using the Integrated EMS Security Administration tool. If required, refer to procedure “Adding new users” in the Integrated EMS Security and Administration document, NN10336-611

11 Disable the users’ status in the Integrated EMS using the Integrated EMS Security Administration tool. If required, refer to procedure “Setting a user profile” in the Integrated EMS Security and Administration document, NN10336-611, for instructions on how to disable a user’s status.

12 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 258 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

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
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnsprov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtc, mgmtc, emsmtc
- 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, lnsprov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtc, mgmtc, emsmtc
- 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, lnsprov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtc, mgmtc, emsmtc
- trkro, lnro, mgcro, mgro, emsro

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

13 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 file <userid>`”.

LIghtweight Directory Access Protocol (LDAP) PAM

At the LDAP server

1 Add the users and permissions to the Integrated EMS using the Integrated EMS Security Administration tool. If required, refer to procedure “Adding new users” in the Integrated EMS Security and Administration document, NN10336-611

2 Disable the users’ status in the Integrated EMS using the Integrated EMS Security Administration tool. If required, refer to procedure “Setting a user profile” in the Integrated EMS Security and Administration document, NN10336-611, for instructions on how to disable a user’s status.

3 Add users and user groups to LDAP server as follows:

Note: For details on user groups, refer to procedure Setting up local user accounts on an SSPFS-based server on page 258 in this document.

a Log in to the LDAP server.

b Add the necessary 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

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.

Below is a sample ldif file to add a user:

```
dn: uid=kcaudill,ou=people,dc=us,dc=nortel,dc=com
cn: kelly Caudill
givename: Kelly
sn: Caudill
gidnumber: 105
homedirectory: /tmp
uidnmuber: 10002
ojectclass: top
ojectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: posixaccount
objectclas: account
ojbectclass: 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

4 Telnet 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

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 Save a backup copy of “nsswitch.conf”, which is located in the “/etc” directory.

9

ATTENTION
This step can reconfigure “nsswitch.conf”, therefore, ensure you saved a backup copy of “nsswitch.conf” before you proceed.

Configure the Solaris Native LDAP 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

10 Replace “nsswitch.conf” with the backup copy of “nsswitch.conf”.

11 Update the “/etc/nsswitch.conf” file as follows:

a Add “ldap” as the first option for the password and group.

The entries would look similar to “passwd: ldap files” and “‘group: ldap files” after the change.

This enables the group information to come from LDAP.

12 Edit the /etc/pam.conf file as follows:

a Add pam_ldap with sufficient setting as the first entry in the pam.conf" file as indicated:

- change "login auth" to " login auth sufficient /usr/lib/security/$ISA//pam_ldap.so.1"
- change "other auth" to " other auth sufficient /usr/lib/security/$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 in the pam.conf" file as indicated:

- change "login account" to " login account sufficient /usr/lib/security/$ISA//pam_ldap.so.1"
- change "other account" to " other account sufficient /usr/lib/security/$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 in the 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"

d Add pam_ldap with sufficient setting as the first entry in the pam.conf" file as indicated:

- change "other password" to " other password sufficient /usr/lib/security/$ISA//pam_ldap.so.1"
- change "sesm password" to " sesm password sufficient /usr/lib/security/$ISA//pam_ldap.so.1 try_first_pass"
- change "secclient password" to " secclient password sufficient /usr/lib/security/$ISA//pam_ldap.so.1"

13 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 file <userid>`".

Configuring the security server SunONE component

Application

Use this procedure to configure the security server SunONE component if you want it to run in secure mode on the central security server and central security clients.

Use one of the methods below according to your office configuration:

- Simplex configuration (one server) on page 310
- High-availability configuration (two servers) on page 312

Prerequisites

An HTTPS certificate must already be installed on the Integrated Element Management System (EMS) server. If required, refer to procedure Installing an HTTPS certificate on an SSPFS-based server on page 420.

Note: In a two-server configuration, the HTTPS certificate must be installed on both servers (active and inactive).

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At your workstation

1 Telnet to the Sun 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_s1isext/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_s1isext.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.

9 You have completed this procedure.

High-availability configuration (two servers)

At your workstation

1 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 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_s1isext/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_s1isext.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

```
# shutdown -i 0 -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_s1isext/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_s1isext.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.

11 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 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 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, re-provision the user accounts on the active server first and then on the inactive server. If required, refer to procedure Setting up local user accounts on an SSPFS-based server on page 258, in this document.

7 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 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you want to configure SSO

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.

14 You have completed this procedure.

Starting Integrated EMS server in HTTPS mode

HTTPS is the secure mode of communication between the client and the server of Integrated EMS.This mode of communication is also known as the Secured Socket Layer (SSL)mode. Data transmitted in this mode is encrypted over the TCP or IP connection and can be viewed through browsers.To view the secured data through the browsers, the “https” (instead of “http”) protocol must be specified in the URL.

Integrated EMS Web Start client can be connected to the server through the HTTPs 9091 port.

To enable or disable HTTPS mode of communication for Integrated EMS, follow these steps:

At Integrated EMS server

1. Connect to the host in which Integrated EMS Server is installed with telnet session.
2. Switch to the <IEMS Home>/bin folder.
3. Run the script SSLUtil.sh with the parameter "Enable" or "Disable". Use "Enable" parameter to enable the HTTPS mode for Integrated EMS Server and use "Disable" option to disable the HTTPS mode.

   Example

   To enable HTTPS mode for Integrated EMS Server, run the script using "Enable" parameter as given in the following example.

   ```
   # SSLUtil.sh Enable
   ```

   Example

   To disable HTTPS mode for Integrated EMS Server, run the script using "Disable" parameter as given in the following example.

   ```
   # SSLUtil.sh Disable
   ```

Security Token Administration GUI overview

Integrated EMS Security Token Administration GUI can be used to:

- view user session (or token) information
- terminate user sessions

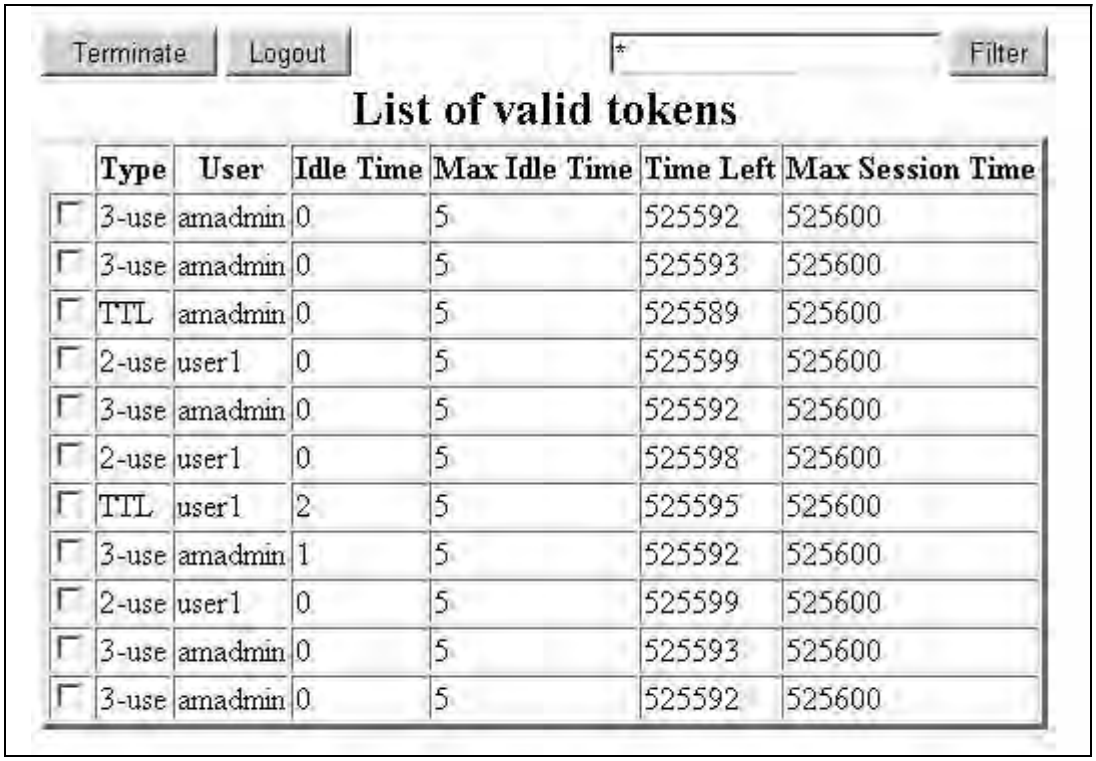
Integrated EMS Security Token Admininstration GUI displays all of the user sessions that are available to the Identity Server and displays the expiration time for each session. See List of valid tokens window.

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



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 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:

`http://hostname:8080/tokenadmin`

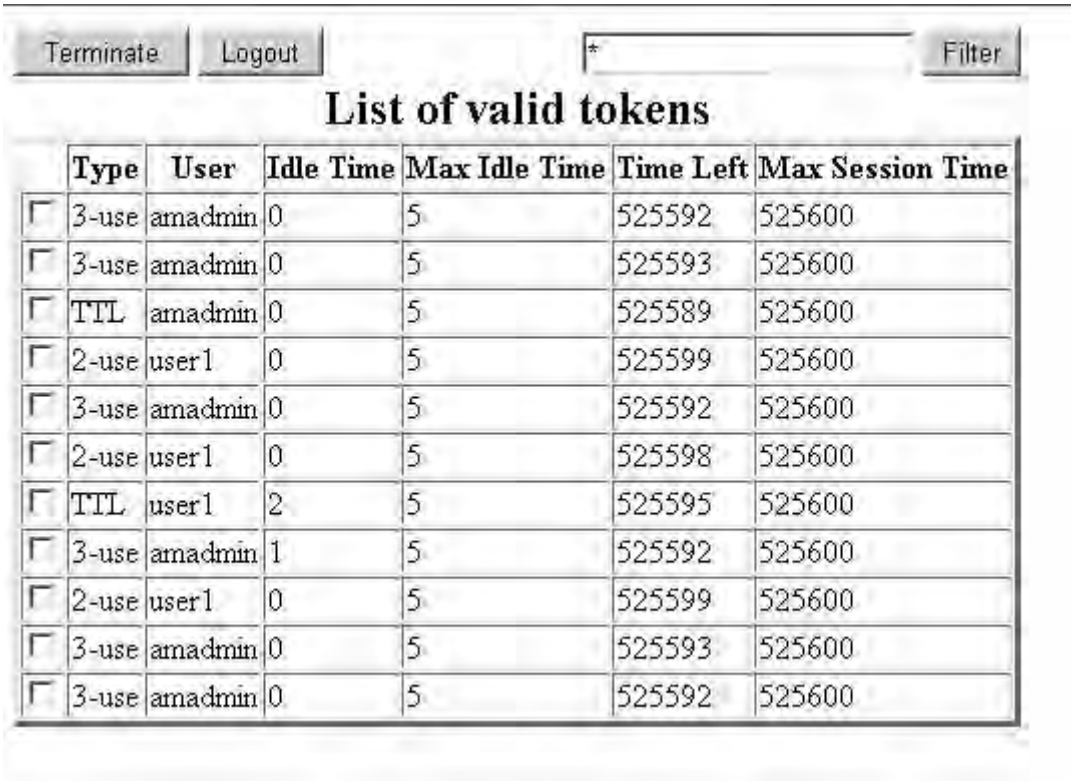
The Token Management window is displayed as in the following figure.

Token Management window

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	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

Viewing a user session

Use this procedure to view one user session or a range of sessions that are available to the Identity Server.

Prerequisites

You require a user account with admininstration privileges to perform this task.

Action

At the Integrated EMS Security Token Administration GUI

1 Log in to the Integrated EMS Security Token Admininstration GUI.

a Open the Token Management window. 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.

	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 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 Admininstration 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.

	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.

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):

- Switching from UNIX to DCE for authentication on page 333
- Switching from DCE to UNIX for authentication on page 337

The default authentication mechanism is UNIX.

Prerequisites

To perform this procedure, you need to have the root user ID and password for the Sun 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 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 258 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, lnsprov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtc, mgmtc, emsmtc
- 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, lnsprov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtc, mgmtc, emsmtc
- 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, lnsprov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtc, mgmtc, emsmtc
- trkro, lnro, mgcro, mgro, emsro

11 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 file <userid>`".

Switching from DCE to UNIX for authentication

At your workstation

1 Telnet to the CS 2000 Management Tools 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 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.

9 You have completed this procedure.

Setting secure FTP proxy

Application

In order to have a secure (i.e. 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 338
- Setting up SSH port forwarding on Windows on page 339

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 CS 2000 Management Tools 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:CS 2000 Management Tools
host:9999 CS 2000 Management Tools host
```

To securely transmit data from machine A to the CS 2000 Management Tools 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 CS 2000 Management Tools server.

5 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 on "Session" and complete the following fields:

- In the "Host Name (or IP address)" field, enter the host name or IP address of the CS 2000 Management Tools server.
- In the "Port" field, enter 22.
- Under "Protocol:" select SSH.

b Click on ”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 CS 2000 Management Tools server, and “port” is the port number on which the CS 2000 Management Tools server listens for input (9999 is the standard port on which the CS 2000 Management Tools server listens for a client connection)
- Select “Local”, and click the Add button.
- Click the Open button.

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 CS 2000 Management Tools server as long as the port-forwarding session you just created exists.

6 Establish a secure connection as follows:

a Click on 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 on ”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 CS 2000 Management Tools server is established.

7 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 Succession 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 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 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.

13 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.

ATTENTION
If you are using this procedure during an upgrade to clone the image of the upgraded node onto the other node running the previous release, at this point, you can easily revert this upgraded node to the previous release. Continuing with this procedure, clones the image of the upgraded node onto the node running the previous release, and once both nodes are upgraded, reverting back to the previous release will require a full system restore.

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you may need console access to the Inactive node

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 Telnet to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Active node in the cluster

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 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
```

6 Use the following table to determine your next step.

If	Do
all applications are running	step 9
one or more applications are not running	step 7

7 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

8 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 9

9 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 11
not running	step 10

10 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 11

11 Use the following table to determine your next step.

If your server is running the	Do
CS 2000 Management Tools software	step 12
MG 9000 software	step 14

12 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
```

13 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 14

14

ATTENTION

In this step, the system clones the image of the Active unit onto the Inactive unit. If this is the first time the unit is being cloned, you will be prompted for the Ethernet address of the Inactive unit. If this is not the first time the unit is being cloned, the system remembers the ethernet address of the Inactive unit, and executes the clone using this ethernet address. However, if you replaced the Inactive unit or executed a reverse restore (i.e. switched unit 0 and 1), the Inactive unit will have a different ethernet address from the one retained in the system. Therefore, you must specify the new ethernet address of the Inactive server in the command (i.e. startb <new ethernet address>). If required, perform steps 15 through 18 to obtain the Ethernet address of the Inactive unit before executing this step.

Start the cloning process using substep a or b. Only use substep b if you replaced the Inactive unit or executed a reverse restore (i.e. switched unit 0 and 1).

a Start the cloning process by typing

```
# startb
```

and press the Enter key.

If the system	Do
prompts you for the Ethernet address	step 15
indicates it is using Ethernet address <EthernetAddress>	step 20

b Start the cloning process by typing

```
# startb <new ethernet address>
```

and press the Enter key.

Note: If required, perform steps 15 through 18 to obtain the Ethernet address of the Inactive unit before executing this step.

Proceed to step 20.

At the console connected to the inactive node

15 Log in to the inactive node through the console (port A) using the root user ID and password.

16 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

17 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.
```

18 Take note of the Ethernet address that is displayed.

At your workstation (telnet session to Active node)

19 Enter the Ethernet address of the inactive node you noted in step 18.

20 Use the following table to determine your next step.

If the system	Do
prompts you to enter the command “boot net - image”	step 21
does not prompt you to enter the command “boot net - image”	step 23

At the console connected to the inactive node

21 Log in to the inactive node through the console (port A) using the root user ID and password if not already logged in.

22 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 (telnet session to Active node)

23 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
```

24 You have completed this procedure.

Starting the SESM server application

Application

Use this procedure to start the SESM server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools 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 Use the following table to determine your next step.

If the release you are running is	Do
(I)SN05	step 6 only
(I)SN06	step 7 only
(I)SN06.2 or greater	step 8 only

6 For the (I)SN05 release, start the SESM server application as follows:

a Start the SESM server application by typing

```
# /opt/nortel/NTptm/bin/ptmctl start
```

and pressing the Enter key.

b Verify the SESM server application started by typing

```
# /opt/nortel/NTptm/bin/ptmctl status
```

and pressing the Enter key.

Example response:

```
PTM PROCESS STATUS
 rmirgistery  Running
 snmpfactory  Running
 proxyagent   Running
 MI2Server    Running
```

7 For the (I)SN06 release, start the SESM server application as follows:

a Start the SESM server application including the Proxy Agent by typing

```
# /opt/nortel/NTsesm/admin/bin/ptmctl -f
start
```

and pressing the Enter key.

b Verify the SESM server application started by typing

```
# /opt/nortel/NTsesm/admin/bin/ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS ----------------

COMPONENT      STATUS
---------      -------
Proxy Agent    RUNNING
RMI Registery  RUNNING
Snmpfactory    RUNNING
MI2 Server     RUNNING

SESM APPLICATION STATUS: All Applications
ready
```

8 For the (I)SN06.2 or greater release, start the SESM server application as follows:

a Start the SESM server application by typing

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

```
# servstart SESMService
```

and pressing the Enter key.

b Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.

c Verify the SESM server application started by typing

```
# servman query -status -group SESMService
```

and pressing the Enter key.

Example response:

```
Executing: /opt/servman/bin/servquery
-status - group SESMService

Succession CS2K Management Tools VERSION:
SESM_7_047_0

Current status of the CS2K Management Tools:
     LMM is running
     TMM is running
     GWCEM is running
     UASEM is running
     OSS Gate is running
```

9 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.

At your workstation

1 Telnet to the CS 2000 Management Tools 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 Use the following table to determine your next step.

If the release you are running is	Do
(I)SN06	step 6 only
(I)SN06.2 or greater	step 7 only

6 For the (I)SN06 release, start the SAM21 Manager server application as follows:

a Start the SAM21 Manager server application by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl start
```

and pressing the Enter key.

b Verify the SAM21 Manager server application started by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl status
```

and pressing the Enter key.

7 For the (I)SN06.2 or greater release, start the SAM21 Manager server application as follows:

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

a Start the SAM21 Manager server application by typing

```
# servstart SAM21EM
```

and pressing the Enter key.

b Verify the SAM21 Manager server application started by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

8 You have completed this procedure.

Starting the NPM server application

Application

Use this procedure to start the Network Patch Manager (NPM) server application.

Prerequisites

Both CORBA and the database must be installed.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 Use the following table to determine your next step.

If the release you are running is	Do
(I)SN05 or (I)SN06	step 6 only
(I)SN06.2 or greater	step 7 only

6 For the (I)SN05 or (I)SN06 release, start the NPM server application as follows:

a Start the NPM server by typing

```
# npmsrvr start
```

and pressing the Enter key.

b Verify the NPM server application started by typing

```
# npmsrvr status
```

and pressing the Enter key.

7 For the (I)SN06.2 or greater release, start the NPM server application as follows:

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

a Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

b Verify the NPM server application started by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

8 You have completed this procedure.

Starting the APS server application

Application

Use this procedure to start the APS server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

At your workstation

1 Telnet to the CS 2000 Management Tools 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 Start the APS server application as follows:

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

a Start the APS server application by typing

```
# servstart APS
```

and pressing the Enter key.

b Verify the APS server application started by typing

```
# servman query -status -group APS
```

and pressing the Enter key.

6 You have completed this procedure.

Launching CS 2000 Management Tools 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)
- Succession 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 374 in this document.

This procedure provides the following four methods to launch a CS 2000 Management Tools client application:

- Launching applications from a web browser on page 363. You must use this method when launching an application for the first time.
- Launching applications from the JWS Application Manager on page 366.

  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 369.

  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 372.

Note: You can also launch applications 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.

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 may experience the “blue screen of death” in your Windows environment. You can obtain information on this issue at the following URL: 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 1.4.1_02 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 1.4.1_02.

Action

Launching applications from a web browser

At your workstation

1 Launch your web browser.

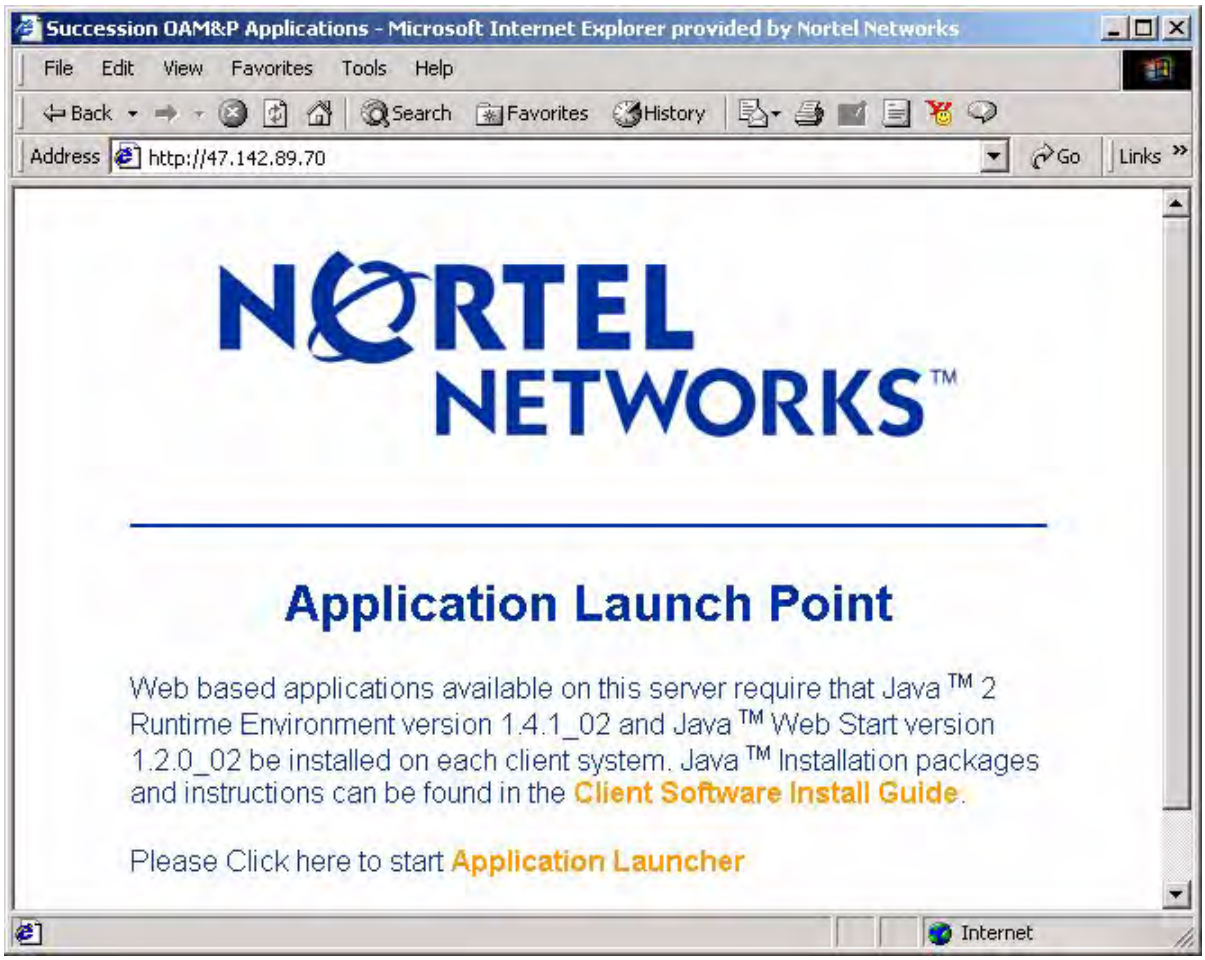
2 Access the CS 2000 Management Tools server by typing

>http://<host>

where

<host>
is the name or IP address of the CS 2000 Management Tools server where the CS2M software package is installed

The “Application Launch Point” page appears.



3 Refer to the following table to determine your next step.

If	Do
you have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 9
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 4
you do not know which version of JRE and JWS you have	step 4

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 1.4.1_02 and JWS 1.2.0_02 installed	step 8
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 5

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.

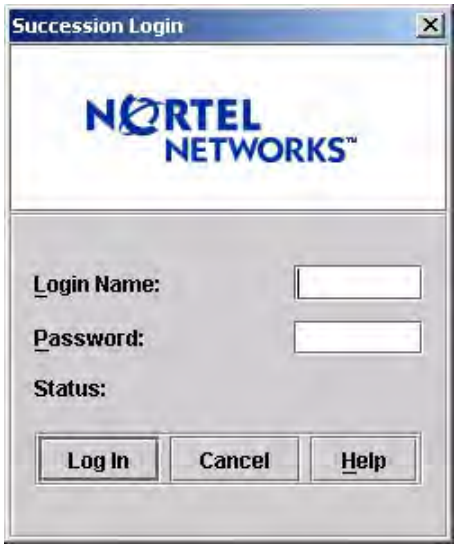
7 Click **Java 2 Runtime Environment Software Download** under “Microsoft Windows” or “Sun Solaris” to download and install the software.

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”.

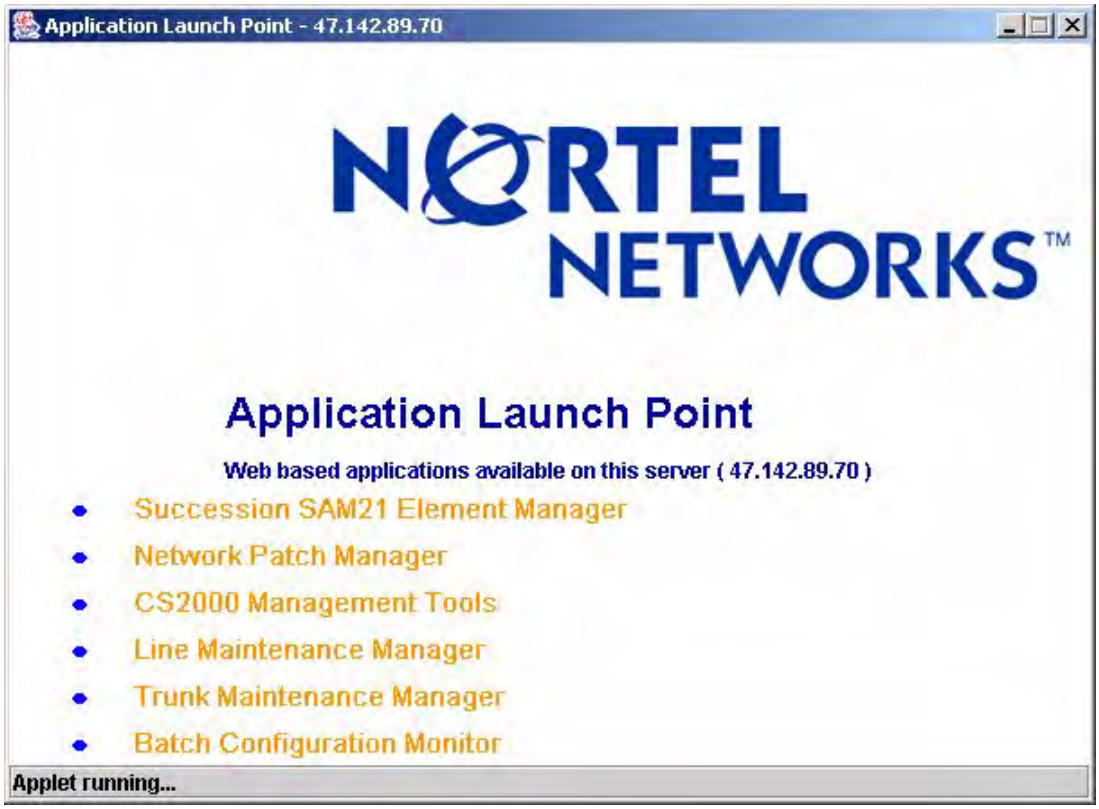
9 Click **Application Launcher**.

The Login window appears.



10 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.



11 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

Note: If you delay clicking on an application link by 5 minutes or more after you log in, the login window will appear requiring you to log in again.

12 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.

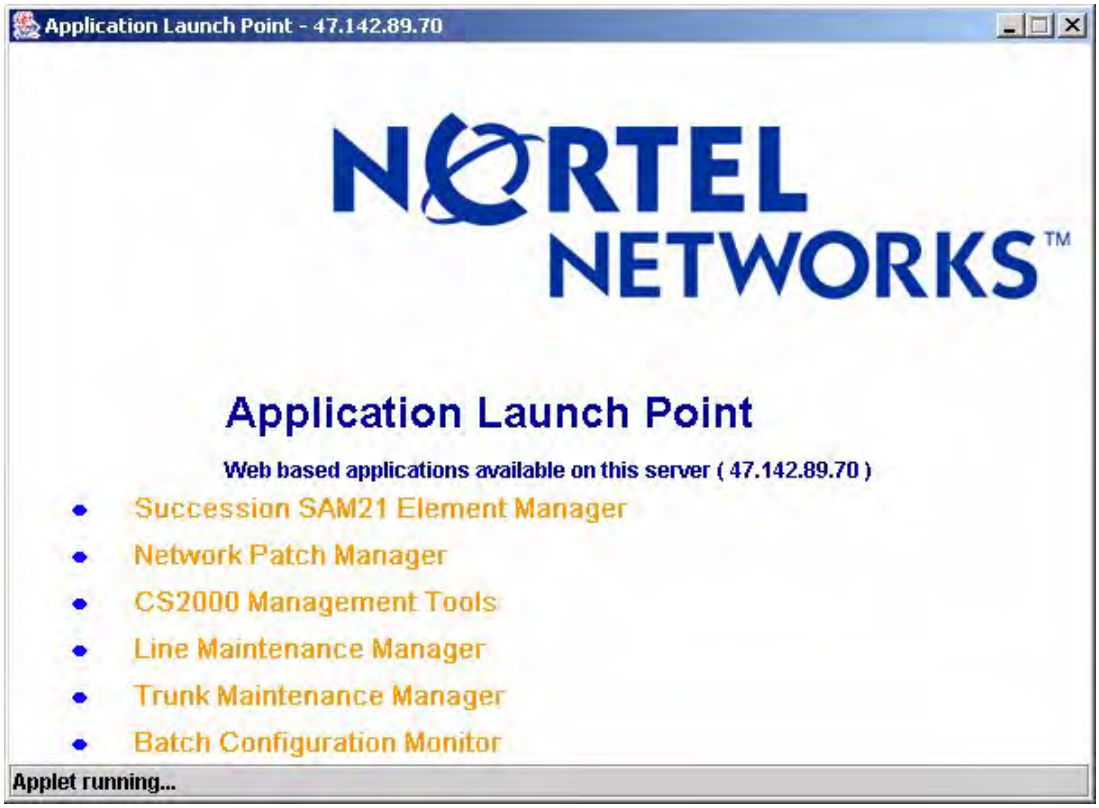
Note: If you do not see the downloaded applications as shown in the example above, on the **View** menu, click **Downloaded Applications**.

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 on the link for the application you want to launch.

The interface for the application you launched, is displayed.

5 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 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.

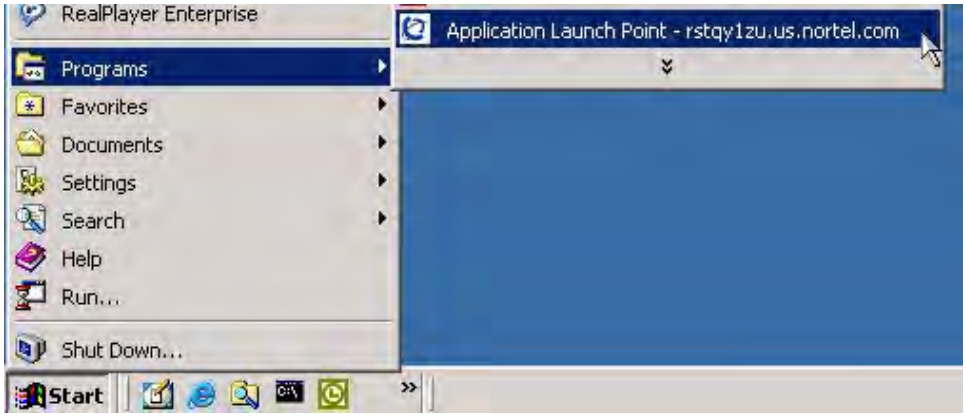
Note: For short-cut icons to be present on your desktop, you must have the right settings under the Shortcut Options tab, which is accessed through **File->Preferences** in the JWS Application Manager.

The Login window appears.

Proceed to step 2.

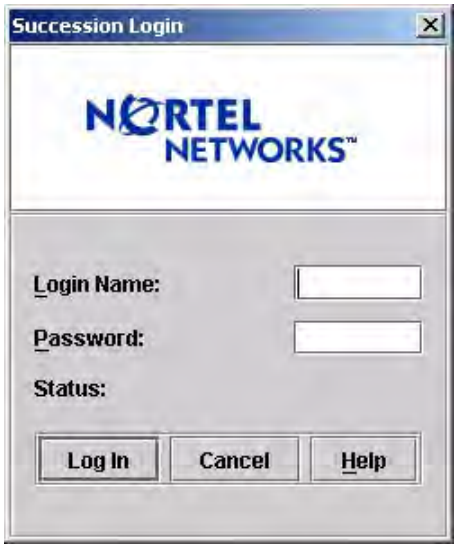
OR

b To launch a CS 2000 Management Tools client application from the Start menu, click **Start->Programs**, then click on the CS 2000 Management Tools client application you want to launch.

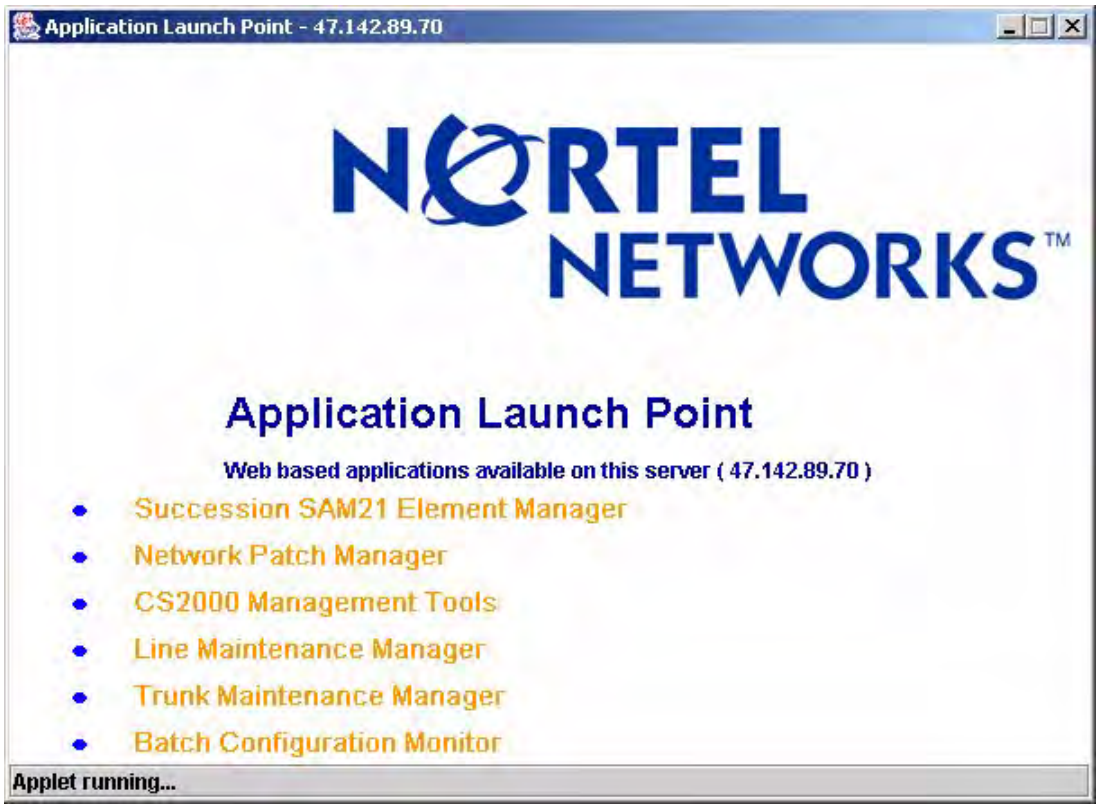


The Login window appears.

2 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



3 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

4 You have completed this procedure.

Launching specific applications using a URL

ATTENTION

You must have Java™ 2 Runtime Environment (JRE) version 1.4.1_02 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 363.

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.

4 You have completed this procedure.

Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and Succession 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 re-launch 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 client applications on page 361 in this document.

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 on page 258 in this document.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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>
```

5 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 Telnet to the CS 2000 Management Tools 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]
```

5 You have completed this procedure.

Connect to OSSGate

Application

Use this procedure to connect to OSSGate.

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 the telnet client

1 Connect to the OSSGate using the OSSGate Server name and the port number.

Example

```
> telnet <host_name> <port_number>
```

where

host_name
is the name of the CS 2000 Management Tools server

port_number
is the port number (default 10023)

Note: The entry of this command depends on your telnet client.

2 When prompted, enter your username and password separated by a space, and press the Enter key.

Example

```
Enter username and password
> ossuser osspassword
```

3 You have completed this procedure.

Changing modes within OSSGate

Application

Use this procedure to change between CI and XML mode in OSSGate. OSSGate supports two modes: 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 (Ctrl+B) at the same time.

```
> ^B
```

and pressing the Enter key.

Note: Based on the terminal settings, the Ctrl+B character may not be 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.
```

3 You have completed this procedure.

Stopping the SESM server application

Application

Use this procedure to stop the SESM server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools 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 Use the following table to determine your next step.

If the release you are running is	Do
(I)SN05	step 6 only
(I)SN06	step 7 only
(I)SN06.2 or greater	step 8 only

6 For the (I)SN05 release, stop the SESM server application by typing

```
# /opt/nortel/NTptm/bin/ptmctl stop
```

and pressing the Enter key.

7 For the (I)SN06 release, stop the SESM server application as follows:

a Stop the SESM server application including the Proxy Agent by typing

```
# /opt/nortel/NTsesm/admin/bin/ptmctl -f stop
```

and pressing the Enter key.

b Verify the SESM server application stopped by typing

```
# /opt/nortel/NTsesm/admin/bin/ptmctl status
```

and pressing the Enter key.

Example response (without stopping Proxy Agent):

```
SESM STATUS --------------------------------

  COMPONENT                  STATUS
  --------                   ------
 Proxy Agent                 NOT RUNNING
 RMI Registry                NOT RUNNING
 Snmpfactory                 NOT RUNNING
 MI2 Server                  NOT RUNNING

Current number of SESM processes running: 0
(of 4)

SESM APPLICATION STATUS: No Applications are
ready
```

8 For the (I)SN06.2 or greater release, stop the SESM server application as follows:

a Stop the SESM server application by typing

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

```
# servstop SESMService
```

and pressing the Enter key.

b Verify the SESM server application stopped by typing

```
# servman query -status -group SESMService
```

and pressing the Enter key.

9 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

At your workstation

1 Telnet to the CS 2000 Management Tools 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 Use the following table to determine your next step.

If the release you are running is	Do
(I)SN06	step 6 only
(I)SN06.2 or greater	step 7 only

6 For the (I)SN06 release, stop the SAM21 Manager server application as follows:

a Stop the SAM21 Manager server application by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl stop
```

and pressing the Enter key.

b Verify the SAM21 Manager server application stopped by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl status
```

and pressing the Enter key.

7 For the (I)SN06.2 or greater release, stop the SAM21 Manager server application as follows:

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

a Stop the SAM21 Manager server application by typing

```
# servstop SAM21EM
```

and pressing the Enter key.

b Verify the SAM21 Manager server application stopped by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

8 You have completed this procedure.

Stopping the NPM server application

Application

Use this procedure to stop the Network Patch Manager (NPM) server application.

Prerequisites

All users of the NPM CLUI and GUI should exit before stopping the NPM server application.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 Use the following table to determine your next step.

If the release you are running is	Do
(I)SN05 or (I)SN06	step 6 only
(I)SN06.2 or greater	step 7 only

6 For the (I)SN05 or (I)SN06 release, stop the NPM server application as follows:

a Stop the NPM server by typing

```
# npmsrvr stop
```

and pressing the Enter key.

b Verify the NPM server application stopped by typing

```
# npmsrvr status
```

and pressing the Enter key.

7 For the (I)SN06.2 or greater release, stop the NPM server application as follows:

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

a Stop the NPM server application by typing

```
# servstop NPM
```

and pressing the Enter key.

b Verify the NPM server application stopped by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

8 You have completed this procedure.

Stopping the APS server application

Application

Use this procedure to stop the APS server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

At your workstation

1 Telnet to the CS 2000 Management Tools 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 Use the following table to determine your next step.

If the release you are running is	Do
(I)SN06	step 6 only
(I)SN06.2 or greater	step 7 only

6 For the (I)SN06 release, stop the APS server application as follows:

a Stop the APS server application by typing

```
# /opt/uas/aps/scripts/killDbServer.sh
```

and pressing the Enter key.

```
# /usr/sbin/pmfadm -s aps KILL
```

and pressing the Enter key.

b Verify the APS server application stopped by typing

```
# pmfadm -l aps
```

and pressing the Enter key.

7 For the (I)SN06.2 or greater release, stop the APS server application as follows:

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

a Stop the APS server application by typing

```
# servstop APS
```

and pressing the Enter key.

b Verify the APS server application stopped by typing

```
# servman query -status -group APS
```

and pressing the Enter key.

8 You have completed this procedure.

Disconnect 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 (Ctrl+B) at the same time.

   > **^B**

   and pressing the Enter key.

   Note: Based on the terminal settings, the Ctrl+B character may not be 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: Based on the terminal settings, the Ctrl+B character may not be displayed on the screen.

4. End the session by typing

   ? **clearconv**

   and pressing the Enter key.

5. 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.

At your workstation

1 Telnet to the CS 2000 Management Tools 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 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 7
stop the PM poller	step 9

7 Start the PM poller as follows:

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

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 9

9 Stop the PM poller as follows:

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

a Start 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.
```

10 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 CS 2000 Management Tools 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 Telnet to the CS 2000 Management Tools 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 Verify the status of QCA by typing

```
# /opt/nortel/qca/query_qca
```

and pressing the Enter key.

6 Use the following table to determine your next step.

If you want to	Do
start QCA	step 7
stop QCA	step 8

7 Start QCA by typing

/opt/nortel/qca/qca_server

and pressing the Enter key.

Example response

```
Attempting to register QCA as Qca with PFMDAM.
Have you checked the qca.properties file? Are
you sure you want to continue? [no or yes]

Registration as Qca was ok. QCA started.

QCA has been started with the following
properties...
MaxFileSize=1 (Range is 1 to 100)
MaxFileTime=15 (Range is 1 to 240)
recycleToD=0 (Range is 0 to 23)
portNumber=20000 (Range is 20000 to 20004)
RetainFileTime=5 (Range is 1 to 30)
fileExt=xml (Default is xml)
nodeName=QCA (Default is QCA)
closedFileCompression=true (Default is 'True')
oldFileCompression=true (Default is 'True')

Please check /var/log/customerlog if any of the
above properties are out of range.
```

When you start QCA, the values in the configuration file (qca.properties) are validated. If a value in the configuration file is invalid or missing, the default value is used. When this occurs, a log is generated to inform you that a default value is being used. If using default values is unacceptable, you can stop QCA at this point, and change the values.

If	Do
a log is generated and you want to stop QCA	step 8
a log is generated but you do not want to stop QCA	you have completed this procedure
no log is generated	you have completed this procedure

8 Stop QCA by typing

```
# /opt/nortel/qca/stop_qca
```

and pressing the Enter key.

Example response

```
Are you sure you want to stop the QCA? Have you
checked the port number in qca.properties? [no
or yes].
```

If you	Do
checked the port number	step 10
did not check the port number	step 9

9 Check the port number in qca.properties, and repeat step 8.

10 Confirm you checked the port number by typing

yes

and pressing the Enter key.

Example response

```
De-registering QCA from servman
Attempting to unregister QCA as Qca from PMFADM.
Attempting to stop local QCA on port : 20001
QCA stopped successfully.
```

11 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 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where SSPFS is installed

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 4
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.
```

5 You have completed this procedure.

Stopping the OMPUSH server application

Application

Use this procedure to stop the OMPUSH server application.

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 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where SSPFS is installed

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 4
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.
```

5 You have completed this procedure.

Initializing the NPM database

Application

Use this procedure to initialize the Network Patching Manager (NPM) database.

Prerequisites

Only the root user can perform this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 - SAM21EM Application Configuration
 3 - PSE Application Configuration
 4 - 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 - PFRS (Patch File Receipt System
     Configuration (PFRS))
 2 - CreateDB (Initialize or re-initialize the
     NPM database)


 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 exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

11 You have completed this procedure.

Viewing patching information for the SSPFS

Application

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server where the application resides by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 that corresponds 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 that corresponds 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.

9 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 407
- High-availability configuration (two servers) on page 412

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 data backup on an SSPFS-based server: (I)SN06.2 or greater on page 63 and Performing a full backup of file systems - (I)SN06.2 or greater on page 70 if required.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

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 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%    /PROV_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 could be 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

```
# echo `/opt/nortel/sspfs/fs/meta.pl fs` 2048
/ 5000 - p | dc
```

and pressing the Enter key.

Note: Use the back quote on the same key as the Tilda (~) for */opt/nortel/sspfs/fs/meta.pl fs.*

The resulting number is the amount of free disk space in megabytes (MB) that can be allocated to existing file systems.

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

b Use the following table to determine your next step.

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

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).

11 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 Telnet 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.

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.

At the Inactive node

5 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 6
“ClusterIndicatorACT”	step 1

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

```
# udstat
```

and pressing the Enter key.

If the file systems are	Do
STANDBY normal UP clean	step 7
not STANDBY normal UP clean	contact your next level of support

7 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%    /PROV_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.

8 Note the file system you want to increase, as well as its current size (under column “Kbytes”).

9 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.

10

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 could be 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 8).

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.

11 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

```
# echo `/opt/nortel/sspfs/fs/meta.pl fs` 2048
/ 5000 - p | dc
```

and pressing the Enter key.

Note: Use the back quote on the same key as the Tilda (~) for */opt/nortel/sspfs/fs/meta.pl fs.*

The resulting number is the amount of free disk space in megabytes (MB) that can be allocated to existing file systems.

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

b Use the following table to determine your next step.

If	Do
the value you determined in step 10 (size by which to increase the file system) is greater than the value you obtained in step 11a (amount of free disk space you can allocate to file systems)	contact Nortel Networks for assistance
the value you determined in step 10 (size by which to increase the file system) is less than the value you obtained in step 11a (amount of free disk space you can allocate to file systems)	step 12

12

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 8)

size
is the size in megabytes (m) by which you want to increase the file system (determined in step 10)

Example

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

Note: The example above increases the "/data/qca" file system by 10 megabytes (MB).

13 Reboot the Inactive node by typing

```
# init 6
```

and pressing the Enter key.

14 Wait for the Inactive node to reboot, then log in again using its physical IP address.

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

```
# udstat
```

and pressing the Enter key.

If the file systems are	Do
STANBY normal UP clean	step 16
not STANBY normal UP clean	contact your next level of support

16 Telnet 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

17 When prompted, enter your user ID and password.

18 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

19 When prompted, enter the root password.

At the Active node

20 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

21 Clone the other node using procedure Cloning the image of one node in a cluster to the other node on page 345 if required.

22 You have completed this procedure.

Verifying disk utilization on an SSPFS-based server

Application

Use this procedure to verify disk utilization by the file systems on a Succession Server Platform Foundation Software (SSPFS)-based server.

Prerequisites

You must have root user privileges.

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 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 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%    /PROV_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
```

7 You have completed this procedure.

Installing 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).

ATTENTION
An HTTPS certificate is preserved over an SSPFS upgrade. Therefore, you do not need to perform this procedure following an SSPFS upgrade if an HTTPS certificate was already installed on the server.

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 websites
- 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.

Use one of the methods below to install the certificate according to your office configuration:

- Simplex configuration (one server) on page 421
- High-availability configuration (two servers) on page 426

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 must 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 must 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

Perform the following steps to complete this procedure.

Simplex configuration (one server)

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 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 - root
```

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.

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.

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 Distringuished 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.

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.

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 the CS2M software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to procedure "Configuring the SESM server application" in the ATM/IP Solution-level Configuration Management document, NN10409-500.

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.

You have completed this procedure.

High-availability configuration (two servers)

At your workstation

1 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 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 - root
```

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.

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.

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 Distringuished 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.

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.

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 the CS2M software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to procedure “Configuring the SESM server application” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

15 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 345.

16 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.

17 You have completed this procedure.

Erasing the contents of a CD/DVD on a Sun server

Application

Use this procedure to erase the contents of a CD/DVD on a Sun server (Netra 240), when you want to re-use the CD/DVD.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the CD/DVD you want to erase into the drive.

At your workstation

2 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Sun server

3 When prompted, enter your user ID and password.

4 Erase the contents of the CD/DVD by typing

```
$ cdrw -b all
```

and pressing the Enter key

Note: You can also use the “fast” and “session” arguments. For more details, refer to the man pages by typing **`man cdrw`**.

5 Remove the CD/DVD from the drive.

6 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.