

Copyright © 2005, Nortel Networks

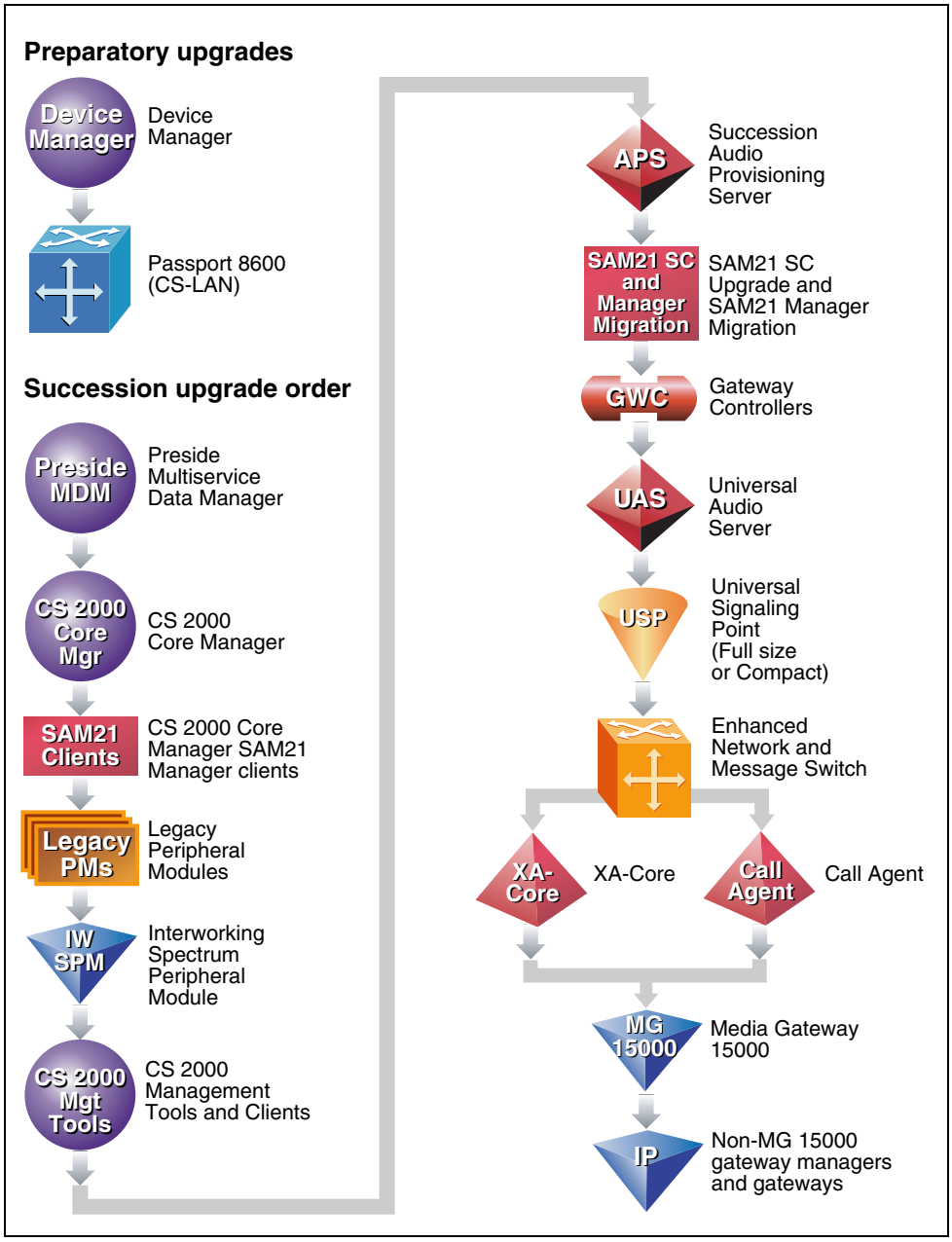

# End-to-end upgrade overview

An end-to-end Succession upgrade involves upgrading all required components in a specific upgrade order.

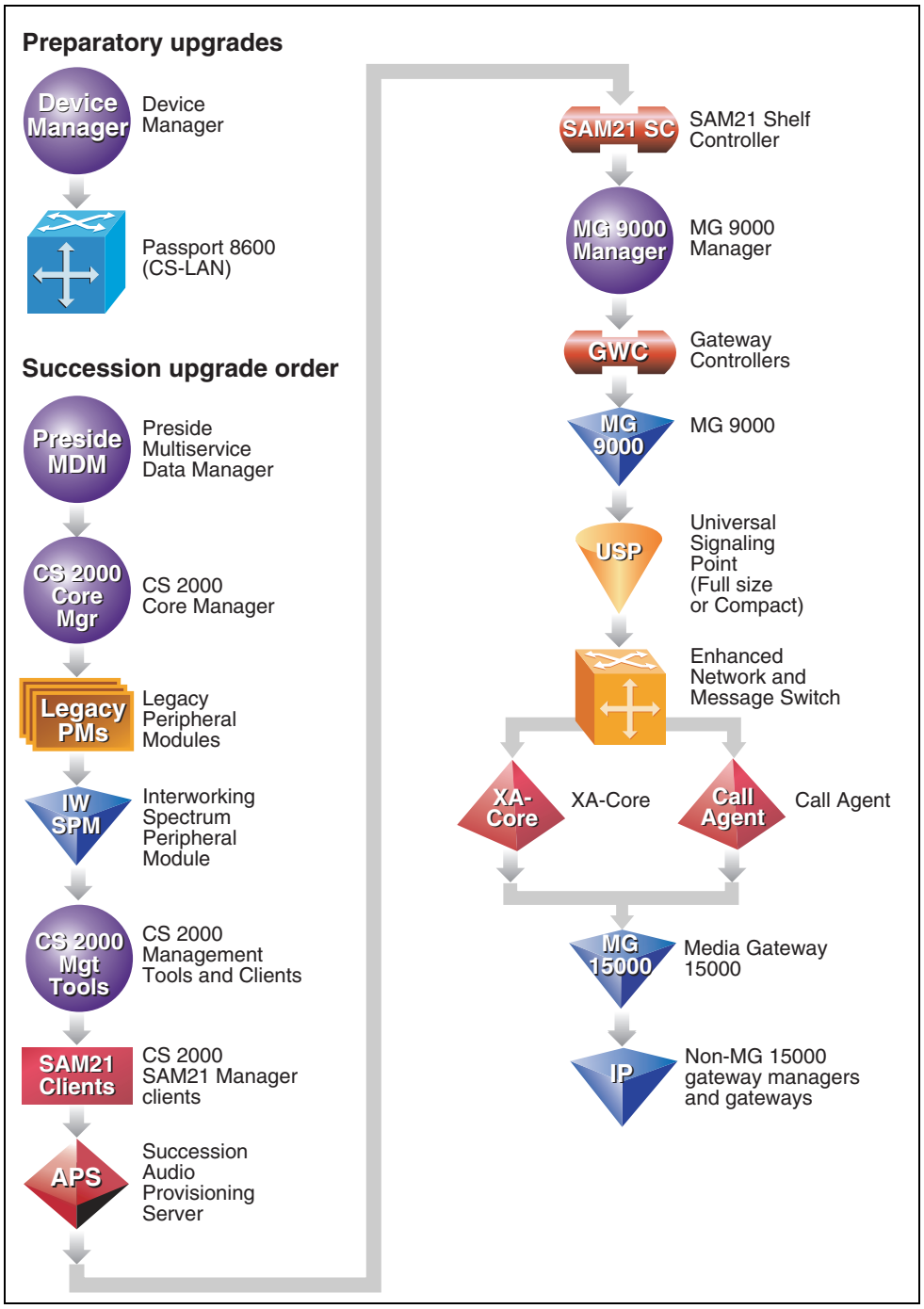
This section provides diagrams showing the upgrade order for each supported upgrade path. Use the corresponding diagram for the appropriate Solution that requires an end-to-end upgrade.

***Note:*** The component icons are hyperlinked. When using this document online, clicking on the graphic for a component links directly to supporting documentation.

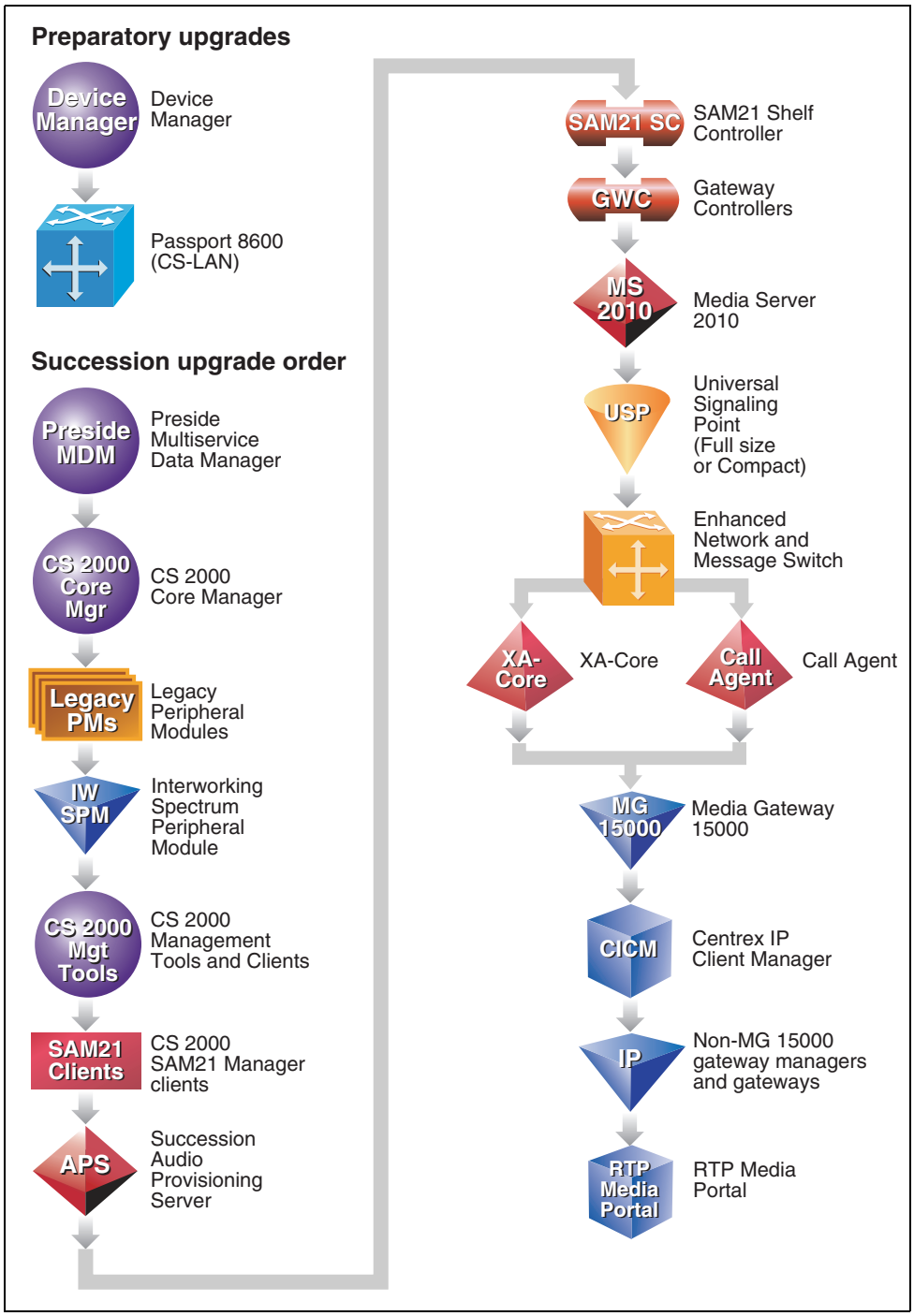
## Figure 1 (I)SN05-to-(I)SN07 IP upgrade order



## Figure 2 (I)SN06-to-(I)SN07 IP upgrade order



## Figure 3 (I)SN06.2-to-(I)SN07 IP upgrade order



# Supported upgrade paths

This section lists supported upgrade paths and information about how to use this document.

The following upgrade paths to (I)SN07 are supported:

- From (I)SN05 to (I)SN07
  - Packet Transit - IP (PT-IP - International)
  - Packet Trunking - IP (PT-IP - North American)
  - Packet Transit - AAL2 (PT-AAL2 - International)
  - Integrated Access - Wireline (IAW)

  ***Note:*** Hybrid configurations of the PT-IP and IAW solutions are also supported.

- From (I)SN06 to (I)SN07
  - Universal Access - IP (UA-IP)
- From (I)SN06.2 to (I)SN07
  - Packet Transit - IP (PT-IP - International)
  - Packet Trunking - IP (PT-IP - North American)
  - Packet Transit - AAL2 (PT-AAL2 - International)
  - Integrated Access - Wireline (IAW)
  - Integrated Access - Cable (IAC)
  - Carrier Hosted Services (CHS)

  ***Note:*** Hybrid configurations of the PT-IP, IAW, and IAC solutions are also supported.

## How to use this document

This NTP is the master document for SN07 solution upgrades. For information about RMRs, refer to Partial network upgrades: SN07-to-SN07 RMRs on page 35.

This document includes details about supported solutions and the required component upgrade order. The upgrade order for each solution is provided in the upgrade flow illustrations in End-to-end upgrade overview on page 1. The detailed upgrade order is provided in

the section Additional information on page 35. This document also includes copies of the basic component upgrade procedures.

***Note:*** Selected component upgrade procedures included in this document are copies of those procedures from the standalone upgrade documents. For detailed rollback and troubleshooting information, refer to the standalone component upgrade NTPs included in the documentation collection for your solution.

When performing an upgrade, complete the three-tiered process of preparation, upgrade, and post upgrade tasks for each individual component (in the order described in (I)SN07 upgrade order on page 8) before beginning the three-tiered process for the next component.

For the list of included upgrade procedures and to navigate between sections, refer to the Adobe Acrobat Bookmarks in the document viewer.

For details about Succession networks and new and changed hardware and software refer to *IP Solutions Basics*, NN10300-100.

***Note:*** This document applies to both North American and International solutions and the prefix “i” in release numbers (for example, “(I)SN07”) means that solutions for both market segments are included.

Statements in this document about upgrades from prior releases assume that all RMRs have been applied unless explicitly stated otherwise.

## Limitations and restrictions

Components outside the scope of this document include:

- Network management layer components such as third-party fault aggregation or service activation systems.
- Transport layer components such as edge and core routers (with the exception of the routers used as part of the central office - LAN) and data service components such as Shasta.
- SS7 network components such as broadband STPs and SCPs
- Third-party offboard systems such as voice mail systems, protocol converters, or test trunk termination systems

This document also does not provide the following:

- Strategy for upgrading the transport components (for example, ATM switches and IP routers that form the data backbone, MUXs for CCS7 backhauling, and so on)
- Strategy for upgrading the Network Management Layer Components such as Third Party Fault Aggregation or Service Activation Systems
- DMS-to-SN07 conversion details

# (I)SN07 upgrade order

This section provides the detailed upgrade order for all IP solutions upgrades to (I)SN07.



**CAUTION**

Before you start an end-to-end upgrade, you must complete Preparing for the upgrade on page 38, which includes upgrading the Passport 8600 (CS-LAN) and JDM.

This book orders the components for each of the following sections: Preparing, Upgrading, and Post Upgrade.

When performing an upgrade, complete the three-tiered process of preparation, upgrade, and post upgrade tasks for each individual component (in the order described in this chapter) before beginning the three-tiered process for the next component.

**ATTENTION**

This section provides the upgrade order for IP solutions. Please disregard components not used in your solution.



**CAUTION**

The upgrade times listed in the following table are estimated. Times will vary depending on your provisioning requirements and do not include time required for pre-upgrade patching.

## Detailed upgrade order

| **Preside MDM** | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| **ATTENTION**<br>*Upgrades from (I)SN05*<br>If you are upgrading from (I)SN05, Preside MDM must be upgraded to (I)SN06.2 before you upgrade to (I)SN07. Refer to *Preside MDM in Succession Networks Upgrade Guide (PT-IP)*, NN10366-461 in your (I)SN06.2 Helmsman collection. | | |
| **(I)SN05 to (I)SN06.2** | | |
| PT-IP<br>PT-AAL2<br>IAW | Up to 1 hour, including<br>• 5 - 10 minutes for prechecks<br>• 30 minutes to install software<br>• 5 minutes for reboot<br>• 10 minutes to activate new features<br>• 5 minutes for post-checks | *Preside MDM in Succession Networks Upgrade Guide (PT-IP)*, NN10366-461 |

## Detailed upgrade order

**Preside MDM (continued)**

| Applicable Solutions | Estimated times | Documentation |
|---|---|---|
| **(I)SN06 and (I)SN06.2 to (I)SN07** | | |
| All solutions | Up to 2 hours total, including<br>• 5 - 10 minutes for prechecks<br>• up to 1 hour to upgrade to the common Voice over IP baseline<br>• 30 minutes to install software<br>• 5 minutes for reboot<br>• 10 minutes to activate new features<br>• 5 minutes for post-checks | For the basic upgrade to (I)SN07, refer to<br>• Preparing to upgrade Preside MDM in Succession SN07 on page 135<br>• Upgrading Preside MDM on page 489<br>For rollback and other upgrade details about upgrading to (I)SN07, refer to *Preside MDM Installation*, 241-6001-100 and *Upgrading Preside MDM in Succession Networks*, NN10185-461 |
| **Service impacts**<br>If the recommended redundant configuration is used, the alternate system provides management of MSS 15000 and MG 15000 nodes, in which case there is no OAM&P impact. | | |
| **Comments**<br>Manager for Multiservice Switch 15000 and Media Gateway 15000. | | |

| CS 2000 Core Manager | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
|  | **CAUTION**<br>If you plan to remove DCE, upgrade the CS 2000 Management Tools server before removing DCE from the CS 2000 Core Manager. For information about removing DCE, refer to *CS 2000 Core Manager Administration and Security*, NN10170-611, included in the Helmsman collection for your solution.<br>**ATTENTION**<br>Once the CS 2000 Core Manager is upgraded, you cannot provision Gateway Controllers (GWC) until the CS 2000 Management (CS2M) software package is installed and configured on the CS 2000 Management Tools server. | |
| All solutions | Enhanced SDM upgrade: 2.5 hr<br>Out-of-Service Mode: 55 min. | For the basic upgrade, refer to<br>• Preparing to upgrade the CS 2000 Core Manager on page 170<br>• Upgrading the CS 2000 Core Manager on page 524<br>• Completing the CS 2000 Core Manager upgrade on page 1393<br>For rollback and other upgrade details refer to *Upgrading the CS 2000 Core Manager*, NN10060-461 |
| **Service impacts**<br>No CallP outage. OAM&P outage depends on the type of upgrade performed.<br>The choice of upgrade type depends on your preference between minimizing outage time or minimizing upgrade time.<br>**Enhanced SDM upgrade service impacts**<br>• During a SWACT the entire system will be out of service for 10 to 12 minutes.<br>• LMM/TMM provisioning will be OOS for up to 20 minutes.<br>• Billing backed up on core during the 10 to 12-minute OOS period. | | |

## CS 2000 Core Manager

**SN05-to-SN07 SAM21 service impacts**

- SAM21 Manager will be unavailable after upgrade of CS 2000 Core Manager and until it has been upgraded on the client.
- No logs will be received from the SAM21 for a few minutes. These logs will still be available on the CS 2000 Core Manager/Shelf controller.
- No management visibility of SAM21 Manager for 55 minutes.

**(I)SN06- or (I)SN06.2-to-(I)SN07 SAM21 service impacts**

- Users of the SAM21 Manager client will not be able to change provisioning on a given card.
- Users of the SAM21 Manager client will not be able to unlock a card and bring it into service.

**Out-of-service upgrade service impacts**

- The entire system will be out of service for 50 minutes.
- LMM/TMM provisioning OOS for up to 60 minutes.
- Billing backed up on the core during the 50-minute OOS period.

**Comments**

For (I)SN05-to-(I)SN07 upgrades, the upgrade of the CS 2000 Core Manager server includes the SAM21 Manager but not the migration of the SAM21 Manager to the CS 2000 Management Tools server, which is done with the SAM21 Shelf Controller upgrade step.

Once the CS 2000 Core Manager is upgraded to CS2E06, users cannot provision Gateway Controllers (GWCs) until the CS 2000 Management Tools software package (CS2M) is installed and configured on the CS2M server.

| CS 2000 Core Manager SAM21 Manager clients (I)SN05 to (I)SN07 only) | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| PT-IP<br>IAW | 10 minutes per client | For the basic upgrade, refer to<br>• Preparing to upgrade the CS 2000 Core Manager on page 170<br>• Upgrading the CS 2000 Core Manager on page 524<br>• Completing the CS 2000 Core Manager upgrade on page 1393<br>For rollback and other upgrade details refer to *Upgrading the CS 2000 Core Manager*, NN10060-461 |
| **Service impacts**<br>CS 2000 SAM21 Manager will be unavailable after upgrade of CS 2000 Core Manager until it has been upgraded on the client.<br>No logs will be received from the SAM21 for a few minutes. These logs will still be available on the CS 2000 Core Manager/Shelf controller.<br>No management visibility of CS 2000 SAM21 Manager for 5 minutes. | | |
| **Comments**<br>During this step you should also upgrade any other CS 2000 Core Manager application clients. Refer to Upgrading the CS 2000 Core Manager on page 524. | | |

| Legacy Peripheral Modules | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| All solutions | Refer to peripheral module documentation. | Refer to the *Peripheral Module Release Document*, 297-9051-599 (intl) or 297-2663-599 (NA) in your SN07 Helmsman DMS collection |
| **Service impacts**<br>Refer to peripheral module documentation. | | |
| **Comments**<br>Includes LCM/XPM/SPM, and LPP/FLPP. | | |

| IW-SPM (IP) | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| All solutions | 1 hour for concurrent upgrade of 1 to 8 IW SPMs | For the basic upgrade, refer to<br>• Preparing to upgrade the IW SPM IP on page 209<br>• Upgrading an IW-SPM IP on page 645<br>For downgrade and other upgrade details refer to *Upgrading the IW-SPM (IP)*, NN10056-461<br>***Note:*** If using the PANTHER tool, the IW SPM IP upgrade may occur in the Legacy Peripheral Modules step. |
| **Service impacts**<br>The inactive/spare card that is being upgraded is out of service for up to 15 minutes per card.<br>No loss of CallP, Billing or Customer visibility to the switch as the traffic is loadshared with redundant components. | | |

| CS 2000 Management Tools and clients | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
|  | **CAUTION**<br>During the upgrade of SSPFS, all logs and alarms are lost, but alarm statuses are resynchronized after the upgrade to ensure accurate status. | |
| All solutions | **SSPFS**<br>**Sun Fire N240 cluster upgrade from (I)SN06.2**:<br>2 hours 33 minutes in total<br>• Disk 1: 62 minutes<br>• Disk 2: 41 minutes<br>**Sun Fire N240 simplex upgrade from (I)SN06**:<br>2 hours 54 minutes in total<br>• Disk 1: 77 minutes<br>• Disk 2: 97 minutes<br>• Cloning time: 45-50 minutes<br>**t1400 simplex upgrade from (I)SN05**:<br>5 hours 1 minute in total<br>• Disk 1: 173 minutes<br>• Disk 2: 128 minutes<br>*Clients*: 10 minutes | Refer to<br>• Preparing to upgrade the CS 2000 Management Tools software on page 240<br>• Upgrading the CS 2000 Management Tools software on page 678<br>• Completing the CS 2000 Management Tools upgrade on page 1549<br>• Downgrading the CS 2000 Management Tools software on page 1842<br>**Note**: For SN05 to SN07 upgrades, upgrading the CS 2000 Management Tools sends the operator to the SAM21 Shelf Controller upgrade at various points in the procedure and then expects the user to return to the CS 2000 Management Tools documented process. |

| CS 2000 Management Tools and clients |
|---|
| **Service impacts**<br>The processor being upgraded is out of service during the upgrade.<br>No loss of CallP and Billing. However, there will be no management visibility of the CS 2000 management tools for up to two hours. |
| **Comments**<br>Includes CS 2000 GWC Manager, LMM, TMM, and SAM21 clients.<br>APS and CS2M upgrades include upgrade of SSPFS.<br>SSPFS supports both t1400 and N240.<br>*Standalone APS servers*<br>In (I)SN07, the use of separate t1400 servers for CS 2000 Management Tools and APS are not supported. If you do have this configuration refer to Combined server upgrade on page 304. |

| APS | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| All IP solutions except CHS | 1 hour | Refer to<br>• Upgrading APS software on page 725<br>• Upgrading the CS 2000 Management Tools software on page 678<br>• Downgrading the CS 2000 Management Tools software on page 1842 |
| **Service impacts**<br>The APS being upgraded is out of service until the upgrade is completed. | | |
| **ATTENTION**<br>Your network must not have separate t1400s for CS2M and for APS. If you do have this configuration contact your Nortel representative for further instructions. | | |
| **Comments**<br>APS upgrade includes upgrade of SSPFS. | | |

| SAM21 Shelf Controller | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| All solutions | 10 minutes for SAM21 Manager<br>25 minutes for SAM21 Shelf Controller | Refer to<br>• Installing SAM21 Platform software on page 744<br>• Migrating the SAM21 network elements to the CS 2000 SAM21 Manager on the CS 2000 Management Tools server on page 762<br>• Upgrading the CS 2000 Management Tools software on page 678 |
| **Service impacts**<br>None | | |
| **ATTENTION**<br>Make sure all ATM connections are established before performing the upgrade SWACT.<br>**Comments**<br>For upgrades from (I)SN05, this step includes the CS 2000 SAM21 Manager migration. | | |

| MG 9000 Manager (UA-IP only) | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| UA-IP | 1 hour for an MG 9000 Manager supporting 4 MG 9000s with 16,000 lines | For the basic upgrade, refer to<br>• Preparing to upgrade the MG 9000 on page 318<br>• Upgrading MG 9000 components on page 776<br>For rollback and other upgrade details refer to *Upgrading the MG 9000*, NN10048-461 |
| **Service impacts**<br>Downtime of MG 9000 Manager during platform upgrade of server (loading new version of SSPFS).<br>No loss of CallP or Billing for MG 9000.<br>***Note:*** Refer to *Upgrading the MG 9000*, NN10048-461 for detailed service impacts and estimated upgrade times. | | |
|  | **CAUTION**<br>To prevent potential data corruption or loss, provisioning of Virtual Media Gateways (VMGs) terminations, switched line services, private line services, DSL, and so on is not permitted during the end-to-end upgrade. | |
|  | **CAUTION**<br>During the upgrade of SSPFS, all logs and alarms are lost, but alarm statuses are resynchronized after the upgrade to ensure accurate status.<br>Buffered security and audit logs are lost during the MG 9000 Manager upgrade, but alarms are sent directly to the OSS and are not lost. | |

| GWCs | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| All solutions | 24 minutes for each GWC node (card pair) for the GWC software. Under a moderately loaded 10BaseT network, the load takes about 2 minutes to transfer. Transfer time can increase over a heavily loaded network. | For the basic upgrade, refer to<br>• Preparing to upgrade the Gateway Controller on page 344<br>• Upgrading the Gateway Controller on page 834<br>For rollback and other upgrade details refer to *Upgrading the Gateway Controller*, NN10196-461 |
| **Service impacts**<br>Stable two-port calls survive GWC SWACT. Calls in setup mode during SWACT are dropped. | | |

## GWCs

Differing GWC types are upgraded in the following order:

**Non-AAL1 GWC upgrade order**

- AC
- VRDN
- SIP-T/APG/RA
- APG/RA
- SIP-T/APG
- APG
- SIP-T
- Trunks
- H.323 (also controls RTP Media Portal)
- V5.2 trunks
- Lines (includes CICM and large- and small-line GWCs)

***Note 1:*** If your solution includes the Session Server, details are available from the following sources:

- *Session Server Basics*, NN1333-111
- The Session Server installation methods document
- RMRs provided by Nortel Networks customer support

***Note 2:*** If you have a series of calls servers serviced by one Session Server, the minimum release for all the supported call servers must be (I)SN06. Session Server is not backwards compatible to (I)SN05 CS 2000 systems.

| GWCs |
|---|
| **Comments**<br>Offices will only have one GWC pair with RA, therefore an office will either have only one APG/RA or only one SIP-T/APG/RA but not one of each.<br>It is not necessary to have one or more SIP-T/APG GWCs in the office, but it is possible depending on numbers of endpoints required in the office. An office with APG and SIP-T might only have APG/RA and SIP-T or only have APG/RA and SIP-T and APG.<br>Parallel upgrades of CS 2000 GWCs are not supported.<br>***Note:*** The CS 2000 Management Tools software generates new middlebox IDs for the following items that have already been provisioned:<br>• network address translators (NATs)<br>• policy enforcement point (PEP) servers<br>For details, refer to CS 2000 call agent identifier required in SN07 on page 351. |

| Media Server 2010 | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| PT-IP<br>UA-IP<br>IAC<br>CICM | *Software upgrade*: 2 minutes<br>*Download of audio announcements (if applicable)*: up to 5 minutes | Upgrading a Media Server 2010 on page 893<br>For full upgrade details, refer to *Upgrading the Media Server 2010*, NN10335-461 |
| **Service impacts**<br>None if you have the recommended n+1 configuration, where “n” represents the base number of servers recommended in the engineering guidelines for your solution and “n+1” represents the recommended redundancy. | | |

| MG 9000 (UA-IP only) | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| UA-IP | 1 to 3 hours depending on the size of the MG 9000 | For the basic upgrade, refer to<br>• Preparing to upgrade the MG 9000 on page 318<br>• Upgrading MG 9000 components on page 776<br>For rollback and other upgrade details refer to *Upgrading the MG 9000*, NN10048-461 |

**Service impacts**

For (I)SN07 upgrades, the MG 9000 upgrade consists of upgrading a series of cards.

Each card is running in duplex mode. During the upgrade, the system runs in simplex mode on one or more of these cards.

SWACTs will occur to switch to the new loads, preventing loss of service.

Provisioning is not supported during upgrade of the MG 9000.

***Note:*** Refer to *Upgrading the MG 9000*, NN10048-461 for detailed service impacts and estimated upgrade times.

| UAS | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| PT-IP IAW | 1 hour to 1.5 hours | For the basic upgrade to (I)SN06.2, refer to Upgrading the UAS on page 930.<br>For rollback and other upgrade details, refer to *Upgrading the UAS*, NN10047-461. |
| **Service impacts**<br>The UAS component being upgraded is out of service for 1 hour.<br>No loss of CallP, billing or customer visibility to the switch as the traffic is loadshared with redundant components. | | |

| USP or USP compact (if present) | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| IAC<br>IAW<br>PT-AAL2<br>PT-IP<br>UA-IP | **USP**<br>3 hours for a 1-shelf system<br>6 hours for a 2-shelf system<br>**USP compact**<br>1 hour<br><br>***Note:*** Total upgrade time is estimated for both USP and USPc, based on the above, and excluding the next-day activity to remove the upgrade package. Removal of upgrade supporting files, loads and directories takes about 30 minutes. | For the basic upgrade, refer to<br>• Preparing to upgrade the USP on page 362<br>• Upgrading the USP on page 1012<br>• Upgrading the USP Compact on page 1101<br>For USP rollback and other upgrade details refer to *Upgrading the USP*, NN10045-461<br>For USPc rollback and other upgrade details refer to *Upgrading the USP Compact*, NN10046-461 |
| **Service impacts**<br>The USP and USPc upgrade is in-service. Traffic is maintained for systems with redundant links configured on different links cards. Every time a blade is taken out of service, a loss of network redundancy occurs. | | |
| **Comments**<br>Nortel Networks recommends that you upgrade the USP in the following order:<br>• Upgrade the USP PC GUI to (I)SN07.<br>• Upgrade the USP using the USP PC GUI.<br>• Make sure that the USP is stable.<br>• Install the USP JAVA GUI on the SSPFS.<br>• Migrate the alternate boot server (ABS) from the PC to the SSPFS.<br>• Disable ABS on the PC.<br>The USP requires a software upgrade from USP 7.0 to USP8.0 then to USP9.0. All (I)SN05 to (I)SN07 upgrades require that the USP be upgraded in two steps. USP07 to USP08 followed by USP08 to USP09.<br>USPc did not have an (I)SN06 (USP08) release, so (I)SN05-to-(I)SN07 and (I)SN06-to-(I)SN07 upgrades for offices with USPc upgrade directly from USP07 to USP09. | | |

| Enhanced Network and Message Switch | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| IAC<br>IAW<br>PT-AAL2<br>PT-IP<br>UA-IP | Refer to TDM standards | *DMS Peripheral Module Software Release Document*, 297-9051-599 (intl) or 297-2663-599 (NA) in your (I)SN07 Helmsman DMS collection |
| **Service impacts**<br>Refer to TDM standards | | |

| CS 2000 Core | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| **XA-Core** | | |
| All solutions | CS 2000 Core: 4 hours<br><br>IOP to HIOP: 10 minutes | *XA-Core Maintenance Manual* (297-8991-510), in your (I)SN07 Helmsman DMS collection<br><br>*Global Software Delivery One Night Process Software Delivery Procedures*, 297-8991-303, in your (I)SN07 Helmsman DMS collection<br><br>*DMS Peripheral Module Software Release Document*, 297-9051-599 (intl) or 297-2663-599 (NA) in your SN07 Helmsman DMS collection |
| **Service impacts**<br>Stable (answered) 2-port calls are unaffected, but new calls cannot be established during restart SWACT. It should be possible to originate calls within one or two minutes after a NoRestartSwact. | | |

## CS 2000 Core

**Comments**

The Atlas PE is supported in (I)SN07.

XA-Core (I)SN05 offices with 3+1 Rhino configurations may upgrade to Atlas before or after the (I)SN05 to (I)SN07 upgrade. Upgrading Rhino to Atlas during an (I)SN05-to-(I)SN07 upgrade is NOT supported.

Any 2+1 Rhino configuration must be upgraded to 3+1 Rhino prior to the upgrade to (I)SN07.

Rhino-to-Atlas network upgrades for networks using Succession IOPs are not supported. An IOP-to-HIOP upgrade must be completed prior to performing a Rhino-to-Atlas upgrade. Refer to IOP/HIOP upgrade instructions.

***Note:*** For all upgrades to (I)SN07, new customer-specific parameters related to the solution fabric are required. The parameters are normally provided to customers via bulletin in the FEATDATA file. Contact Nortel Networks technical support if you require more information.

## CS 2000 Compact

| Applicable Solutions | Estimated times | Documentation |
|---|---|---|

**ATTENTION**

The CS 2000 Compact must first be upgraded to (I)SN06.2 before you upgrade to (I)SN07. Refer to *Upgrading the Call Agent*, NN10065-461 in your (I)SN06.2 Helmsman collection.

| | | |
|---|---|---|
| All solutions except CHS | CS 2000 Compact: Platform and PCL upgrade (ONP): 1.5 hours (+ additional customer test acceptance time, if required). | For the basic upgrade, refer to<br>• Preparing to upgrade CS 2000 Compact on page 367<br>• Upgrading the CS 2000 Compact on page 1123<br>For rollback and other upgrade details refer to *Upgrading the Call Agent*, NN10065-461 |

**Service impacts**

Stable (answered) 2-port calls are unaffected, but new calls cannot be established during restart SWACT. It should be possible to originate calls within one or two minutes after a NoRestartSwact.

**Comments**

CS 2000 Compact includes 3PC and PCL.

## Multiservice Switch 15000

| Applicable Solutions | Estimated times | Documentation |
|---|---|---|
| **ATTENTION**<br>Direct upgrade from SN05 to SN07 is not supported for Nortel Networks Multiservice Switch/Media Gateway 7480/15000/20000 nodes. Upgrade to SN06.2 first and then upgrade from SN06.2 to SN07. Refer to NTP 241- 5701- 272 Passport 7400, 15000, 20000 Software Upgrade in the SN06.2 Helmsman collection for the upgrade to SN06.2 and then return to this document to complete the upgrade to SN07. | | |
| MG 15000: All solutions<br>MG 15000 and MSS 15000 combo: UA-IP only | **In-service MG 15000 5.2 upgrade**<br>20 minutes to 3.5 hours, depending on the number of calls and components that have been provisioned on the MG 15000<br><br>**PLUS** time required to do deferred link blocking on all links on the MG 15000 (20 seconds to several minutes per link, depending on the number and duration of calls on the links)<br><br>**PLUS** time required to rts all links (20 seconds per link)<br><br>**Out-of-service MG 15000 upgrade**<br>20 minutes to 3.5 hours, depending on the number of calls and components that have been provisioned on the MG 15000 | For the basic upgrade, refer to<br>• Preparing to upgrade the Multiservice Switch 15000/Media Gateway 15000/20000 in Succession IP Solutions on page 428<br>• Upgrading Multiservice Switch 15000/Media Gateway 15000 in Succession Networks (UA-IP) on page 1231<br>For rollbacks and other upgrade details refer to *Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP)*, NN10419-461 |

| Multiservice Switch 15000 | |
|---|---|
| | **PLUS** time required to deactivate all V5 interfaces on the MG 15000 (1 minute per interface)<br><br>**PLUS** time required to active all V5 interfaces on the MG 15000 (1 to 30 minutes per interface depending on the number of lines, and whether APA is used or not) |

**Service impacts**

All established calls will be lost once the upgrade is initiated as 4pGigE FP is not carrier grade enabled in (I)SN06.2.

Service interruptions (for new calls) during the upgrade will vary depending on whether VRAP capabilities are enabled, however an estimate of 5-7 seconds can be expected as the 4pGigE FP will not be carrier grade enabled until the (I)SN07 time frame. All other cards on the PP 15000 shelf are carrier grade enabled so the service interruption time is reflective of only the 4pGigE card.

Starting in PCR 5.1, MG 15000 has limited HSM/EP capability. PCR 5.1 ASPEN with 4-port OC3 upgrading to PCR 6.1 supports HSM.

HSM is not supported during rollbacks.

**VoIP networks**

Change from ASPEN to H.248 is also supported after the upgrade to PCR 6.1. The H.248 control of MG 15000 is enabled by provisioning and is not automatically enabled by migration. Therefore, a MG 15000 configured for VGCP (ASPEN) will continue to use ASPEN after upgrading to H.248.

When upgrading from an ASPEN-controlled network, MG 15000 can have its software upgraded to PCR 6.1 and then have H.248 enabled on a node-by-node basis.

**VoAAL2 networks**

When upgrading from an ASPEN-controlled network, to ensure SDP interoperability all MG 15000s must be upgraded to a minimum level of PCR 5.1 before enabling H.248 with RFC 3108 SDP on any MG 15000. When configured for H.248, MG 15000 will send SDP with a slightly different format and ASPEN MG 15000s must be at PCR5.1 to accept this new format. Therefore, until all MG 15000s in the network are at PCR 5.1 or higher, H.248 AAL2 MG 15000s must be configured to send non-RFC3108 SDP using the attribute **sdpFormat**, under the **Nsta/x Vgs H248/y** component.

## Multiservice Switch 15000

**Comments**

The following MG 15000 upgrade scenarios are supported:

- PCR 5.1 to PCR 6.1 (UA-IP only)
- PCR 5.2 to PCR 6.1

Refer to OAM guidelines on page 41 and *Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP)*, NN10419-461

## Centrex IP Client Manager (CICM)

| Applicable Solutions | Estimated times | Documentation |
|---|---|---|
| CHS | Sequence 1 - Split CICM: 35 minutes<br>Sequence 2 - New CICM RTS: 20 minutes<br>Sequence 3 - Transferring Control: 55 minutes | For the basic upgrade, refer to<br>• Preparing to upgrade CICM on page 466<br>• Upgrading CICM on page 1314<br>For rollback and other upgrade details, refer to *Upgrading CICM*, NN10230-461 and IM-65-0580. |

**Service Impacts**

*Creating a new network identity for CICM-101-B (datafill GWC / CS2M)*

Terminal connectivity is enabled but no Call Processing will be available on either node for 10 minutes.

*Terminal handovers*

Calls are dropped on the originating node on expiration of the shutdown timeout. Capacity is reduced for 10-15 minutes.

**Comments**

The (I)SN06.2 CICM release is only supported on a 5370 card mounted on a SAM16 chassis.

For new installations, the (I)SN07 CICM release is supported on a 5385 card mounted on a SAM21 chassis. For upgrades, the (I)SN07 CICM release is supported on a 5370 card mounted on a SAM16 chassis.

| Non-MG 15000 gateway managers and gateways | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| IAC<br>IAW | For estimated upgrade times, refer to OEM/third-party media gateway upgrade documentation | Refer to OEM/third-party media gateway upgrade documentation |
| **Service impacts**<br>Refer to the appropriate component upgrade documentation. | | |
| **Comments**<br>Either CS 2000 or MCS can upgrade independently. However, MCS must be upgraded prior to the CS 2000.<br><br>First, upgrade the gateway manager for one type of gateway, and then upgrade all the gateways of that type. Then upgrade the gateway manager for gateways of the second type and then upgrade all gateways of the second type.<br>For each gateway type, perform the upgrade on the gateway manager followed by the upgrade for the gateways of that type and then go on to the next gateway type. | | |

| RTP Media Portal | | |
|---|---|---|
| **Applicable Solutions** | **Estimated times** | **Documentation** |
| IAW<br>CHS | 7 hours 15 minutes<br><br>***Note:*** The following MCS components upgrade to (I)SN07 (from MCS 2.0 to MCS 3.0) during this step:<br>• RTP Media Portal<br>• Database Module<br>• System Management Console | For the basic upgrade, refer to<br>• Upgrading the MCS Management Server on page 1338<br>• Full release upgrades on page 1364<br>For rollback and other upgrade details, refer to<br>• *Upgrading the CS 2000 T1400/T1405 Servers*, NN10414-461<br>• *RTP Media Portal Basics*, NN10367-111<br><br>***Note:*** Hardware upgrades from SUN Fire t1400 to SUN Netra 240 can only be done after the network is at (I)SN07 and MCS 3.0. The hardware upgrade is documented separately.<br>Refer to *RTP Media Portal Element Manager Hardware Upgrade (Sun T1400 to Sun N240)*, SSIP 0430 |
|  | **Service Impacts**<br>**CAUTION**<br>Upgrading all RTP Media Portals concurrently will cause a service outage.<br>It is possible to update and reboot one RTP Media Portal in a chassis, while the RTP Media Portal in the other half of the chassis continues to run the previous software.<br>Once one RTP Media Portal is updated, the other RTP Media Portal in the chassis can be shutdown, locked, updated, and rebooted. This rolling upgrade will only impact available capacity and will not cause a service outage. | |

## RTP Media Portal



**CAUTION**

The CS 2000 may try to contact the RTP Media Portal while the update is in progress, potentially generating error logs.

To minimize impact to service, the RTP Media Portal should first be SHUTDOWN so that it does not accept new service requests. While shutting down, the RTP Media Portal continues to process established media sessions.

These pre-existing media sessions are cleared as the associated calls end. The RTP Media Portal automatically transitions into the LOCKED state when there are no active media sessions present. When this occurs, it is safe to proceed with the upgrade without affecting service.

**Comments**

The RTP Media Portal upgrade can be done at any time after the GWC upgrade.

***Note:*** Software upgrades are separate from hardware upgrades from t1400 to n240 servers. The network software must be upgraded MCS 3.0 or (I)SN07 before a hardware upgrade from t1400 to Sun Fire n240 servers can be done. Hardware upgrades (also referred to as conversions) are documented in installation methods.

# SN07-to-SN07 RMR upgrade order



**CAUTION**

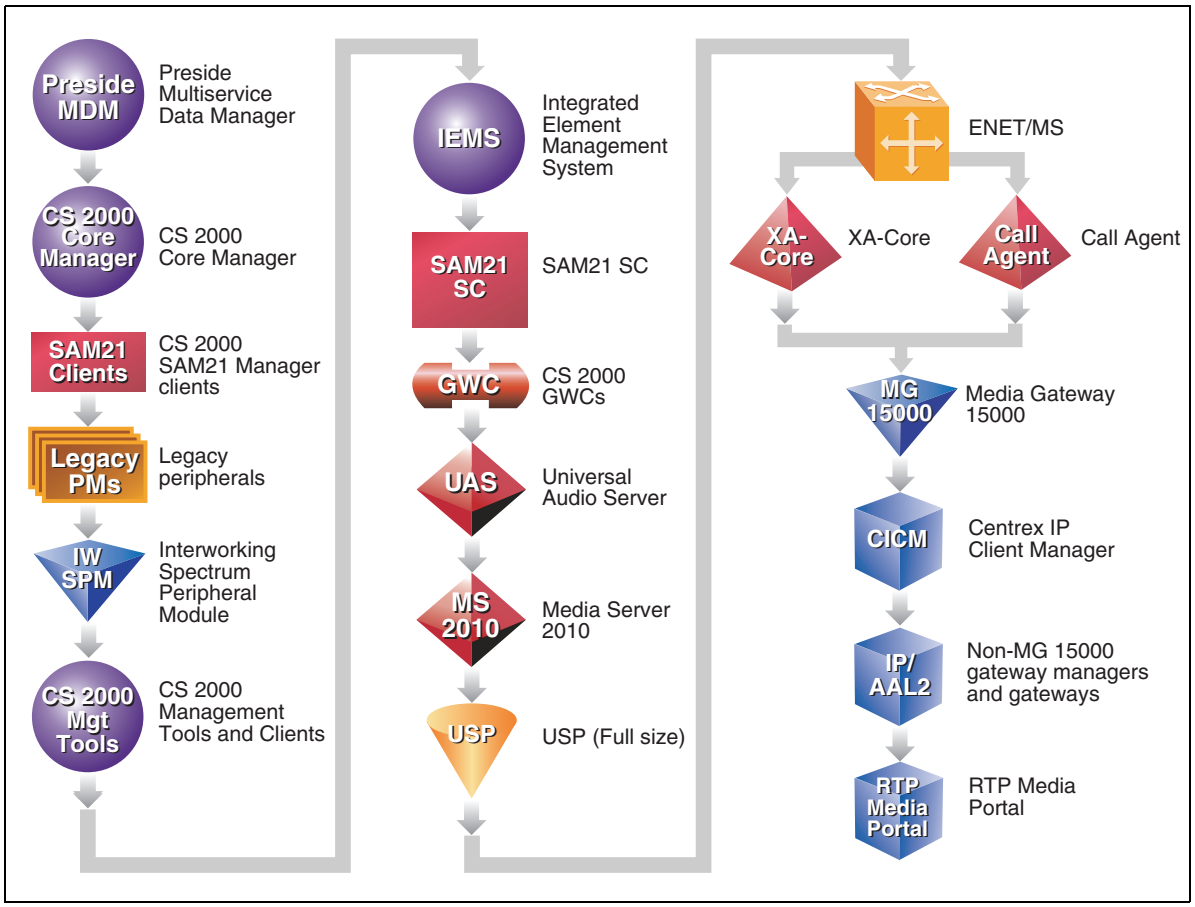
The documentation provided with any regular maintenance release (RMR) release supersedes this section. For information about obtaining RMRs, refer to Prerequisites on page 39.

Individual components must be individually upgradeable or reloadable from SN07 to SN07 without affecting the rest of the components.

The upgrade or reload of any component is supported.

When multiple components must be upgraded in a RMR, use the upgrade order shown in (I)SN07-to-(I)SN07 IP RMR upgrade order on page 34 unless the RMR documentation supersedes this order.

**Figure 1 (I)SN07-to-(I)SN07 IP RMR upgrade order**



# Additional information

Any conversions or installations of new Succession components introduced in SN07 cannot be performed until after the solution has been upgraded to SN07.

For more information about upgrade order, estimated time lines, documentation, and service impacts for upgrades to SN07, refer to (I)SN07 upgrade order on page 8.

## Partial network upgrades: SN07-to-SN07 RMRs

An SN07-to-SN07 upgrade may be necessary to introduce a maintenance release or major upgrade. These upgrades are referred to as regular maintenance release (RMR) upgrades. SN07 RMRs support upgrade or reload of individual components without affecting the rest of the components. For information about obtaining RMRs, refer to Prerequisites on page 39.

RMRs typically consist of an upgrade to network components with a software maintenance release. In this document, the term “network components” refers to one of the components, such as Preside MDM, that make up a given solution.

When performing an RMR upgrade you must follow the solution upgrade order outlined in the SN07-to-SN07 RMR upgrade order on page 33 unless explicitly stated otherwise in the RMR documentation. If there are network components whose release software does not require an upgrade in the RMR, then omit these network components but maintain the solution upgrade order found in the detailed upgrade order. All network components with new software in the RMR must be upgraded. Failure to upgrade network components with new RMR loads results in unsupported load line-ups. The only supported load line-ups are those defined in the RMR load line-up documents. This means that even if the only software fix required by a particular Succession network is solely within the Preside MDM for example, all network components with new loads in that RMR must be upgraded.

Installing RMR upgrades consecutively however, is not required. For example, if a site is running load line-up RMR1, the site can upgrade to RMR3 without first upgrading to RMR2. You can upgrade from a given RMR to any later RMR within the same major release.

Although SN07-to-SN07 RMR upgrades are in-service upgrades, some components require additional hardware or special procedures for in-service upgrades.

## Patching



**CAUTION**

Do not activate any activatable patches until instructed to do so in the upgrade documentation.

For other details about patching, refer to *Patch Currency* and *Succession Patching* in this document.

Also refer to the following documents:

Patching for the CS 2000 Core

- *Post Release Software Manager (PRSM)*, 297-8991-540
- *Post Release Software Manager (PRSM) Reference Manual*, 297-8991-542

Patching for the CS 2000 Compact

- *Upgrading the Call Agent*, NN10065-461

## Service impacts affecting components

Service impacts for components are listed in (I)SN07 upgrade order on page 8 and the component upgrades sections of this document.

## Abort strategy



**CAUTION**

Abort procedures are excluded from this document. In the event that an abort is required, refer to the full component upgrade procedures included in your Helmsman collection.

During the end-to-end upgrade timeline, there are several pre-defined abort points. First, the upgrade can be aborted between any of the component upgrades. Second, each component has defined specific abort points, where the load can be taken back down to the older version.

Abort procedures are excluded from this document. In the event that an abort is required, refer to the full component upgrade procedures included in your Helmsman collection.



**CAUTION**

If a component upgrade must be aborted and the software rolled back to the previous load, the component upgrade should be repeated as soon as possible to minimize the window during which the Succession solution is running an unofficial load line-up.



**CAUTION**

The SSPFS upgrade process does not have rollback capability. Prior versions of the operating system files and third-party common services will be erased. As noted in Preparing for the upgrade on page 38, you must back up your system before performing the SSPFS upgrade process.



Copyright © 2005, Nortel Networks 

# Preparing for the upgrade

Your organization's upgrades planners must determine which solution type must be upgraded. If in doubt, refer to your organization's account manager for clarification.

Perform the upgrade pre-checks listed in this section before starting the end-to-end upgrade. Nortel Networks recommends that these pre-checks be performed as soon as an upgrade is scheduled. Refer to the following for details:

- Prerequisites on page 39
  - Required pre-upgrade procedures on page 39
- *Software Delivery, Planning and Provisioning Guide, NN10500-190*
- the component-level upgrade procedures included in this document

***Note:*** Normal service activation is supported during upgrades windows providing that no hardware changes are made at the same time.

## Prerequisites



**CAUTION**

Do not activate any patches until instructed to do so in the upgrade documentation.



**CAUTION**

Security certificates are required for all SSPFS based servers in SN07. All security certificates must be available prior to starting the upgrade to SN07.

Ensure that the following procedures and upgrades are completed prior to upgrading your network to SN07.

**Table 1 Required pre-upgrade procedures**

| Requirement | Applicable Solutions | Documentation |
|---|---|---|
| **1. Obtain and read any applicable technical bulletins** | All | Technical bulletins provided by customer support are available from the Nortel Networks web site as follows:<br>1. Go to nortelnetworks.com and select **Technical Documentation**.<br>2. Under Other Resources, select **Search for Technical Bulletins**.<br>3. Enter your search criteria (for example, “RMRs”) and click **Search**.<br>***Note:*** Customers are urged to register to receive technical documentation updates and news at the Support site. |
| **2. Ensure that the latest RMRs are installed** | All | For information about finding technical bulletins for RMRs, refer to the previous step. |

**Table 1 Required pre-upgrade procedures**

| Requirement | Applicable Solutions | Documentation |
|---|---|---|
| **3. Complete the Device Manager for Passport 8600 upgrade** | All | Java Device Manager for Passport 8600, later in this document |
| **4. Complete the Passport 8600 (CS-LAN) upgrade** | All | Passport 8600 Software Upgrade/ Rollback (CS-LAN), later in this document |
| **5. Ensure all components are patch current** | All | Refer to Succession patching on page 1636.<br><br>***Note:*** Use the Regional Patch Selector (RPS) tool from nortelnetworks.com to determine which patches you require. Refer to Ensuring patch currency on page 484 |
| **6. Ensure all patches for SN07 are available** | All | Refer to Succession patching on page 1636.<br><br>***Note:*** Use the Pre-Upgrade Patch Calculator and Patch Audit tool from nortelnetworks.com to determine which patches you require. Refer to Ensuring patch currency on page 484 |
| **7. Complete all upgrade software delivery, planning and provisioning requirements** | All | *Software Delivery, Planning and Provisioning Guide, NN10500-190* |
| **9. Verify your lab or network against the hardware baseline for a release** | All | Hardware baselines are covered in the solution specifications. Contact customer service for a copy of *Voice over IP Solution Specification*. |
| **10. Disable the Network Patch Manager patch autoapply function** | All | Disable the patch autoapply function for the duration of the office upgrade. This activity entails disabling the execution of the SYSTEMPLAN, which includes the AUTOAPPLY task.<br><br>Refer to Modifying a plan using the NPM on page 1759 |

**Table 1 Required pre-upgrade procedures**

| Requirement | Applicable Solutions | Documentation |
|---|---|---|
| **11. Complete the network and component backups** | All | *Global ATM/IP Administration and Security*, NN10402-600 |
| **12. Return to the upgrade order section of this book** | All | (I)SN07 upgrade order on page 8 |

## OAM guidelines

If your PVG configuration does not support Hitless Software Migration (HSM), use the Post By Gateway feature within TMM to post all the trunks on the PVGs on that shelf and BSY them out. This must be done prior to the PVG upgrade to prevent active calls from being dropped during the upgrade.

This feature allows active calls to complete before the trunk goes BSY, but will not allow new calls to originate on those PVGs on the selected shelf.

UAS and MS 2010 redundancy: There should be N+1 sparing for UAS units for the following reasons:

- UASs are simplex, and therefore a spare must be provided for redundancy. Even though 2 UASs can fit on a SAM16 shelf, spreading them across shelves would provide complete redundancy in case of a shelf problem.
- Upgrade of a UAS unit causes it to go out of service during its upgrade, and active calls are dropped. There should therefore be another UAS unit which can be used during this upgrade.

GWCs in (I)SN05 and (I)SN06: the same AC GWC can be used for conferencing, announcements and LI if capacity permits.

# Device Manager for Passport 8600

This chapter provides information about:

- Device Manager documentation – how to acquire detailed software installation documentation on the Device Manager
- Device Manager software – how to prepare the Device Manager software for the upgrade process, including procedures for Electronic Software Delivery (ESD) and compact disk (CD) software delivery methods

## Device Manager documentation

Refer to document Installing and Using Device Manager, Part No. 316341-B, within this Succession Networks Solution documentation collection for additional information on the Device Manager.

Document Installing and Using Device Manager is also available online from eService Technical Support from the Technical Support link off of the Nortel Networks website:

*http://www.nortelnetworks.com*

## Device Manager software

**ATTENTION**

If upgrading to a current Device Manager software version, remove the existing version before installing the current Device Manager software. Use the software removal utility that your operating system (e.g., Windows, Solaris, HP UNIX, or Linux) supports to remove the existing version of the Device Manager software.

Beginning with SN07, software for the Device Manager is stored in the Nortel Networks Software Vault. The Software Vault is a repository for maintaining and distributing controlled copies of software loads to Nortel customers.

The Software Vault provides the following benefits:

- version control
- access control
- query and persistency capabilities using a distributed multi-client, multi-server architecture
- transaction control

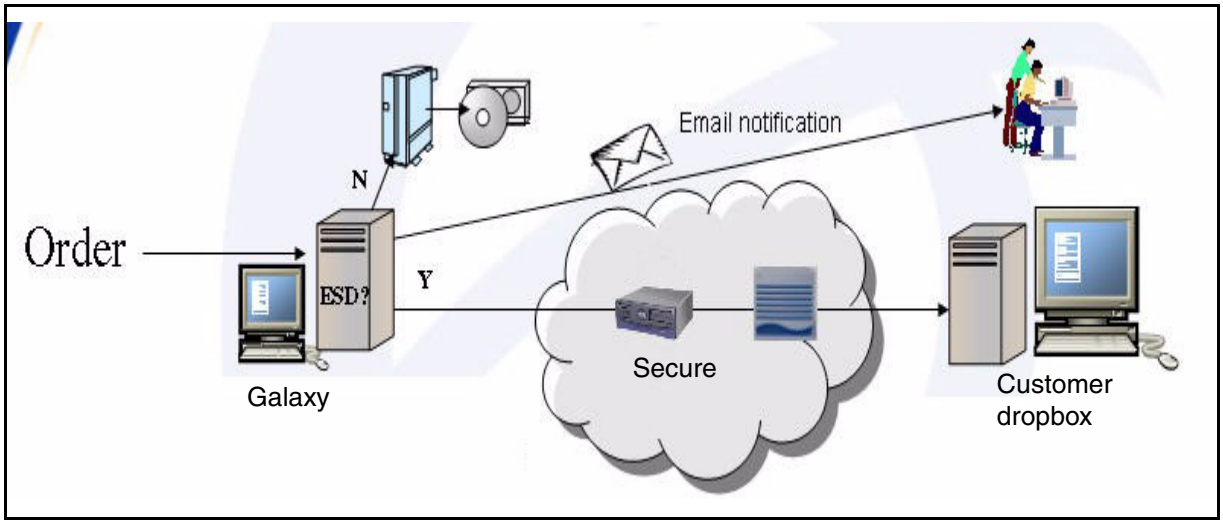
### Software delivery methods

Customers receive the Device Manager software either through ESD or manufactured on physical media, such as a CD, and couriered to their site.

The Galaxy ESD tool accommodates global software delivery using business-to-business processes and automated electronic distribution of Nortel products to customer locations.

The following figure shows a high-level example of how the software is released to the customer site through ESD.

**Figure 1 Software order and ESD delivery overview**




Galaxy compresses the software file into a tar.gz file for delivery. The file adheres to ESD filenaming conventions. The Device Manager software is included as part of the ordering code in the Passport 8600 load for the CS-LAN. An example of the vaulted software load file for the Passport 8600 follows.

**Example**
P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz

**where**

P86S00X0.X refers to the ordering code for the Passport 8600 software for the SN0X release (this value changes for each release)

V refers to the product release (V for VO; R for Released)

NCL refers to the software load type (NCL for non-CM load; MNCL for maintenance non-CM load)

NAP refers to the processor type

VAULT refers to the Nortel software repository source

X refers to the Nortel product repository version (if applicable)

D refers to the software file format reason (Distribution)

tar refers to a tarred file

gz refers to a zipped file

### Preparing the software file for an upgrade

Before starting an upgrade on the Device Manager, perform the following software preparative measures:

- Move the software [load] file(s) to the appropriate directory on the SuperNode Data Manager (SDM)/CS 2000 Core Manager or the Core and Billing Manager (CBM). If retrieving the software from ESD, the software load file is located in the ESD drop box.

  **where:**

  P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz is the software load file

- Unzip and untar the software load file.
- Rename, unzip, and untar the Device Manager file.

  **where:**

  device_mgr_XXXX_tar.gz.tape is the Device Manager file

***Note:*** The final destination for the software file is on a personal computer (PC) where the Device Manager application operates, such as a PC in a network operations center.

The following two procedures show how to prepare the Device Manager software for an upgrade.

Use the first procedure when retrieving the Device Manager software from an ESD delivery.

**Procedure 1 Preparing the ESD version of the Device Manager**

**software for an upgrade**

***At the workstation***

**1** Select the location of the ESD drop box follows:

| If the ESD drop box is | Do |
|---|---|
| not in the /swd directory of the SDM/CS 2000 Core Manager or the CBM | step 2 |
| in the /swd directory of the SDM/CS 2000 Core Manager or the CBM | step 3 |

**2** Use trivial file transfer protocol (TFTP) or file transfer protocol (FTP) to transfer the software load file as a binary file to the /swd directory of the SDM/CS 2000 Core Manager or the CBM.

**3** Access the directory on the core manager that contains the software load file.

**cd /swd**

**4** Uncompress the software load file.

**gzip -d P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz**

**5** Untar the software load file.

**tar -xvf P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar**

*The following individual files result from uncompressing and untarring the vaulted software load file and are placed in a new directory:*

- *device_mgr_XXXX_tar.gz.tape – compressed software file of the Device Manager*
- *pp8600_XXXX_tar.gz.tape – compressed software file of the Passport 8600*
- *cs_lan_XXXX.readme.tape – basic instructions for handling and preparing these software files*

***where:***
*XXXX is the release of the software being upgraded*

**6** Access the new directory that contains the individual files.

**cd /P86S00X0.X.V.NCL.NAP.VAULT.D**

**7** Rename and move the Device Manager file for it to be recognizable for uncompression into the /swd directory.

**mv device_mgr_XXXX_tar.gz.tape /swd/device_mgr_XXXX.tar.gz**

8 Reaccess the /swd directory on the core manager that contains the Device Manager software file.

**cd /swd**

9 Uncompress the Device Manager file.

**gzip -d device_mgr_XXXX.tar.gz**

10 Untar the Device Manager file to create the files in the appropriate directory structure.

**tar -xvf device_mgr_XXXX.tar**

*The directory structure for the files is created under the directory path .../dm/XXXX.*

*where <XXXX> is the new directory to hold the files for this release*

*The files are prepared for the software upgrade process.*

11 The procedure is complete.

***Note 1:*** Delete the following files after the upgrade has been completed successfully:

- all files in the /swd directory on the core manager
- software load file in the /tmp directory on the CS 2000 Management Tools server (applies just to the SDM/CS 2000 Core Manager)

***Note 2:*** A condensed version of these steps also is available on the file cs_lan_XXXX.readme.tape. For details on uncompressing the load files for the upgrade from the cs_lan_XXXX.readme.tape, use command:

**# more cs_lan.readme.tape**

Use this second procedure when the Device Manager software is delivered on a CD.

**Procedure 2 Preparing the CD version of the Device Manager**

**software for an upgrade**

***At the workstation***

1 Enter the following commands to set up the directory structures on the core manager into which the Device Manager files are to reside.

**cd /swd**

**mkdir dm**

**chmod 755 dm**

**cd dm**

**mkdir XXXX**

**where**
XXXX matches the new release of the Device Manager software (e.g., 5821)

**chmod 755 XXXX**

2 Select the core manager used in the network configuration.

| If the core manager is | Do |
|---|---|
| a CBM | step 3 |
| an SDM/CS 2000 Core Manager | step 6 |

3 Insert the CD into the CD drive on the CBM. Access the appropriate CD ROM directories.

**cd /cdrom/cdrom0**

4 Enter the following command to copy each of the Device Manager software files from the CD into the /swd/dm/XXXX directory of the CBM.

copy <filename> /swd/dm/XXXX/<filename>

5 Eject the CD.

**eject cdrom**

Continue to step 10.

6 Insert the CD into the CS 2000 Management Tools server. Access the appropriate CD ROM directories.

**cd /cdrom/cdrom0**

7 Enter the following command to copy each of the Device Manager software files from the CD into a temporary location on the CS 2000 Management Tools server.

**copy <filename> /tmp/<filename>**

8 Eject the CD.

**eject cdrom**

9 Use trivial file transfer protocol (TFTP) or file transfer protocol (FTP) to transfer each of Device Manager files as binary files from the /tmp directory to the /swd/dm/XXXX directory of the SDM/CS 2000 Core Manager.

10 Access the directory on the appropriate core manager that contains the Device Manager software files.

**cd /swd/dm/XXXX**

11 Change the access permissions on all the files in the directory as follows:

**chmod 755 ***

12 The procedure is complete.

# Passport 8600 Software Upgrade for the CS-LAN

## Upgrading Passport 8600 software for the CS-LAN

This procedure upgrades Passport 8600 software on routers that support the Succession Communication Server LAN (CS-LAN).

**ATTENTION**

Nortel Networks strongly recommends thoroughly reading this introduction, especially Important upgrade considerations, *before* attempting procedure Upgrading Passport 8600 software for the CS-LAN.

### Software upgrade strategy

The Succession CS-LAN uses pairs of Passport 8600 (8010co chassis) routers in a virtual router redundancy protocol (VRRP) configuration. Although this is not the only Succession architecture to use Passport 8600 pairs, this software upgrade procedure only applies to Passport 8600s that support the CS-LAN.

**Passport 8600 Router – Chassis 8010co Front View**



In the VRRP configuration, one Passport 8600 (typically Chassis 0) acts as the master router; the other (Chassis 1) acts as the slave. The multi-link trunks (MLT) that interconnect these redundant Passport 8600s use open shortest path first (OSPF) protocol. The interface between CS-LAN and core network also uses the OSPF protocol. This means that VRRP monitors the LAN-side and OSPF monitors the WAN-side of the CS-LAN network connectivity. This architecture provides effective and reliable, non-load sharing redundancy for the network.

This redundancy makes a phased approach to the upgrade of Passport 8600 software possible. Phased upgrades begin by upgrading the software on the slave router. Next, a switch of activity occurs and the newly upgraded, inactive slave side becomes the active master. Finally, a software upgrade occurs on the previously active, now inactive side. This technique minimizes the likelihood of service interruptions.

## Important upgrade considerations



**CAUTION**

To avoid network services disruption when upgrading the call processing unit (CPU) memory of a Passport 8600, perform the memory upgrade only when indicated in step 81. At this point, all traffic has been migrated to the other Passport 8600 chassis before the CPU is powered down for the memory upgrade.

Beginning with SN07, this upgrade procedure addresses Passport 8600 configurations with dual CPUs. Therefore, execute all CPU-related commands on the master CPU, except where otherwise noted.

***Note:*** If your configuration involves a dual CPU, ensure you have access the both CPUs independently (that is, one established connection to each CPU).

In addition, customers with a fully patched current load upgrading from SN06 (or greater) to SN07 can skip the following steps addressing the Gateway Controller (GWC) in this procedure:

- step 33e
- step 40 to step 41c (*but* perform step 41d)
- step 87

However, customers upgrading from SN05 to SN07 ***must*** perform all steps addressing the GWC.

Also, refer to sub-section Text conventions for brief descriptions and examples of filenames that appear in commands throughout this procedure. This subsection also includes descriptions for distinguishing between the master and standby CPUs in the command line interface (CLI).

The Universal Signaling Point-Compact (USP-Compact) is addressed in the Passport 8600 Software/Upgrade Rollback (CS-LAN) procedures. However, no specific steps addressing the Universal Signaling Point (USP) are required in these procedures.

### Supported solutions

The Passport 8600 Software Upgrade and Rollback (CS-LAN) procedures apply to all IP and ATM solutions, unless specified otherwise. One exception is the PT-AAL1 solution, in which the Passport 8600 does not carry call processing traffic. The PT-AAL1 solution includes the use of just the following Succession components:

- Dynamic Packet Trunking (DPT) Spectrum Peripheral Modules (SPM)
- Interworking Spectrum Peripheral Modules (IW SPM)
- Multi-service Gateway 4000 (MG 4000)

Other Succession components involved in the procedures for upgrading and rolling back the Passport 8600 software do ***not*** apply to PT-AAL1. Therefore, execute just the following steps in procedure Upgrading Passport 8600 software for the CS-LAN for a PT-AAL1 solution:

- step 1 to step 9
- step 72 to step 80
- step 99d and step 100

### Acquiring Passport 8600 software for the CS-LAN

Beginning with SN07, software for the Succession Passport 8600 is stored in the Nortel Networks Software Vault. The Software Vault is a repository for maintaining and distributing controlled copies of software loads to Nortel customers.

The Software Vault provides the following benefits:

- version control
- access control
- query and persistency capabilities using a distributed multi-client, multi-server architecture
- transaction control

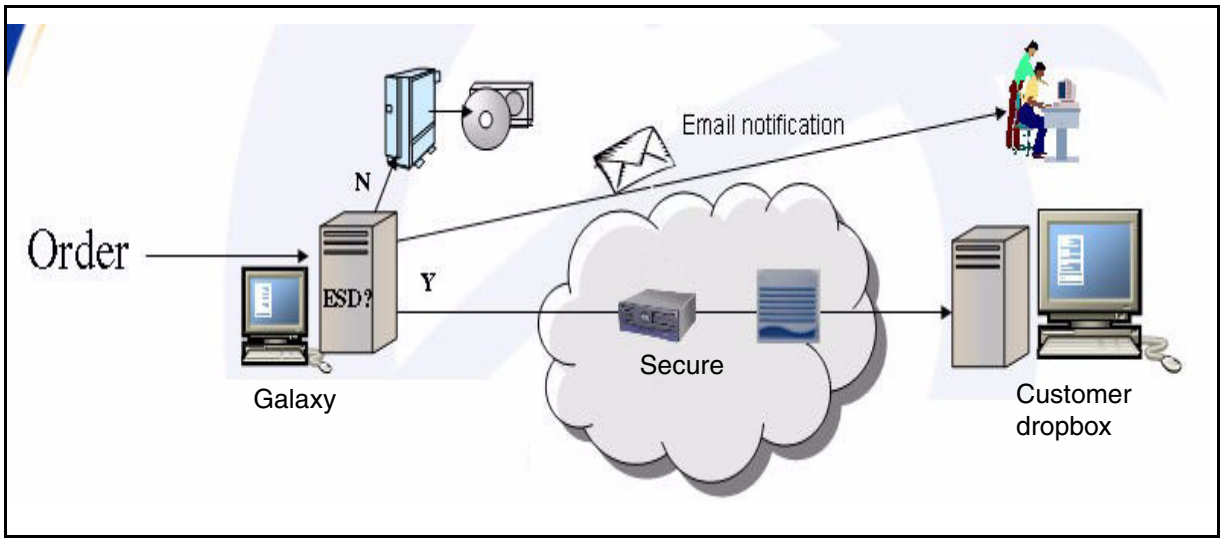
#### Software delivery methods

Customers receive the Passport 8600 software either through electronic software delivery (ESD) or manufactured on physical media, such as a compact disk (CD), and couriered to the customer site.

The Galaxy ESD tool accommodates global software delivery using business-to-business processes and automated electronic distribution of Nortel products to customer locations.

The following figure shows a high-level example of how the software is released to the customer site through ESD.

**Software order and ESD delivery overview**




Galaxy compresses the software file into a tar.gz file for delivery. The file adheres to ESD filenaming conventions. The following is an example of the vaulted software load file for the Passport 8600:

**Example**
P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz

**where**

P86S00X0.X refers to the ordering code for the Passport 8600 software in the SN07 release

V refers to the product release (V for VO; R for Released)

NCL refers to the software load type (NCL for non-CM load; MNCL for maintenance non-CM load)

NAP refers to the processor type

VAULT refers to the Nortel software repository source

X refers to the Nortel product repository version (if applicable)

D refers to the software file format reason (Distribution)

tar refers to a tarred file

gz refers to a zipped file

**Preparing the software file for an upgrade**
Before starting an upgrade on the Passport 8600, perform the following software preparative measures:

- Move the Passport 8600 software [load] file(s) to the appropriate directory on the SuperNode Data Manager (SDM)/CS 2000 Core Manager or the Core and Billing Manager (CBM). If retrieving the software from ESD, the software load file is located in the ESD drop box.

  **where:**
  P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz is the software load file

- Unzip and untar the software load file.
- Rename, unzip, and untar the Passport 8600 file.

  **where:**
  pp8600_XXXX_tar.gz.tape is the Passport 8600 file

***Note:*** The final destination for the Passport 8600 software file is the /flash/ directory on the Passport 8600.

The following two procedures show how to prepare the Passport 8600 software for an upgrade.

Use the first procedure when retrieving the Passport 8600 software from an ESD delivery.

**Preparing the ESD version of the Passport 8600 software for an upgrade**

***At the workstation***

**1** Select the location of the ESD drop box follows:

| If the ESD drop box is | Do |
|---|---|
| not in the /swd directory of the SDM/CS 2000 Core Manager or the CBM | step 2 |
| in the /swd directory of the SDM/CS 2000 Core Manager or the CBM | step 3 |

**2** Use trivial file transfer protocol (TFTP) or file transfer protocol (FTP) to transfer the software load file as a binary file to the /swd directory of the SDM/CS 2000 Core Manager or the CBM.

**3** Access the directory on the core manager that contains the software load file.

**cd /swd**

4 Uncompress the software load file.

**gzip -d P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz**

5 Untar the software load file.

**tar -xvf P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar**

*The following individual files result from uncompressing and untarring the vaulted software load file and are placed in a new directory:*

- *pp8600_XXXX_tar.gz.tape – compressed software file of the Passport 8600*
- *device_mgr_XXXX_tar.gz.tape – compressed software file of the Device Manager*
- *cs_lan_XXXX.readme.tape – basic instructions for handling and preparing these software files*

***where:***
*XXXX is the release of the software being upgraded*

6 Access the new directory that contains the individual files.

**cd /P86S00X0.X.V.NCL.NAP.VAULT.D**

7 Rename and move the Passport 8600 file for it to be recognizable for uncompression into the /swd directory.

**mv pp8600_XXXX_tar.gz.tape /swd/pp8600_XXXX.tar.gz**

8 Reaccess the /swd directory on the core manager that contains the Passport 8600 software file.

**cd /swd**

9 Uncompress the Passport 8600 file.

**gzip -d pp8600_XXXX.tar.gz**

10 Untar the Passport 8600 file to create the files in the appropriate directory structure.

**tar -xvf pp8600_XXXX.tar**

*The directory structure for the files is created under the directory path .../pp8600/XXXX.*

*where <XXXX> is the new directory to hold the files for this release*

*The files are prepared for the software upgrade process.*

11 The procedure is complete. Continue to procedure Upgrading Passport 8600 software for the CS-LAN.

***Note 1:*** Delete the following files *after* the upgrade has been completed successfully:

- all files in the /swd directory on the core manager
- software load file in the /tmp directory on the CS 2000 Management Tools server (applies just to the SDM/CS 2000 Core Manager)

***Note 2:*** A condensed version of these steps also is available on the file *cs_lan_XXXX.readme.tape*. For details on uncompressing the load files for the upgrade from the cs_lan_XXXX.readme.tape, use command:

**# more cs_lan.readme.tape**

Use the second procedure when the Passport 8600 software is delivered on a CD.

### Preparing the CD version of the Passport 8600 software for an upgrade

***At the workstation***

1 Enter the following commands to set up the directory structures on the core manager into which the Passport 8600 files are to reside.

**cd /swd**

**mkdir pp8600**

**chmod 755 pp8600**

**cd pp8600**

**mkdir XXXX**

**where**
XXXX matches the new release of the Passport 8600 software (e.g., 3720)

**chmod 755 XXXX**

2 Select the core manager used in the network configuration.

| If the core manager is | Do |
|---|---|
| a CBM | step 3 |
| an SDM/CS 2000 Core Manager | step 6 |

3 Insert the CD into the CD drive on the CBM. Access the appropriate CD ROM directories.

**cd /cdrom/cdrom0**

4 Enter the following command to copy each of the Passport 8600 software files from the CD into the /swd/pp8600/XXXX directory of the CBM.

**copy <filename> /swd/pp8600/XXXX/<filename>**

5 Eject the CD.

**eject cdrom**

Continue to step 10.

6 Insert the CD into the CS 2000 Management Tools server. Access the appropriate CD ROM directories.

**cd /cdrom/cdrom0**

7 Enter the following command to copy each of the Passport 8600 software files from the CD into a temporary location on the CS 2000 Management Tools server.

**copy <filename> /tmp/<filename>**

8 Eject the CD.

**eject cdrom**

9 Use trivial file transfer protocol (TFTP) or file transfer protocol (FTP) to transfer each of Passport 8600 files as binary files from the /tmp directory to the /swd/pp8600/XXXX directory of the SDM/CS 2000 Core Manager.

10 Access the directory on the appropriate core manager that contains the Passport 8600 software files.

**cd /swd/pp8600/XXXX**

11 Change the access permissions on all the files in the directory as follows:

**chmod 755 ***

12 The procedure is complete. Continue to procedure Upgrading Passport 8600 software for the CS-LAN.

### When to use this procedure

Use this procedure to upgrade the software load Passport 8600s supporting the CS-LAN as required by release changes.

If the software upgrade must be reversed, use the procedure titled Rolling Back Software Upgrades on Passport 8600s Supporting CS-LANs to restore the original software load.

### Prerequisites

Make sure a TFTP server is available. Console ports must be accessible.

### Text conventions

This briefly describes text conventions for displaying filenames that appear in commands throughout this procedure.

***Note:*** Refer to this section, as needed throughout the course of the upgrade and rollback procedures, for clarifications on the different software files.

**<a.b.c.d>**
is the IP address of the TFTP server

**<bootbkup>**
is the name of the backup copy of the boot configuration file on the PCMCIA card

**<cfgbkup>**
is the name of the backup copy of the software configuration file on the PCMCIA card

**<new3DES>**
is the name of the new Triple data encryption standard (3DES) file on the PCMCIA card

*for example:*
p80cXXX.img

*where:*
cXXX is the release number

**<newATM>**
is the name of the new ATM load file on the PCMCIA card

*for example:*
p80tXXXX.dld

*where:*
XXXX is the release number of the load

**<newboot>**
is the name of the new boot monitor image file on the PCMCIA card

*for example:*
p80bXXXX.img

*where:*
XXXX is the release number of the load (for example, p80b3320.img)

***Note:*** Use the boot monitor image file when executing a boot command.

**<newDES>**
is the name of the new data encryption standard (DES) file on the PCMCIA card

*for example:*
p80cXXX.des

*where:*
cXXX is the release number

**<newload>**
is the name of the new software image file on the PCMCIA card

*for example:*
p80aXXXX.img

*where:*
XXXX is the version of the software (for example, p80a3320)

***Note:*** Use the primary or secondary (or both) software image files when configuring a bootconfig command.

**<old3DES>**
is the name of the original DES file

*for example:*
p80cXXX.img

*where:*
cXXX is the release number

**<oldATM>**
is the name of the original ATM load file

*for example:*
p80tXXXX.dld

*where:*
XXXX is the release number of the load

**<oldboot>**
is the name of the original boot monitor image file

*for example:*
p80bXXXX.img

*where:*
XXXX is the release number of the load (for example, p80b3320.img)

**<oldDES>**
is the name of the original DES file

*for example:*
p80cXXX.des

*where:*
cXXX is the release number

**<oldload>**
is the name of the original software image file

*for example:*
p80aXXXX.img

*where:*
XXXX is the version of the software (for example, p80a3320)

**<slot>**
is the slot number for the Passport 8600

**<sonetif >**
is the Sonet interface on the ATM blade

**<swloadbkup>**
is the name of the backup version of the software image file

*for example:*
p80aXXXX.img

*where:*
XXXX is the version of the software (for example, p80a3320)

**<vid>**
is the identifier of each virtual local area network (VLAN)

**<vrid>**
is the VRRP identifier

**CPU syntax**

The CLI prompt syntax for the CPUs is as follows:

**<Passport_chassis_name>:CPU-slot#**

*where:*

the absence or inclusion of the “@” symbol at the beginning of the command syntax identifies the master or standby CPU, respectively.

**8600_04:5#**

refers to the master CPU

**@8600_04:6#**

refers to the standby CPU

## Instructions

This upgrade procedure applies to Passport 8600s that control the CS-LAN. The procedure uses a phased approach to upgrade one Passport 8600 at a time. This approach prevents service interruptions due to CS-LAN failure that would occur if both Passport 8600s are taken out of service at the same time.

The stepwise Upgrading Passport 8600 software for the CS-LAN procedure uses an iterative structure (two passes). The first pass upgrades the software on the slave router then does a switch of activity. When this change of activity completes, the slave Passport 8600 takes on the master Passport 8600 function (the previous master Passport 8600 becomes the slave). The procedure then cycles back to the first set of steps to repeat the software upgrade process on the second Passport 8600 supporting the CS-LAN.

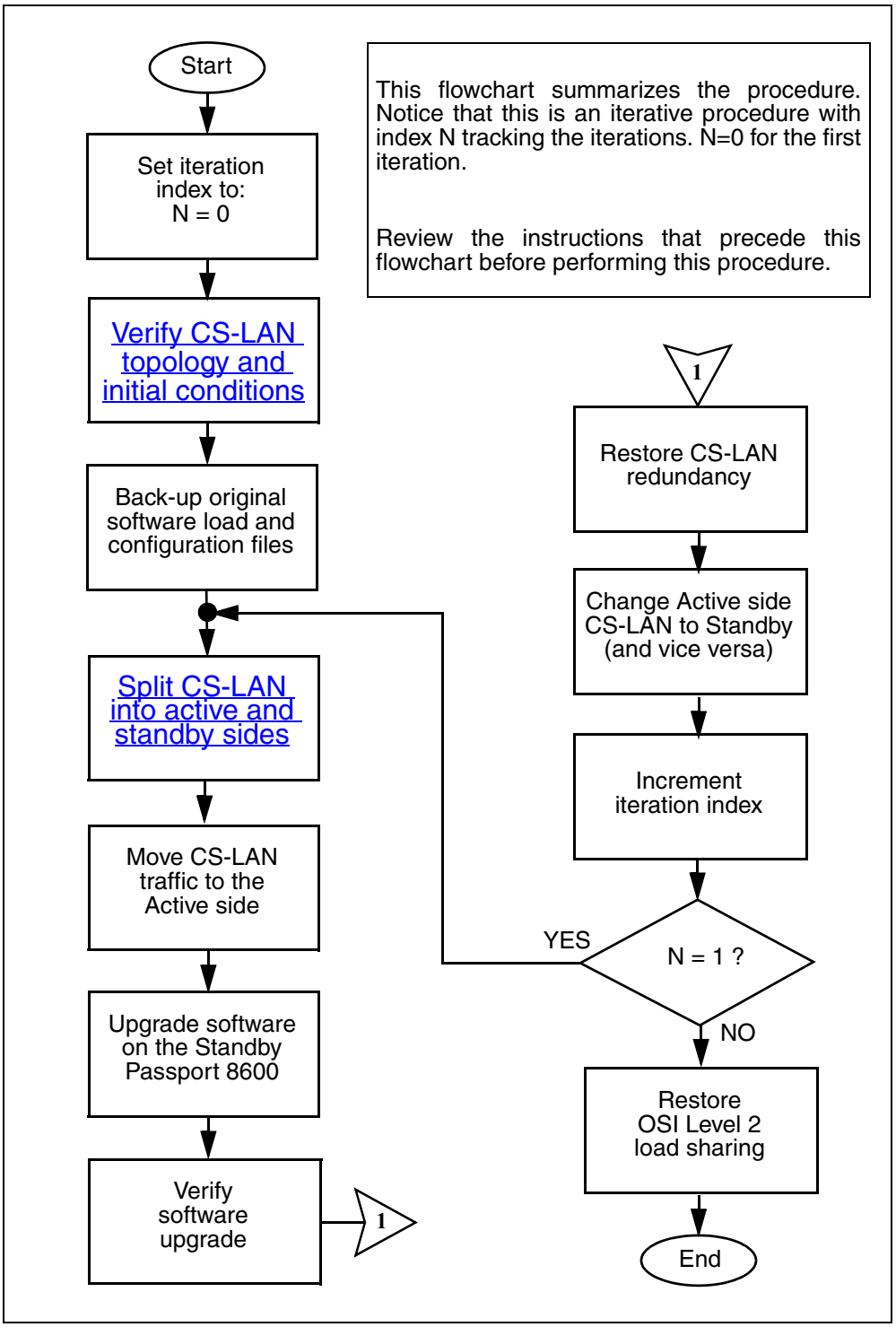
> ***Note:*** On the second pass through the iterative steps, the master and slave roles are swapped. Take this change into account as you perform the second pass on the repeated steps in this procedure.

Nortel Networks recommends that all network element Unit 0s subtend Passport 8600 Chassis 0 and all Unit 1s subtend Chassis 1. The Upgrading Passport 8600 software for the CS-LAN procedure assumes the topology of your CS-LAN conforms to this recommendation.

> ***Note 1:*** If the topology of your CS-LAN does not conform to this recommendation, take this variation into account as you perform this procedure.
>
> ***Note 2:*** If your solution includes Passport Voice Gateways (PVG), offload traffic from the slave to the master Passport 8600 before upgrading the slave software (see Procedure , Upgrading Passport 8600 software for the CS-LAN -- step 14 to step 28).

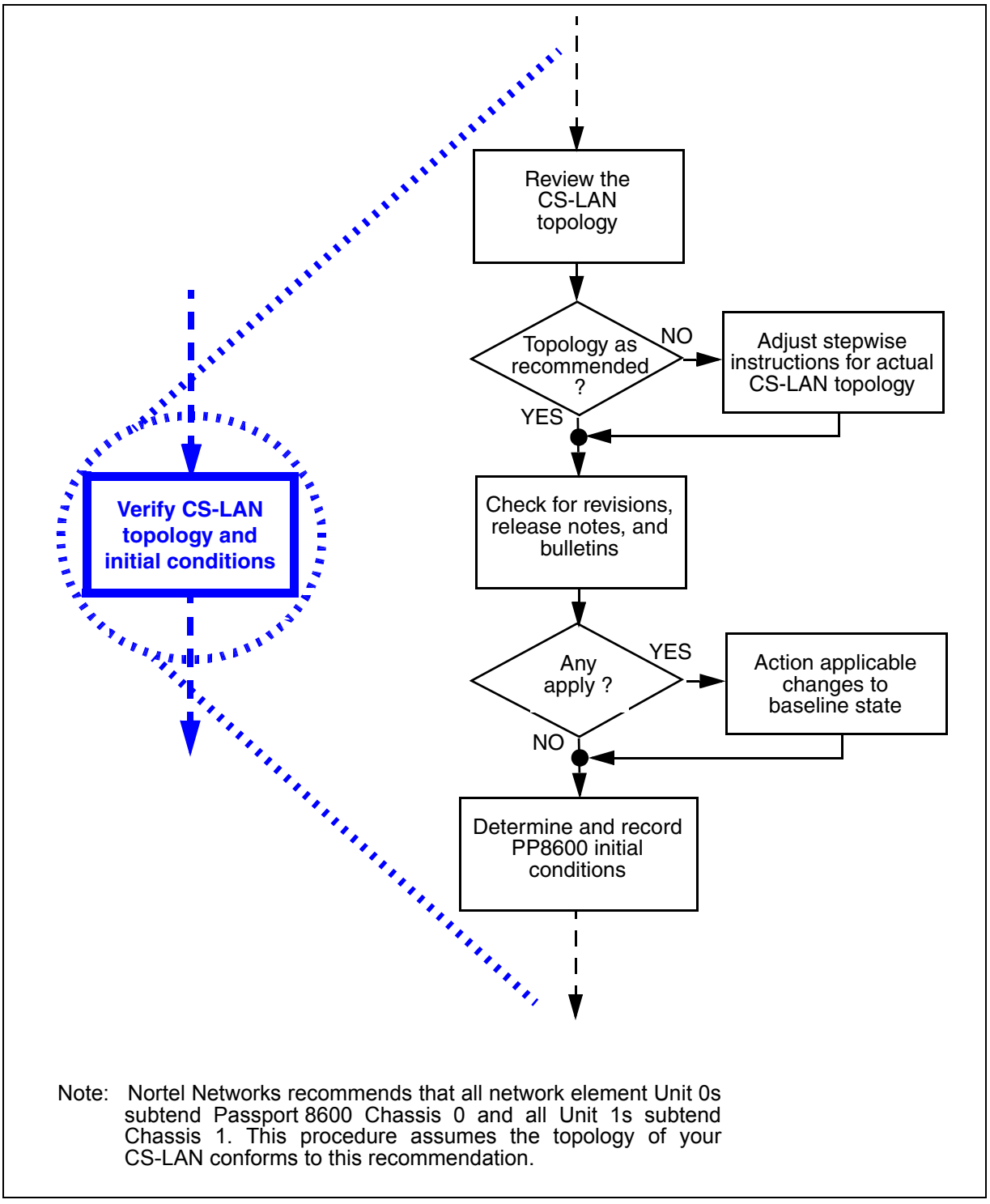
The following flowchart summarizes the overall software upgrade procedure.

### Upgrading Passport 8600 software for the CS-LAN



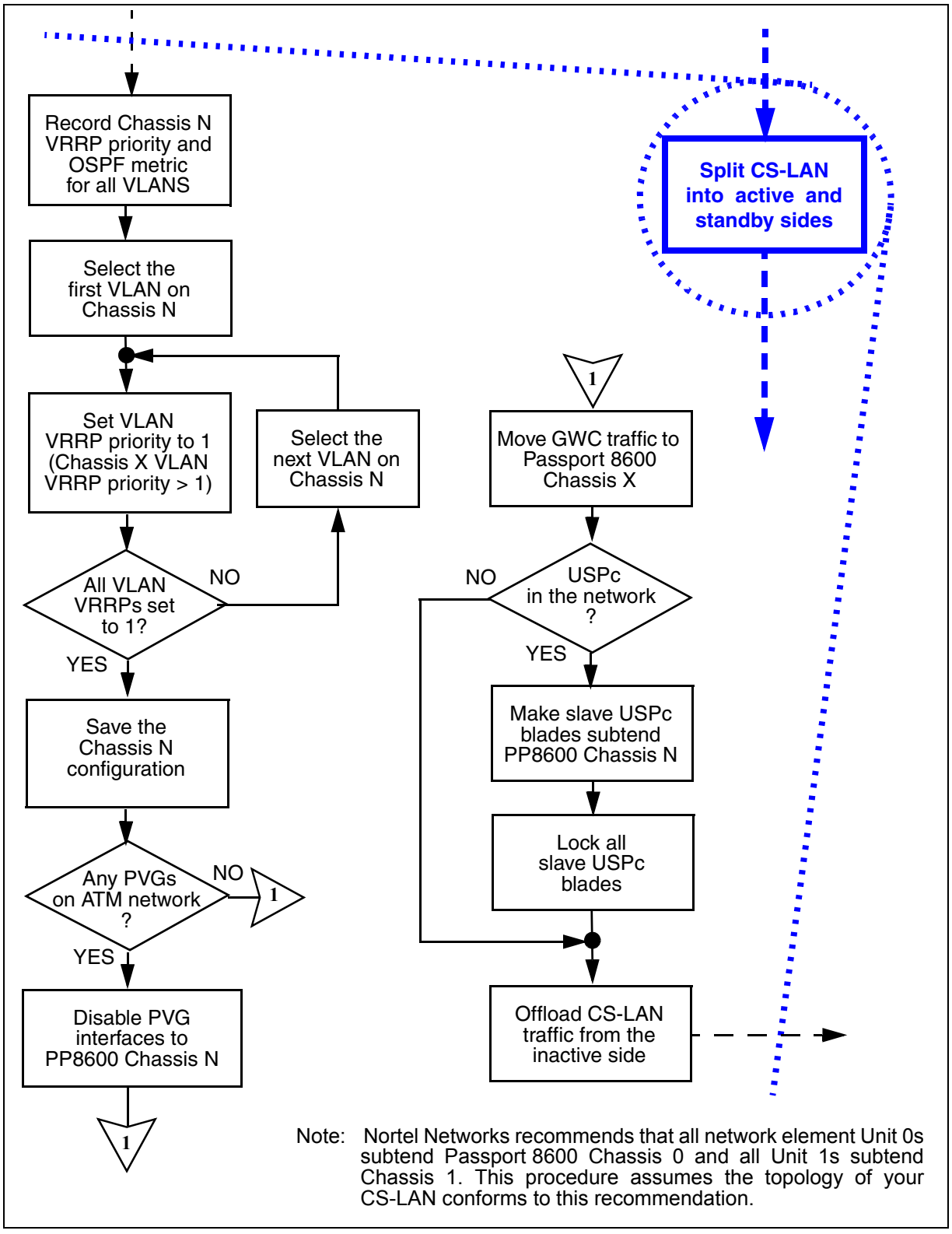
The following flowcharts provide additional detail to the Upgrading Passport 8600 software for the CS-LAN flowchart.

## Verify CS-LAN topology and initial conditions




Note: Nortel Networks recommends that all network element Unit 0s subtend Passport 8600 Chassis 0 and all Unit 1s subtend Chassis 1. This procedure assumes the topology of your CS-LAN conforms to this recommendation.

## Split CS-LAN into active and standby sides




Note: Nortel Networks recommends that all network element Unit 0s subtend Passport 8600 Chassis 0 and all Unit 1s subtend Chassis 1. This procedure assumes the topology of your CS-LAN conforms to this recommendation.

Access the Passport 8600s using the serial (console) port. You can use a direct serial connection and a terminal program from an attached PC or a TELNET connection to an appropriately configured IP address on a terminal server connected to the console port.

Make sure you use READ/WRITE/ALL (RWA) login and/or password privileges when performing this procedure. For more information about RWA privileges, refer to Passport Documentation in the Nortel Networks website.

Select the *Documentation* option for *Passport 8600 Routing Switch* and choose *Getting Started*.

**ATTENTION**

The GUI/HMI graphics that support this procedure are current as of (I)SN07. Although these illustrations differ from the GUI/HMI you are using, perform all stepwise actions by accessing your element managers and making the equivalent choices.

**ATTENTION**

This upgrade procedure causes ALARMS to occur on CS-LAN components. These ALARMS report the loss of certain redundant paths during the upgrade process. These losses are not service affecting and the paths are restored on completion of the upgrade.

**ATTENTION**

This is an iterative procedure that includes two passes. Make sure you understand the Instructions and flowchart that support this procedure before you begin Upgrading Passport 8600 software for the CS-LAN. The iterations (passes) proceed as follows:

- step 1 to step 9 establish initial conditions for the iterative procedure *to be completed on both CS-LAN routers*
- first pass (N=0) includes step 10 to step 100
- second pass (N=1) includes step 10 to step 101

## Upgrading Passport 8600 software for the CS-LAN

**ATTENTION**

Ensure that you complete step 1 through step 9 on *both* routers before continuing to step 10.

***With reference to documentation supporting your CS-LAN (contact your system administrator if necessary):***

**1** Review your CS-LAN topology to verify the following:

**a** Passport 8600s are in-service and use VRRP configuration.

**b** all network element Unit 0s subtend Passport 8600 chassis 0 and all Unit 1s subtend Passport 8600 chassis 1

***Note 1:*** If your CS-LAN does not conform with this topology take local variations into account as you perform this procedure.

***Note 2:*** The following table defines the Passport 8600 master/slave conventions for this procedure.

| Iteration | Slave Passport 8600 | Master Passport 8600 |
|---|---|---|
| First Pass | Chassis N = 0 | Chassis X = 1 |
| Second Pass | Chassis N = 1 | Chassis X = 0 |

**2** Check the Nortel Networks website for and action any bulletins, release notes, and revisions that impact this procedure.

Select option *Documentation* under *Passport 8600 for Succession* and check for bulletins, release notes, and revisions that impact this procedure.

***Use the Passport 8600 CLI to verify Passport 8600 initial conditions:***

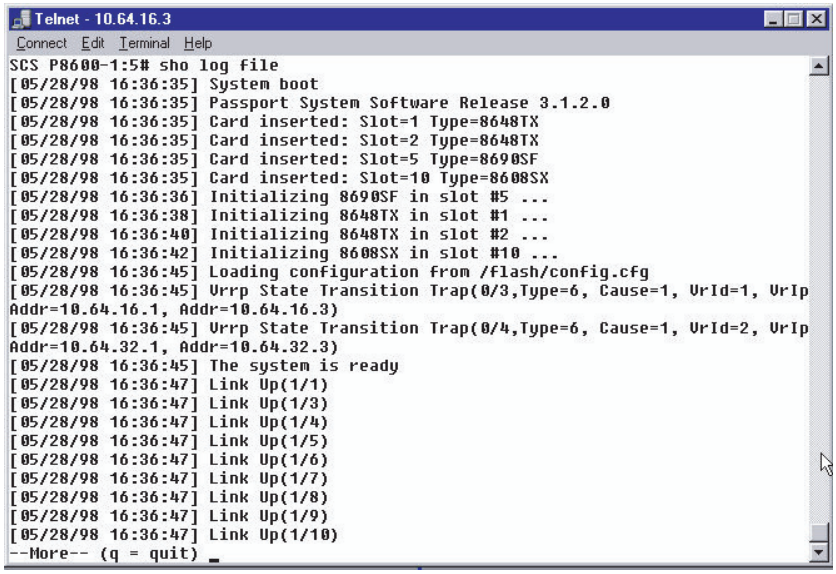
**3** Verify the correct operation of the Passport 8600 as follows:

**a** check the log file by typing:

**sho log file**

*Review the log file (see the following figure) and correct any errors or problems reported.*

***Note:*** *For more information, refer to "Succession Fault Management Logs Reference", NN10275-909, or contact your next level of support.*




**b** check the configuration by typing:

**sho config**

*The configuration file appears showing network topology.*

***Note:*** *Topology should conform with the recommended configuration (see Instructions and step 1, sub-step b).*

**c** check the address resolution protocol information by typing:

**sho ip arp info**

*Compare the output for the IP ARP command against your*

*expected configuration and correct any discrepancies.*

***Note:** For more information, select option Documentation for Passport 8600 Routing Switch on the Nortel Networks website. Or contact your next level of support.*

**4** Verify all subtending links and nodes as follows:

**a** check supplemental router port statistics by typing:

**sho port error extended**

*Review the output for the extended port error command (see the following figure) and correct any problems reported.*

Terminal

Window Edit Options Help

```
SCS P8600-1:5# sho port error main

================================================================================
                                      Port Ethernet Error
================================================================================
PORT   ERROR   ERROR   FRAMES  TOO     LINK    CARRIER CARRIER SQETEST
NUM    ALIGN   FCS     LONG    SHORT   FAILURE SENSE   ERRORS  ERRORS
--------------------------------------------------------------------------------
1/1    0       0       0       0       0       0       0       0
1/2    0       0       0       0       0       0       0       0
1/3    0       0       0       0       0       0       0       0
1/4    0       0       0       0       0       0       0       0
1/5    0       0       0       2       0       0       0       0
1/6    0       0       0       21      0       0       0       0
1/7    0       0       0       1       0       0       0       0
1/8    0       0       0       0       0       0       0       0
1/9    0       0       0       15      0       0       0       0
1/10   0       0       0       22      0       0       0       0
1/11   0       0       0       103     0       0       0       0
1/12   0       0       0       0       0       0       0       0
1/13   0       0       0       2       0       0       0       0
1/14   0       0       0       0       0       0       0       0
1/15   0       0       0       0       0       0       0       0
1/16   0       0       0       0       0       0       0       0
1/17   0       0       0       0       0       0       0       0
1/18   0       0       0       0       0       0       0       0
1/19   0       0       0       0       0       0       0       0
1/20   0       0       0       0       0       0       0       0
1/21   0       0       0       0       0       0       0       0
1/22   0       0       0       0       0       0       0       0
1/23   0       0       0       0       0       0       0       0
1/24   0       0       0       0       0       0       0       0
1/25   0       0       0       0       0       0       0       0
1/26   0       10      0       5       0       1       0       0
1/27   0       0       0       0       0       0       0       0
1/28   0       0       0       0       0       1       0       0
1/29   0       0       0       0       0       0       0       0
1/30   0       0       0       0       0       0       0       0
1/31   0       0       0       0       0       0       0       0
1/32   0       0       0       0       0       0       0       0
1/33   0       0       0       0       0       0       0       0
1/34   0       0       0       0       0       0       0       0
1/35   0       0       0       0       0       0       0       0
```

***Note:*** *For more information, select option Documentation for Passport 8600 Routing Switch on the Nortel Networks website. Or contact your next level of support.*

**b** check router port error statistics by typing:

**sho port error main**

*Review the output for the main port error command (see the following figure) and correct any problems.*

Terminal

Window Edit Options Help

```
SCS P8600-1:5# sho port error main

================================================================================
                                      Port Ethernet Error
================================================================================
PORT   ERROR    ERROR    FRAMES   TOO      LINK     CARRIER CARRIER SQETEST
NUM    ALIGN    FCS      LONG     SHORT    FAILURE  SENSE   ERRORS  ERRORS
--------------------------------------------------------------------------------
1/1    0        0        0        0        0        0       0       0
1/2    0        0        0        0        0        0       0       0
1/3    0        0        0        0        0        0       0       0
1/4    0        0        0        0        0        0       0       0
1/5    0        0        0        2        0        0       0       0
1/6    0        0        0        21       0        0       0       0
1/7    0        0        0        1        0        0       0       0
1/8    0        0        0        0        0        0       0       0
1/9    0        0        0        15       0        0       0       0
1/10   0        0        0        22       0        0       0       0
1/11   0        0        0        103      0        0       0       0
1/12   0        0        0        0        0        0       0       0
1/13   0        0        0        2        0        0       0       0
1/14   0        0        0        0        0        0       0       0
1/15   0        0        0        0        0        0       0       0
1/16   0        0        0        0        0        0       0       0
1/17   0        0        0        0        0        0       0       0
1/18   0        0        0        0        0        0       0       0
1/19   0        0        0        0        0        0       0       0
1/20   0        0        0        0        0        0       0       0
1/21   0        0        0        0        0        0       0       0
1/22   0        0        0        0        0        0       0       0
1/23   0        0        0        0        0        0       0       0
1/24   0        0        0        0        0        0       0       0
1/25   0        0        0        0        0        0       0       0
1/26   0        10       0        5        0        1       0       0
1/27   0        0        0        0        0        0       0       0
1/28   0        0        0        0        0        1       0       0
1/29   0        0        0        0        0        0       0       0
1/30   0        0        0        0        0        0       0       0
1/31   0        0        0        0        0        0       0       0
1/32   0        0        0        0        0        0       0       0
1/33   0        0        0        0        0        0       0       0
1/34   0        0        0        0        0        0       0       0
1/35   0        0        0        0        0        0       0       0
```

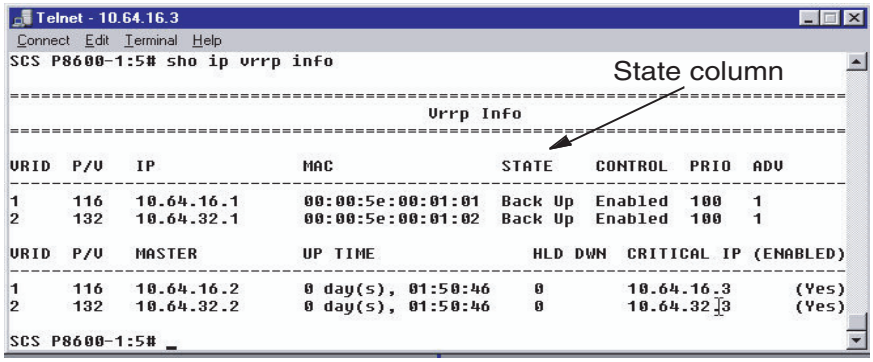
***Note:*** *For more information, select option Documentation for Passport 8600 Routing Switch on the Nortel Networks website. Or contact your next level of support.*

**5** Complete table Passport 8600 - Initial conditions as follows:

**a** type

**sho ip vrrp info**

*Output for the virtual router redundancy protocol command appears.*




**b** review the **State** column and record the master (State = Master) and slave (State = Back Up) status for each Passport 8600 Chassis in the table below.

***Note:*** If you cannot determine the master/slave status, call the next level of support.

c ***for each VLAN listed in the virtual router redundancy protocol file*** (see sub-step a), record the **VRID**, **VID (P/V)**, and **PRIO** information for each CS LAN Passport 8600 Chassis 0 and 1 in the table below.

**Passport 8600 - Initial conditions**

| | Status | | | | |
|---|---|---|---|---|---|
| | | Chassis 0 | | Chassis 1 | |
| **VRID** | **VID** | **OSPF Metric** | **VRRP PRIO** | **OSPF Metric** | **VRRP PRIO** |
| VRID 1 | | | | | |
| VRID 2 | | | | | |
| VRID 3 | | | | | |
| VRID 4 | | | | | |
| VRID 5 | | | | | |
| VRID 6 | | | | | |
| VRID 7 | | | | | |
| VRID 8 | | | | | |
| VRID 9 | | | | | |
| VRID 10 | | | | | |

***Note:*** **VID** is the VLAN identifier of each VLAN. **VRID** is the VRRP identifier. **PRIO** determines the priority setting for the related chassis. Setting the **PRIO** setting on the master router to a value less than that for the slave causes

a switch in master/slave status. The OSPF metric also is required when recording the VRRP priority.

***Use the Passport 8600 CLI to back up the original software load and configuration files:***

**6** Get the name of your current primary image file by typing:

**sho boot config**

*A sample output of the sho bootconfig command follows:*

*flags telnetd true*
*choice primary image-file "/flash/p80a3320.img"*
*choice secondary image-file "/pcmcia/p80a3224.img"*

**7** Select the next step as follows.

| If your CS-LAN | Do |
|---|---|
| is a dual CPU configuration per chassis | step 8 |
| is a single CPU configuration per chassis | step 9 |

**8**

**ATTENTION**
Do not delete the current software load ***before*** successfully completing the upgrade. Current software must remain available as the secondary load to support Passport 8600 failback capabilities.

**ATTENTION**
Before addressing any commands with a peer option, ensure that the DNS entries were created previously for each CPU. For details on creating DNS entries, refer to the v3.7.0.0 Release Notes.

**ATTENTION**
Refer to section Text conventions on page 59 for brief definitions and examples of the software filenames used in the following command lines.

For CS-LANs with a dual-CPU configurations, back up the current config, bootconfig, and software load files to the PCMCIA card as follows:

**a** First save the current config and bootconfig files. Type the following two commands:

**sav config**

**sav bootconfig**

***Note:*** For Passport 8600s using a dual CPU configuration, the above commands save the config and bootconfig files on the flash for both CPUs. If the switch response does not show the file being saved to the standby CPU, copy the two files to the standby CPU. Type:

**copy /flash/config.cfg peer:/flash/config.cfg**

**copy /flash/boot.cfg peer:/flash/boot.cfg**

In the following sub-steps, both commands must be executed on the master CPU.

The Passport 8600 automatically copies files to the PCMCIA card using the same name as the current file. Therefore, it is not necessary to enter a new filename in the command for the backup version of the files in step 8b through step 8f.

**b** Back up the software image file. Type:

**copy /flash/<oldload> /pcmcia/**

**copy peer:/flash/<oldload> peer:/pcmcia/**

where **<oldload>** is the original software image filename

*Software image backs up from flash memory to PCMCIA.*

**c** Back up the boot monitor load file. Type:

**copy /flash/<oldboot> /pcmcia/**

**copy peer:/flash/<oldboot> peer:/pcmcia/**

where **<oldboot>** is the original boot monitor image filename

**d** ***Only*** if the Passport 8600 uses an ATM blade, back up the ATM load file. Type:

**copy /flash/<oldATM> /pcmcia/**

**copy peer:/flash/<oldATM> peer:/pcmcia/**

where **<oldATM>** is the original ATM load filename

**e** If the Passport 8600 uses data encryption standard (DES), back up the file. Type:

**copy /flash/<oldDES> /pcmcia/**

**copy peer:/flash/<oldDES> peer:/pcmcia/**

where **<oldDES>** is the original DES filename

**f** If the Passport 8600 uses Triple DES (3DES), back up the file. Type:

**copy /flash/<old3DES> /pcmcia/**

**copy peer:/flash/<3oldDES> peer:/pcmcia/**

where **<old3DES>** is the original 3DES filename

**g** Back up the config file. Type:

**copy /flash/config.cfg /pcmcia/<cfgbkup>**

**copy peer:/flash/config.cfg peer:/pcmcia/<cfgbkup>**

where **<cfgbkup>** is the name for the backup copy of this file on the PCMCIA card

**h** Back up the bootconfig file to the PCMCIA card. Type:

**copy /flash/boot.cfg /pcmcia/<bootbkup>**

**copy peer:/flash/boot.cfg peer:/pcmcia/<bootbkup>**

where **<bootbkup>** is the name for the backup copy of this file on the PCMCIA card

Go to step 10.

**9**

**ATTENTION**

Do not delete the current software load ***before*** successfully completing the upgrade. Current software must remain available as the secondary load to support Passport 8600 failback capabilities.

For CS-LANs with a single CPU configuration, back up the current config, bootconfig, and software load files to the PCMCIA card as follows:

**a** First save the current config and bootconfig files. Type the following two commands:

**sav config**

**sav bootconfig**

The Passport 8600 automatically copies files to the PCMCIA card using the same name as the current file. Therefore, it is not necessary to enter a new filename in the command for the backup version of the files in step 9b through step 9f.

**b** Back up the software image file. Type:

**copy /flash/<oldload> /pcmcia/**

where **<oldload>** is the original software image filename

*Software image backs up from flash memory to PCMCIA.*

**c** Back up the boot monitor load file. Type:

**copy /flash/<oldboot> /pcmcia/**

where **<oldboot>** is the original boot monitor image filename

**d** ***Only*** if the Passport 8600 uses an ATM blade, back up the ATM load file. Type:

**copy /flash/<oldATM> /pcmcia/**

where **<oldATM>** is the original ATM load filename

**e** If the Passport 8600 uses data encryption standard (DES), back up the file. Type:

**copy /flash/<oldDES> /pcmcia/**

where **<oldDES>** is the original DES filename

**f** If the Passport 8600 uses 3DES, back up the file. Type:

**copy /flash/<old3DES> /pcmcia/**

where **<old3DES>** is the original 3DES filename

**g** Back up the config file. Type:

**copy /flash/config.cfg /pcmcia/<cfgbkup>**

where **<cfgbkup>** is the name for the backup copy of the software configuration file on the PCMCIA card

**h** Back up the bootconfig file to the PCMCIA card. Type:

**copy /flash/boot.cfg /pcmcia/<bootbkup>**

where **<bootbkup>** is the name for the backup copy of the boot configuration file on the PCMCIA card

Go to step 10.

***Note:*** If upgrading the CS-LAN software in a PT-AAL1 solution, skip to step 72.

***Use the Passport 8600 CLI to split the CS-LAN into active and standby sides (Passport 8600s in simplex mode)***

**10**

| | |
|---|---|
| | **ATTENTION**<br>Ensure that you have completed step 1 through step 9 on *both* routers during the first pass before continuing with this upgrade procedure. |

Record Chassis N VRRP priority and OSPF metrics as follows:

***Note:*** For second pass (N=1), replace Chassis N with Chassis X when record of information is required.

**a** type:

**config vlan <vid> ip vrrp <vrid> info**
refer to table Passport 8600 - Initial conditions in step 5 for **VID** and **VRID** information for Chassis N

**b** record the priority information for the **<vrid>** for use in step 99



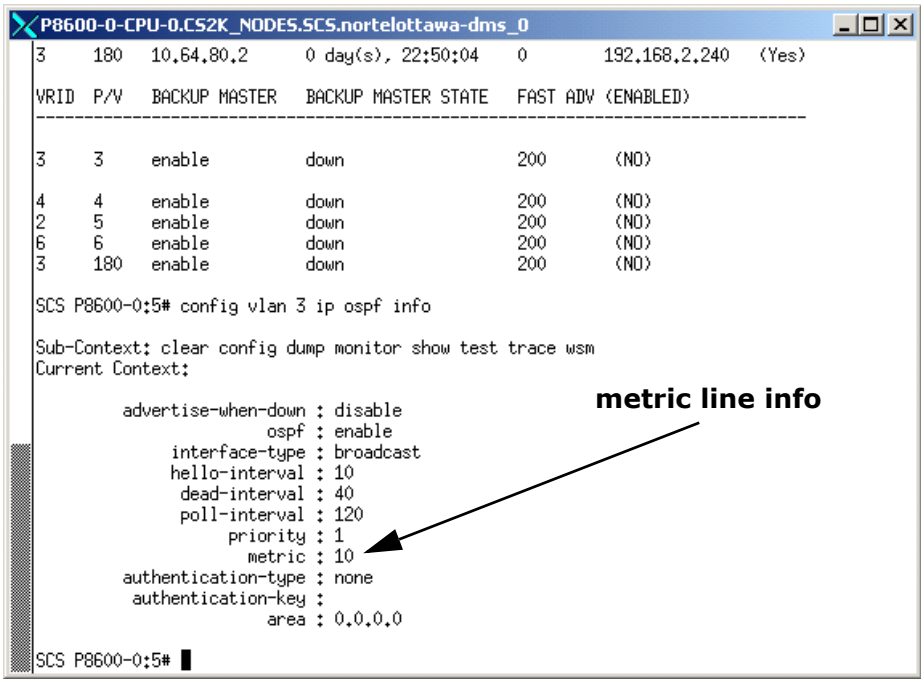

**c** type:

**config vlan <vid> ip ospf info**

*The CLI displays the OSPF information (see graphic below).*

**d** record the OSPF metric information for use in step 99

**e** repeat sub-step a to sub-step d for each VLAN provisioned on the router




**11** Make sure that Passport 8600 Chassis N is the slave as follows:

**a** set the VRRP priority to 1 by typing

**config vlan <vid> ip vrrp <vrid> prio 1**

***Note:*** Setting Passport 8600 Chassis N **<prio>** to 1 makes it slave (Chassis X **<prio>** is greater than 1 making it the master).

**b** set the OSPF priority to 1000 by typing

**config vlan <vid> ip ospf metric 1000**

**c** repeat sub-step a and sub-step b for each VLAN provisioned on the router

**12** Save the new Passport 8600 Chassis N configuration by typing:

**sav config**

*This updates the new Passport 8600 configuration so that VRRP settings are maintained after any subsequent reboot.*

**13** Select the next step as follows:

| If your CS-LAN: | Do |
|---|---|
| includes ATM PVGs directly connected to the Passport 8600 (i.e., a non-VR solution) | step 14 |
| includes PVGs connected by Gig Ethernet (GigE) | step 29 |
| does not include PVGs | step 29 |
| includes ATM interfaces connected to a Passport 15000 chassis running VR or VrAp | step 29 |

***Note 1:*** The following steps (step 14 to step 28) offload PVG traffic from the Passport 8600 chassis undergoing a software upgrade. Offloading PVG traffic using these steps minimizes the impact of the software upgrade process on call processing.

***Note 2:*** These steps apply to full-featured, Packet Trunking Transit Solutions that use Passport Voice Gateways with the CS-LAN.

### *Use the PVG CLI to determine the PVG IP addresses*

**14** Check the provisioning information for the VSPs, NSTA, and VGS subcomponents as follows:

**a** display media and signaling gateway IP addresses by typing:

**d -p nsta/* vgs ctrl/***

*The following list provides sample MG and SG IP addresses for a single VSP card provisioned in slot 7:*

```
+=====+====+--------------+---------------
|Nsta |Ctrl|    ipAddr    |    dnsList
+=====+====+--------------+---------------
|    7|mg  |172.16.201.2  |
|    7|sg  |172.16.201.6  |
```

***Note:*** *The ... **nsta/* vgs ctrl/** component of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows MG and SG IP addresses for a single VSP card provisioned in slot 7.*

**b** display the IPmcon IP address by typing:

**d -p nsta/* vgs ipmcon**

*The following list provides a sample IPmcon IP address for a single VSP card provisioned in slot 7:*

```
+=====+---------------+-----+--------------
|Nsta |    ipAddr     |udpBa|Response
|     |               | se  |
+=====+---------------+-----+--------------
|    7|172.16.201.10  |49152|
```

***Note:*** *The ... **nsta/* vgs ipmcon** component of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows IPmcon IP address for a single VSP card provisioned in slot 7.*

***Use each Passport 8600 CLI to verify that the PVGs are set up redundantly***

**15** Check the VLAN configuration file by typing the following command on each Passport 8600 chassis:

**sho config module vlan**

*This command outputs all VLANs provisioned on the Passport 8600 Chassis. The example that follows shows the output of this command for only one VSP blade:*

```
vlan 702 create byport 1 name "PVG40-vsp07-mg"
vlan 702 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 702 ports add 8/1 member portmember
vlan 702 ip create 172.16.201.1/255.255.255.252 mac_offset 5
vlan 706 create byport 1 name "PVG40-vsp07-sg"
vlan 706 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 706 ports add 8/1 member portmember
vlan 706 ip create 172.16.201.5/255.255.255.252 mac_offset 14
vlan 710 create byport 1 name "PVG40-vsp07-media"
vlan 710 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 710 ports add 8/1 member portmember
vlan 710 ip create 172.16.201.9/255.255.255.252 mac_offset 6
```

***Note:*** *Both Passport 8600s should display the identical PVG VLAN configuration. The **vlan ### ports add** entry identifies each VSP ATM Sonet connection. This information is required in* step 21*.*

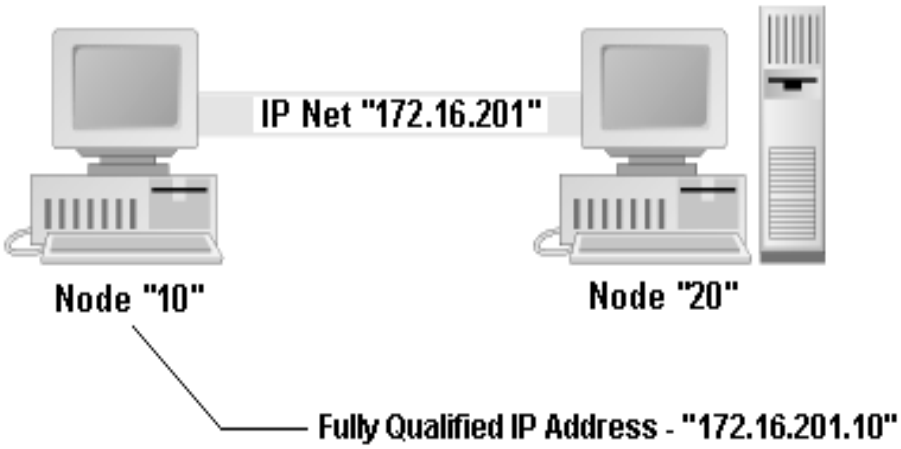
**16** Check the routing table information for each Passport 8600 chassis as follows:

**a** type:

**sho ip route info ip x.y.z**

where x.y.z specifies the IP Net address provided at step 14.

***Note:*** Specifying the x.y.z octets limits the command output to those nodes served by the specified IP Net.




*The following list provides an example for the command output for one of the Passport 8600s:*

```
================================================================================================
                                Ip Route
================================================================================================
          DST             MASK              NEXT         COST   VLAN   PORT    PROT  AGE  TYPE PRF
------------------------------------------------------------------------------------------------
   172.16.201.0 255.255.255.252   172.16.201.1     1  702   -/-    LOC    0 DB     0
   172.16.201.4 255.255.255.252   172.16.201.5     1  706   -/-    LOC    0 DB     0
   172.16.201.8 255.255.255.252   172.16.201.9     1  710   -/-    LOC    0 DB     0

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.
------------------------------------------------------------------------------------------------
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW
```

*The following list provides an example for the command output for the other Passport 8600 Chassis:*

```
================================================================================================
                                Ip Route
================================================================================================
         DST            MASK              NEXT         COST  VLAN  PORT  PROT   AGE TYPE PRF
------------------------------------------------------------------------------------------------
   172.16.201.0 255.255.255.252   172.30.242.230   20   80  -/-  OSPF   0 IB   120
   172.16.201.4 255.255.255.252   172.30.242.230   20   80  -/-  OSPF   0 IB   120
   172.16.201.8 255.255.255.252   172.30.242.230   20   80  -/-  OSPF   0 IB   120

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.
------------------------------------------------------------------------------------------------
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW
```

***Note 1:*** *The routing information under the PROT column heading should indicate either VSP subnet LOC or OSPF.*

***Note 2:*** *If both Passport 8600s indicate the same status for the same VSP subnet, this is a non-standard condition. Contact your next level of support.*

To prevent service interruption VSP VLANs on Chassis N of the Passport 8600 must be OSPF (LOC for Chassis X). Detailed steps forcing compliance to this requirement begin at step 23.

**b** repeat sub-step a for each VSP VLAN on the Passport 8600 Chassis N

**c** repeat sub-step a and sub-step b for Passport 8600 Chassis X.

***Use the PVG CLI to verify the correct provisioning of each VSP***

**17** Check the SPVCAP subcomponent of each VSP VGS Ctrl/<mg,sg> and IPmcon as follows:

**a** display the provisioning information for each VSP by typing:

**d -p -no nsta/* vgs ctrl/* spvcap**

*The following list shows VSP provisioning information for slot 7. The actual command output lists all VSP information.*

```
Nsta/ 7 VGS Ctrl/mediaGateway SpvcAp
   atmServiceCategory = nrtVariableBitRate
   peakCellRate  = 800 cells
   sustainedCellRate= 400 cells
   maximumBurstSize= 100 cells
   retryLimit    = 0
   localAddress  = 45613512123400002F000000010020480D527001
   remoteVpiVci  = 7.2
   addressToCall = 45613512123400002F000000010020480D008D00
Nsta/ 7 VGS Ctrl/signalingGateway SpvcAp
   atmServiceCategory = nrtVariableBitRate
   peakCellRate  = 450 cells
   sustainedCellRate= 210 cells
   maximumBurstSize= 60 cells
   retryLimit    = 0
   localAddress  = 45613512123400002F000000010020480D527002
   remoteVpiVci  = 7.2
   addressToCall = 45613512123400002F000000010020480D008D00
```

**b** type:

**d -p -no nsta/* vgs ipmcon spvcap**

*The following list shows information for the IPmcon in slot 7. The actual command output lists information for all IPmcon sub-components of the NSTA VGS.*

```
Nsta/ 7 VGS IpMcon SpvcAp
   atmServiceCategory  = rtVariableBitRate
   peakCellRate        = 336000 cell/s
   sustainedCellRate   = 336000 cell/s
   maximumBurstSize    = 1 cells
   retryLimit    = 0
   localAddress  = 45613512123400002F000000010020480D517000
   remoteVpiVci  = 7.10
   addressToCall = 45613512123400002F000000010020480D008D00
```

**18** Confirm that the VSP VGS **addressToCall** (ATMIF UNI address) for **Ctrl/mediaGateway**, **Ctrl/signaling Gateway**, and **IpMcon** are identical.

***Note:*** If they are not identical, contact your next level of support.

**19** Check the ATMIF UNI addresses provisioned as primary and alternate by typing:

**l atmif/* uni addr/***

*A sample of the command output for the ATMIFs present on the PVG shelf follows:*

```
Atmif/141  Uni Addr/45613512123400002F000000010020480D008D00, primary

Atmif/151 Uni Addr/45613512123400002F000000010020480D008D00,alternate
Atmif/151 Uni Addr/45613512123400002F000000010020480D009700,primary
```

***Note:*** *Make sure the ATMIF UNI provisioning reflects a Primary and Alternate configuration for the same address for each VSP (Refer to your engineering guidelines for more information). If they do not match, contact your next level of support.*

***Use the PVG CLI to verify the PVG ATM (software) connection to the Passport 8600s***

**20** Determine which ATMIF the VSP VGS Ctrl/<mg,sg> and IPmcon ATMCON subcomponents point to as follows:

**a** display the VGS Ctrl/<mg,sg> ATMCON subcomponent for all VSPs by typing:

**d nsta/* vgs ctrl/* atmconn**

*A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.*

```
+=====+====+--------------------+------
|Nsta |Ctrl|      nextHop       |state
+=====+====+--------------------+------
|    7|mg  |AtmIf/141 Vcc/7.2 Ep|connec
|    7|sg  |AtmIf/141 Vcc/7.6 Ep|connec
```

***Note:*** *Make sure the AtmIf information for each VSP is identical to the primary interface information listed in* step 19*. If it is not contact your next level of support.*

**b** display the NSTA VGS IPmcon ATMCON subcomponent for the VSPs by typing:

**d nsta/* vgs ipmcon atmcon**

*A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.*

```
+=====+------------------+-------+--------
| Nsta|     nextHop      |state  |Response
+=====+------------------+-------+--------
|    7|AtmIf/141 Vcc/7.10|connec |
```

***Note:*** *Make sure the AtmIf information for each VSP is identical to the primary interface information listed in* step 19*. If is not identical, contact your next level of support.*

**21** Check the physical connections between each PVG ATM interface and their related Passport 8600s.

***Note:*** See step 15 for the Passport 8600 local route tables for the VSPs to be offloaded and verify the fiber connectivity between the PVGs and Passport 8600s. Refer to your engineering guidelines for additional information.

***Use the PVG CLI to disable the ATM interface to the Passport 8600 undergoing the software upgrade.***

**22** Select the next step as follows (refer to step 16):

| If all VSP VLANs for Passport 8600 Chassis N are | Do |
|---|---|
| OSPF (see Note) | step 29 |
| LOC | step 23 |

***Note:*** OSPF routing does not require manual maintenance to reduce the risk of call processing outage, as the link redundancy on PVGs fails over nearly immediately.

**23** Disable the ATM interface for each VSP as follows:

**a** identify the ATM interfaces and Sonet layer by typing:

**d -p -no lp/* sonet/* sts/0**

*A sample of the command output for the first Sonet interface on each card follows. The actual command output lists all Sonet interfaces on the PVG.*

```
Lp/14 Sonet/1 Sts/0
   applicationFramername     = Atmif/141
   txPathTrace               = ""
   expectedReceivePathTrace  = ""
   concatNumber              = 0
   customerIdentifier        = 0
   ifAdminStatus             = up
   ifIndex                   = 6
Lp/15 Sonet/1 Sts/0
   applicationFramername     = Atmif/151
   txPathTrace               = ""
   expectedReceivePathTrace  = ""
   concatNumber              = 0
   customerIdentifier        = 0
   ifAdminStatus             = up
   ifIndex                   = 472
```

**b** LOCK all Sonet layer connections related to the ATM ports connected to Passport 8600 Chassis N by typing:

**lock -force lp/<slot> sonet/<sonetif>**

where **<slot>** is the slot number of the Passport 8600, and **<sonetif>** is the Sonet interface on the ATM blade

***Note:*** This command results in Sonet layer ALARMS.

**c** record all locked Sonet interfaces

**24** Confirm the ATM (software) connection switch over is successful as follows:

**a** display the VGS Ctrl/<mg,sg> ATMCON subcomponent for the VSPs by typing:

**d nsta/* vgs ctrl/* atmconn**

*A sample of the command output for the switched ATMCON for the Ctrl/* to the ATMIF in slot 7 follows. This example shows a switchover from Atmlf/141 (see step 20) to Atmlf151.*

```
+=====+====+--------------------+------
|Nsta |Ctrl|      nextHop       |state
+=====+====+--------------------+------
|    7|mg  |AtmIf/151 Vcc/7.2 Ep|connec
|    7|sg  |AtmIf/151 Vcc/7.6 Ep|connec
```

**b** display the VGS IPmcon ATMCON subcomponent for the VSPs by typing:

**d nsta/* vgs ipmcon atmcon**

*A sample of the command output for the switched ATMCON for the IPmcon in slot 7 follows. This example shows a switchover from Atmlf/141 (see step 20) to Atmlf/151.*

```
+=====+-------------------+------+------
|Nsta |      nextHop      |state |Response
+=====+-------------------+------+------
|    7|AtmIf/151 Vcc/7.10 |connec|
```

***Use the Passport 8600 CLI to verify the IP route table for the offloaded VSP VLANs***

**25** Display the routing table for both Passport 8600s by typing:

**sho ip route info ip x.y.z**

where x.y.z is the IP Net address (see step 16)

***Note:*** The routing information under the PROT column heading should indicate OSPF for all VSP VLANs on Passport 8600 Chassis N.

**26** Select the next step as follows:

| If switchover of all VSPs is: | | Do |
|---|---|---|
| incomplete | (not all VSPs switched over) | step 23 |
| complete | (i.e., all switched over) | step 27 |

***Use the PVG CLI to re-enable all disabled ATM ports***

**27** Unlock all Sonet ports locked at step 23 by typing:

**unlock lp/<slot> sonet/<sonetif>**

where **<slot>** is the slot number of the Passport 8600, and **<sonetif>** is the Sonet interface on the ATM blade

Or unlock a four-port GigE card by typing:

**unlock lp/<slot> ethernet /<port>**

where **<port>** is the port number

***Use the Passport 8600 CLIs to check the IP route tables***

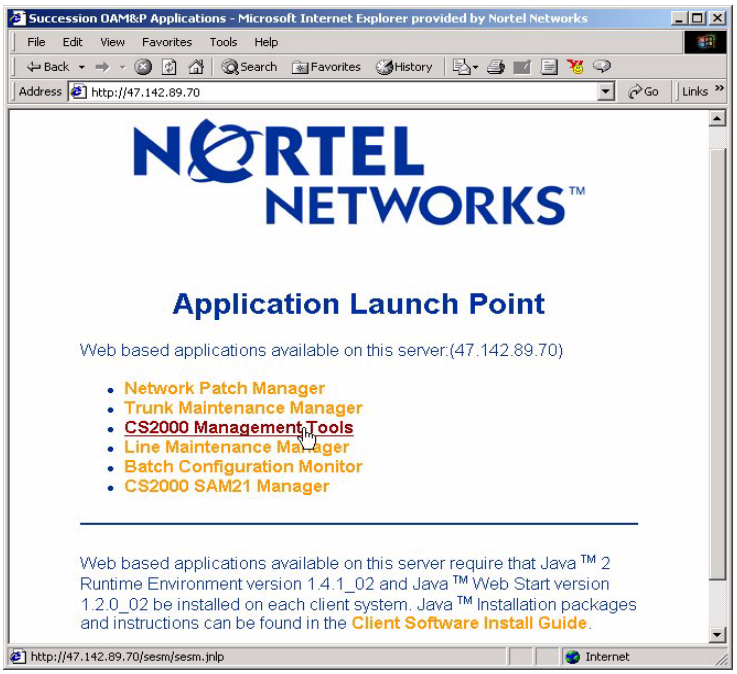
**28** Make sure all VSP VLANs remain OSPF on Passport 8600 Chassis N and LOC on Passport 8600 Chassis X by typing:

**sho ip route info ip 172.16.201**

*The routing information under the PROT column heading must indicate OSPF for all VSP VLANs on Passport 8600 Chassis N. If it does not contact your next level of support.*

***Use CS 2000 Management Tools to make the devices that subtend the slave Passport 8600 inactive:***

**29** Launch CS 2000 Management Tools from your web browser.




***Note 1:*** If Java Web Start is not installed on your workstation, you will be prompted to install Java Web Start.

***Note 2:*** If you are not using this Application Launch Point bypass this step go directly to you CS Management Tools GUI. Continue from step 31.

**30** Click on the CS2000 Management Tools link.

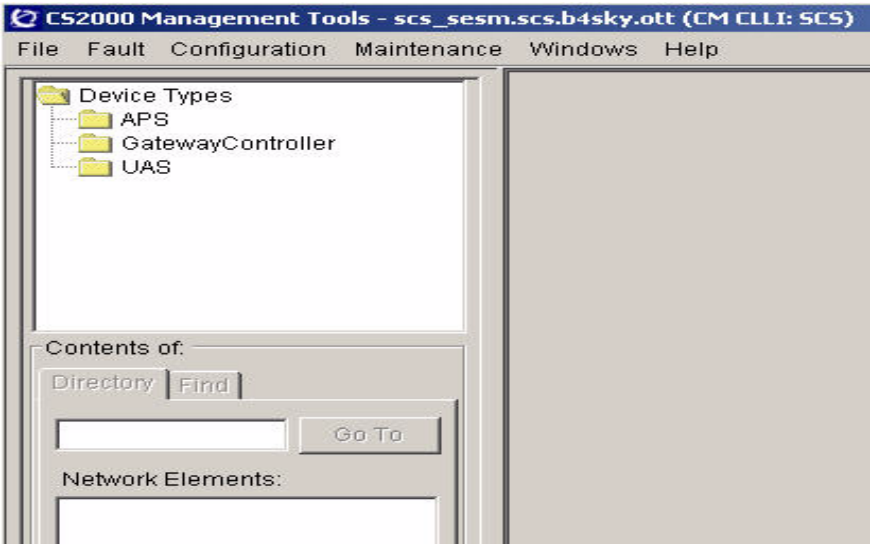
*The Login window appears.*



**31** Enter your Login Name. Press the tab key or click in the Password field and enter your Password, which is not echoed when input for security purposes. Click the Log In button.

***Note:*** Make sure to login with RWA privileges (see Instructions).

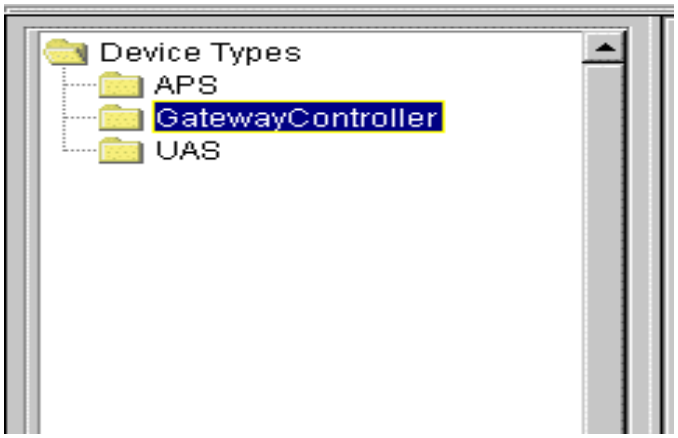
*The CS 2000 Management Tools GUI opens in a new browser window.*




**32** Activate the Maintenance information window for the GWCs as follows:

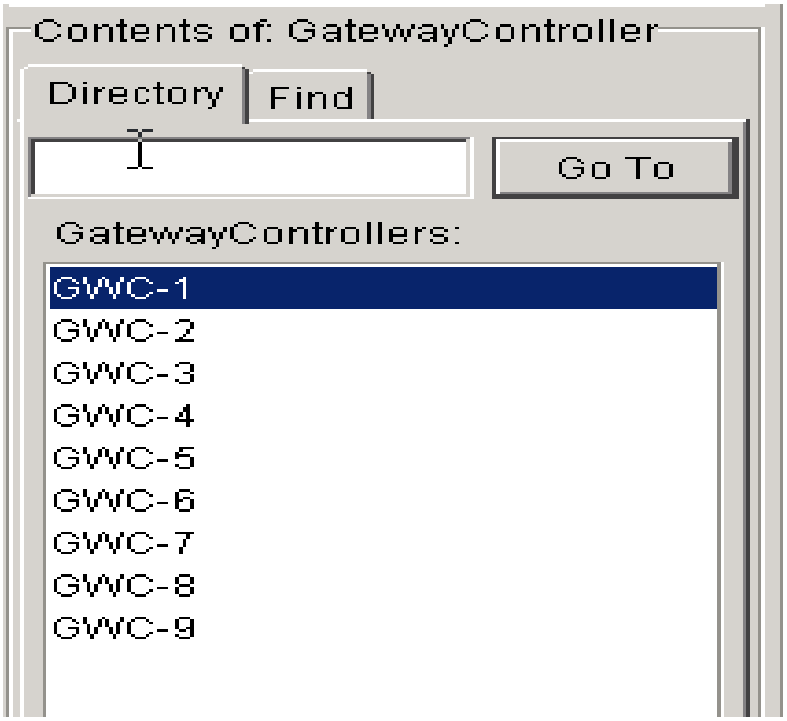
**a** select **GatewayController** from the **Device Types** field of the CS2000 Management Tools GUI

*The **GatewayController** folder in the **Device Types** field is highlighted.*



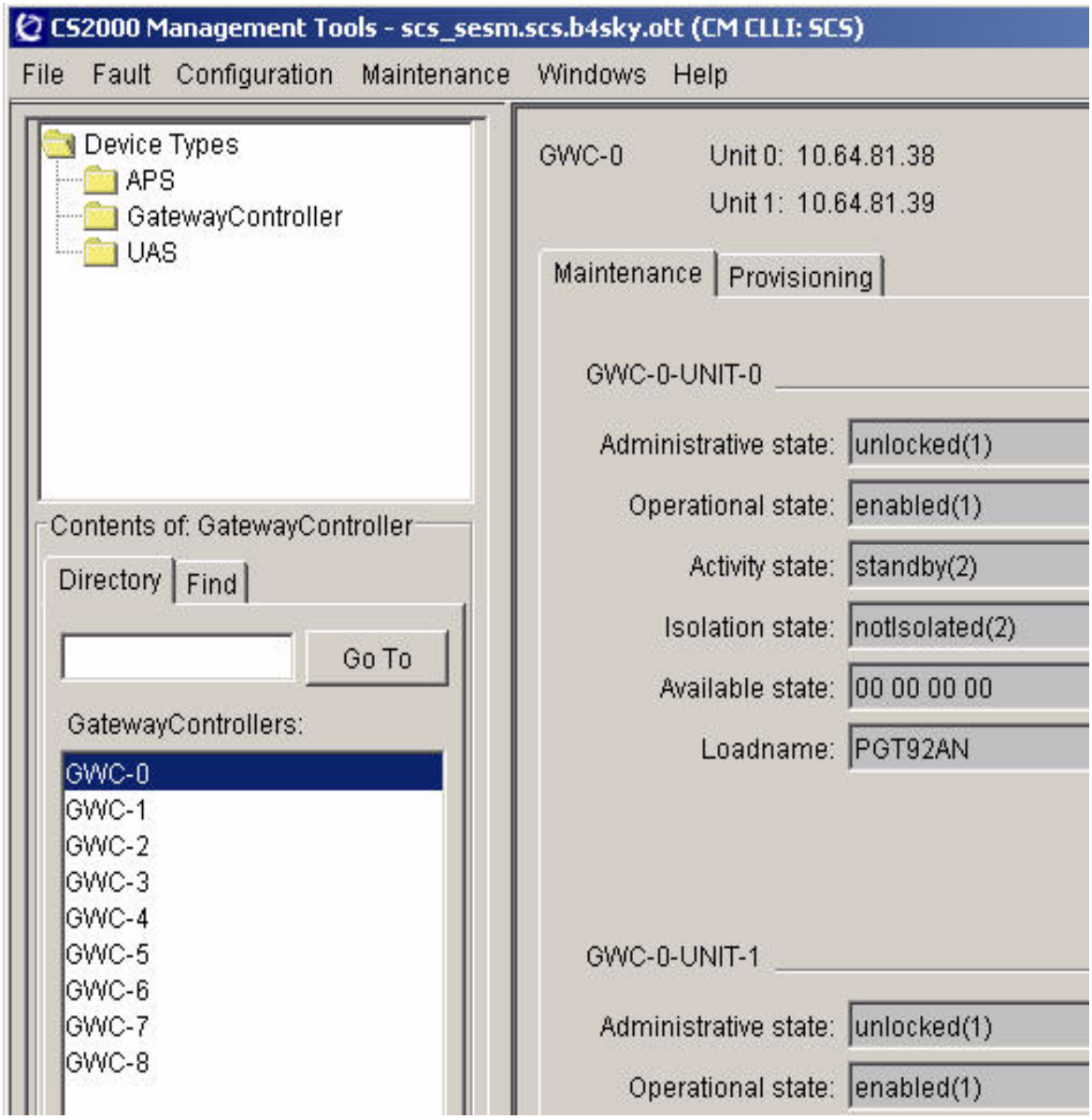
**b** select the **Directory** tab on the **Contents of: Gateway Controlle**r field

*The list of Gateway Controllers appears.*




**c** select the first GWC in the list displayed in the **Contents of: Gateway Controller** field

*The GWC is highlighted and the related Maintenance or Provisioning information, depending on the active tab, appears in the large right-hand field.*




**d** select the **Maintenance** tab to make sure the Maintenance information is active.

**33** Move all traffic onto Passport 8600 Chassis **X** (see note below) as follows:

***Note:*** This step makes the following assumptions:

- Unit 0 network elements subtend Passport 8600 Chassis 0
- Unit 1 network elements subtend Passport 8600 Chassis 1
- N = 0 and X = 1 for the first iteration of this procedure
- N = 1 and X = 0 for the second iteration of this procedure

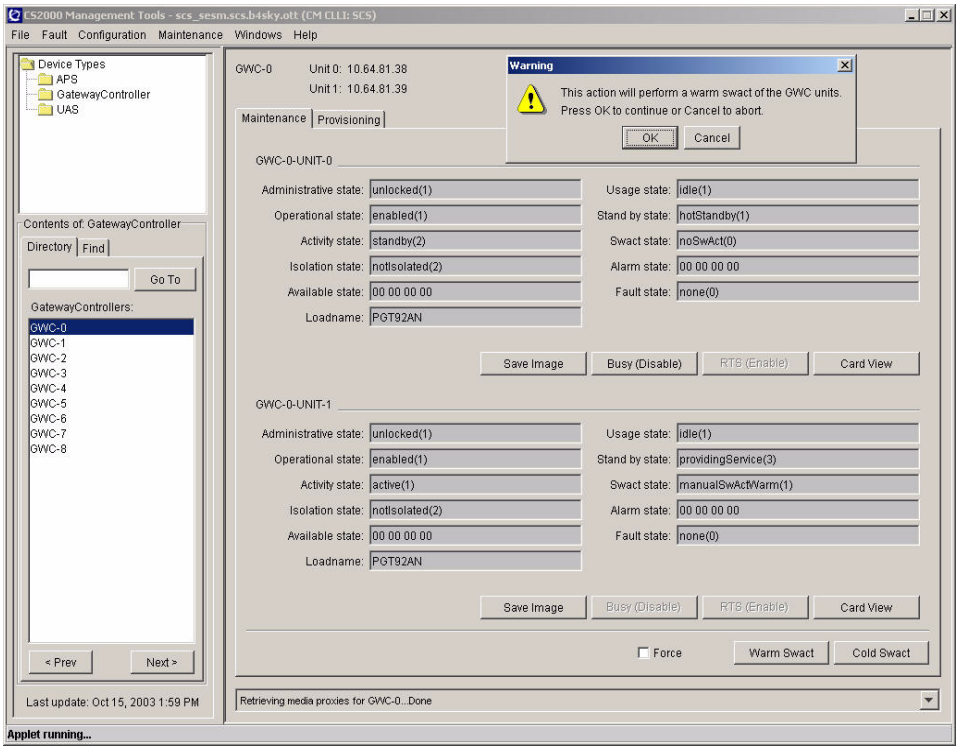
**a** check the **Activity State** field to determine which unit is **active** and which is **standby**

***Note:*** If the **Activity State** field for **GWC-#-Unit-#** is standby, instead of **inactive,** go to sub-step f.

**b** press **WarmSwact**

*A warning window appears.*

***Press OK to continue or Cancel to abort.***






**c** press OK and wait for the activity change to complete

*The selected GWC undergoes a change of activity. The change of activity can take a minute or two.*

**d** select the next step as follows

| If upgrading to SN07 from | Do |
|---|---|
| release *lower than* SN06 | step 33e |
| release SN06 (or greater) | step 33f |

**e** press **Busy (Disable)** button to manually busy the selected inactive GWC unit (the button is located at the bottom of the **Maintenance** information window).

***Note:*** A warning message may appear for GWC Units provisioned with MG9Ks that are set up with the ABI option. Check the Force option and re-press the **Busy (Disable)** button to complete this sub-step.

*The selected inactive unit of the GWC is set to the manually busy state.*

**f** select the next GWC in the list **Contents of: Gateway Controller** and repeat these sub-steps until the **Activity State** field for **Unit: N Status** is **inactive** for all GWCs.

**34** Select the next step as follows:

| If the Communication Server uses | Do |
|---|---|
| XA-Core and IOPs with ETHR packlets | step 35 |
| XA-Core and HIOPs or HCMICs | step 37 |
| Compact chassis | step 39 |

***Use the XA-Core MAP terminal to disable the Ethernet link with the inactive Passport 8600***

**35** Access the ETHR level of the MAP display by typing:

**>MAPCI;MTC;XAC;ETHR**

*The following is a sample MAP display for the ETHR level.*

```
 XAC      MS      IOD      Net       PM       CCS      Lns    Trks    Ext     APPL
  .       .       .        .         .        .        .      .       .       .

 ETHR                 Front:  111111111  Rear: 111111   SM     PE     IO      PKLT
 0 Quit              1234567890123456789  456789012345  .      .      .       ETHR M
 2                Sta   . ..-..-..-.- ..  ....------...  0      0      0       2
 3                Dep                      FF       FF
 4                Typ:                     **       **
 5                Slot: Side: Packlet:  Status: Port  Link
 6 Tst_            5    Rear   Lower             .     .
 7 Bsy_            6    Rear   Lower             .     .
 8 RTS_           13    Rear   Lower             .     .
 9                14    Rear   Lower             .     .
10 LoadFW_
11
12 Uneq_
13
14 Alarm_
15
16
17 Indicat_
18 Query_
```

**36** Refer to the figure and table below and disable the Ethernet link between the XA-Core and Chassis N of the Passport 8600 as follows:

**a** Type:

**bsy <slot1> r l link force**

Wait for the command to complete, then type

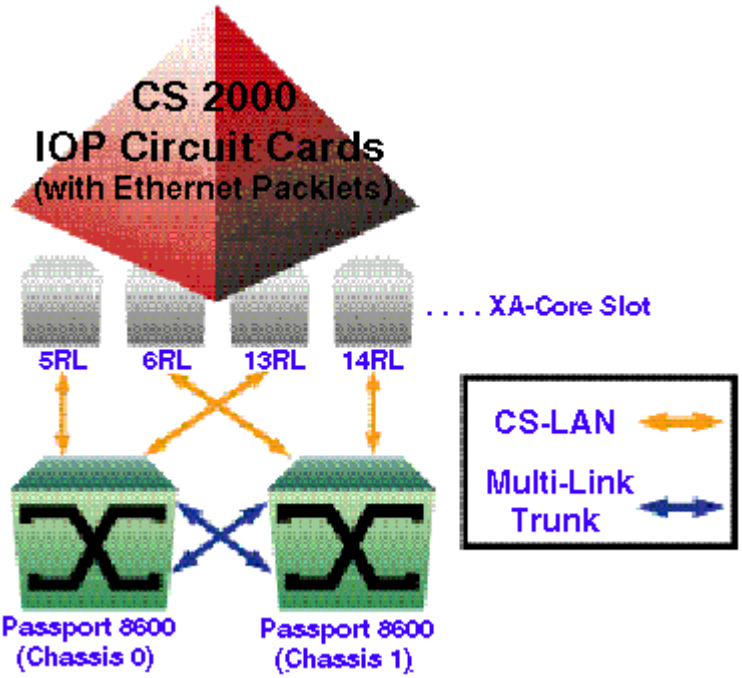
**bsy <slot2> r l link force**

where:
**l** (lower case letter “l”) refers to the lower packlet for the Ethernet link
**u** (lower case letter “u”) refers to the upper packlet for the Ethernet link

***Note 1:*** Executing these commands produces an alarm indicating that the port is down. Ignore this alarm.



***Note 2:*** Ensure that the XA-Core Ethernet ports are connected to chassis 0 and 1 of the Passport 8600 as in the following figure.




| IOP with ETHRs | N = 0 | N = 1 |
|---|---|---|
| **<slot1>** | 5 | 6 |
| **<slot2>** | 13 | 14 |

***Note:*** To prevent single points of failure, the figure and table assume the Ethernet connections for each link use IOP ETHR packlet pairs connected to separate power supplies (5 and 13 rear for Chassis 0, 6 and 14 rear for Chassis 1).

where:
5 is active and 6 is inactive, but only services 5,
13 is active and 14 is inactive, but only services 13

Therefore, an EIOP configuration can have a maximum of four connections; two to each Passport 8600 in any combination.

**b** Go to step 39.

**37** Access the ETHR level of the MAP display by typing:

**>MAPCI;MTC;XAC;ETHR**

*The following is a sample MAP display for the ETHR level.*

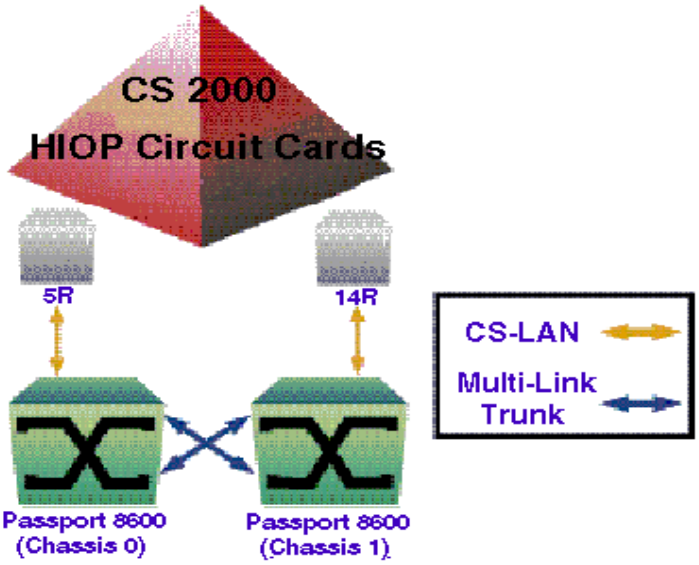
```
 XAC       MS      IOD       Net       PM       CCS      Lns      Trks      Ext      APPL
  .        .        .         .         .        .        .         .        .         .

 ETHR                 Front:   111111111  Rear: 111111  SM      PE      IO      PKLT
 0 Quit              123456789012345678  456789012345  SM M    .       HIOPfl  LINKfl
 2                Sta  . .......M--. -.    ..........    1       0       3       2
 3                Dep  F               F    FFF      F FF
 4                Typ:                       **       * *
 5                Slot: Side: Packlet:  Status: Port   Link
 6 Tst_            5     Rear                      .     .
 7 Bsy_            14    Rear                      .     .
 8 RTS_
 9
10 LoadFW_
11
12 Uneq_
13
14 Alarm_
15 Cntrs_
16
17 Indicat_
18 Query_
```

**38** Refer to the figure and table below, and disable the XA-Core to Passport 8600 Chassis N Ethernet link by typing:

**bsy <slot> r link force**

***Note:*** Executing this commands produces an alarm indicating that the port is down. Ignore this alarm.




| HIOPs/HCMICs | N = 0 | N = 1 |
|---|---|---|
| <slot> | 5 | 14 |

***Note:*** In the previous configuration, one HIOP is connected to each Passport 8600.

**39** Select the next step as follows.

| If upgrading to SN07 from | Do |
|---|---|
| release lower than SN06 | step 40 |
| release SN06 (or greater) | step 41d |

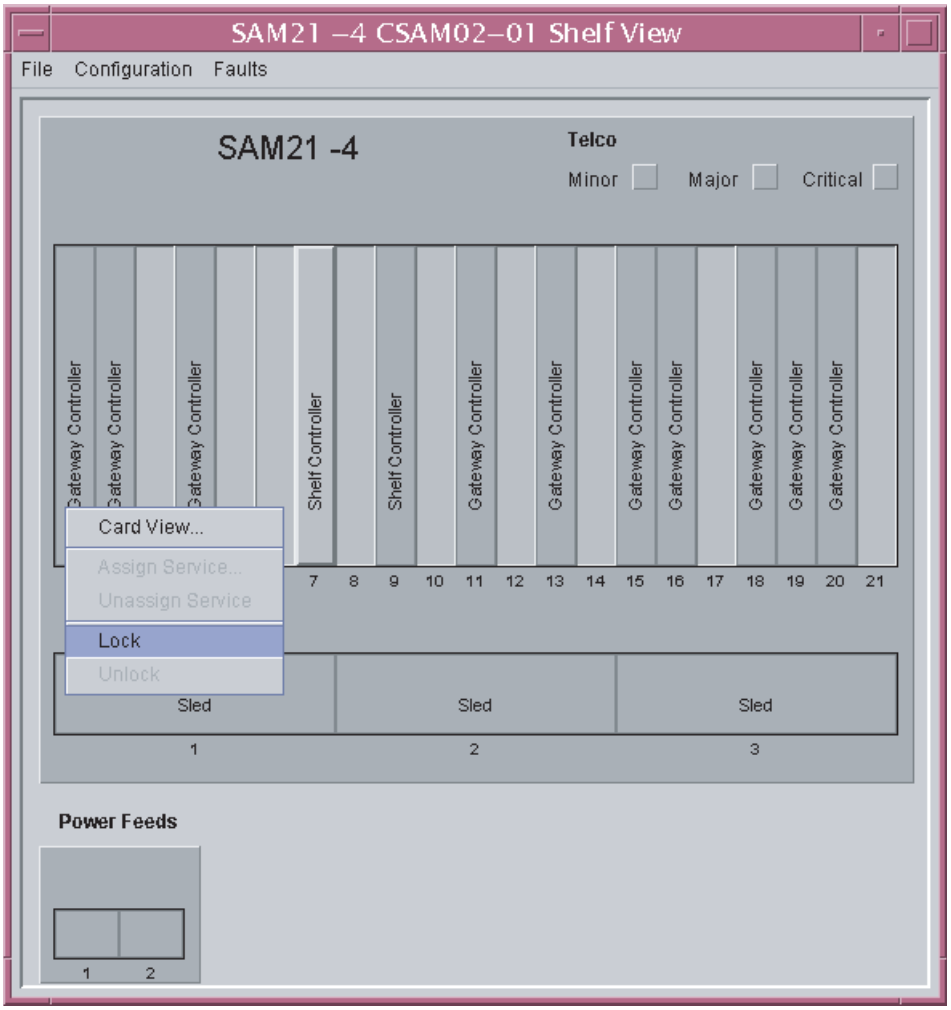
***Use the SAM21 Element Manager to lock the inactive GWCs:***

**40** Launch the SAM21EM client.

*The SAM21 EM GUI appears.*

**41** Lock the inactive GWCs as follows:

**a** from the SAM21 EM shelf view, right click on each **standby** Gateway Controller Unit (see step 33, sub-step a) in turn




**b** select **Lock** from the drop-down menu that appears.

*This sets the **standby** GWC Units to Locked.*

***Note:** If the SAM21 EM displays a warning message stating the GWC Unit is in service, abort the lock, go to step 33, and make sure the GWC Unit is inactive. If the warning persists contact your next level of support.*

**c** repeat sub-step a and sub-step b until all **standby** Gateway Controller Units are locked.

**d** select the next step as follows:

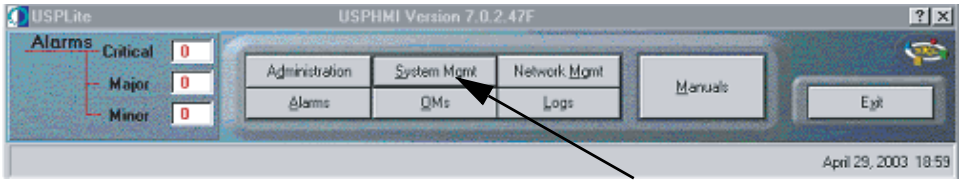
| If you have | Do |
|---|---|
| a 3PC with a USP Compact | step 42 |
| a 3PC with a standard USP | step 59 |
| an XA-Core | step 67 |

***Use the USP Compact (USPc) GUI to lock the slave USPc blade:***

**42** Refer to your network diagram and determine the USPc blade to Passport 8600 connectivity as follows:

***Note:*** The USPc slave blade must connect to Chassis N of the Passport 8600, master blade to Chassis X (see step 43).

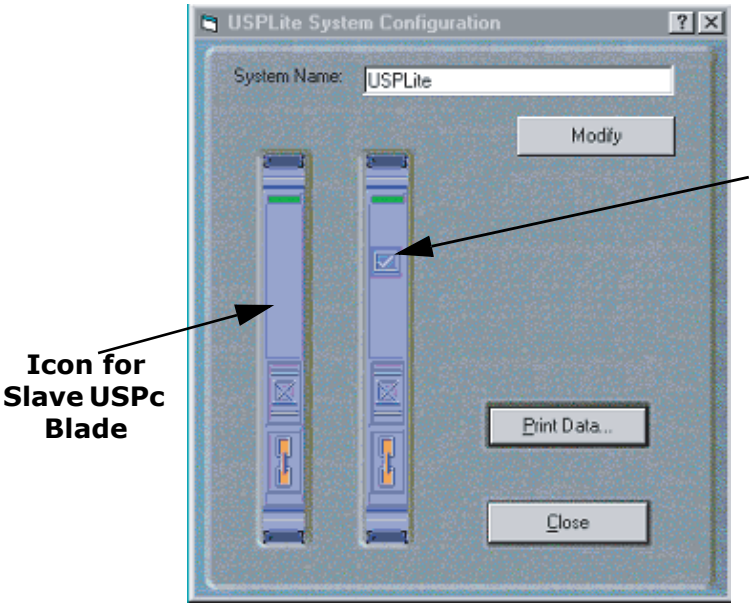
**a** Launch the USPc GUI.




**System Management Button**

**b** Click the System Management button on the USPc GUI Main Toolbar to start the System Configuration GUI

*The System Configuration window appears.*




**Icon for Master USPc Blade (indicated by checkmark)**

**Icon for Slave USPc Blade**

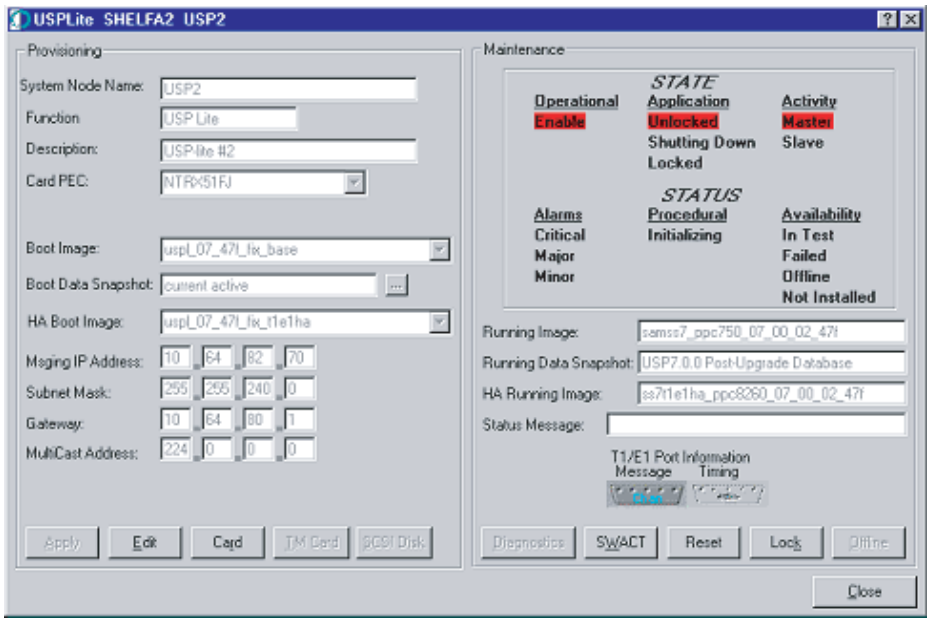
**c** Determine the master/slave status for each USPc blade icon in the System Configuration window.

***Note:*** Both USPc blades carry traffic and are inservice. The blade icon with a checkmark identifies the master USPc. The icon with no checkmark identifies the slave USPc.

**43** Make slave USPc blade subtend Passport 8600 Chassis N by:

**a** clicking on the USPc blade icon connected to the slave Passport 8600 router to start the GUI for Shelf management

*The GUI for the selected USPc blade appears.*

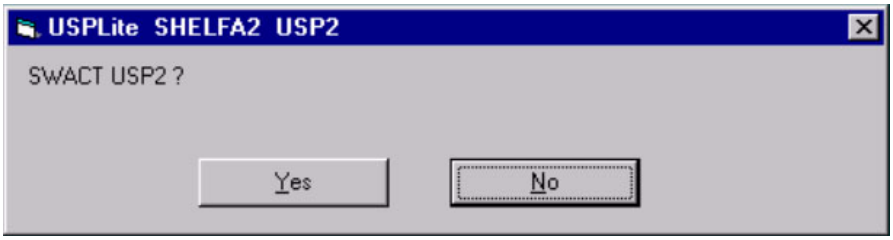



**b** check the *STATE* information for the slave USPc blade connected to the slave Passport 8600 router and continue as follows:

| If the USPc blade STATE activity is: | Do |
|---|---|
| Master | step 44 |
| Slave | step 46 |

**44** Click the SWACT button to change the USPc blade *STATE* Activity to **Slave**.

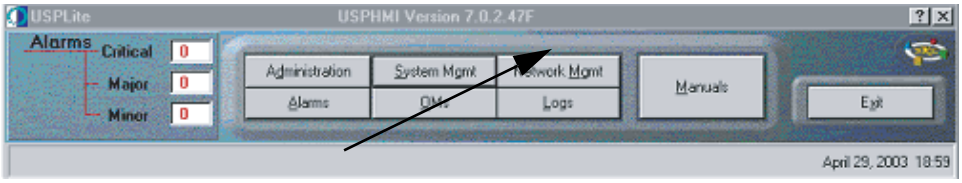
*Press Yes in the SWACT confirmation window to continue.*




**45** Go to step 43.

***Note:*** Return to step 43 to confirm the change in *STATE* Activity to **Slave**. If the *STATE* Activity did not change and you return to this step in the same iteration (same value for N), contact your next level of support.

**46** Click the Network Management button on the USPc GUI Main Toolbar.

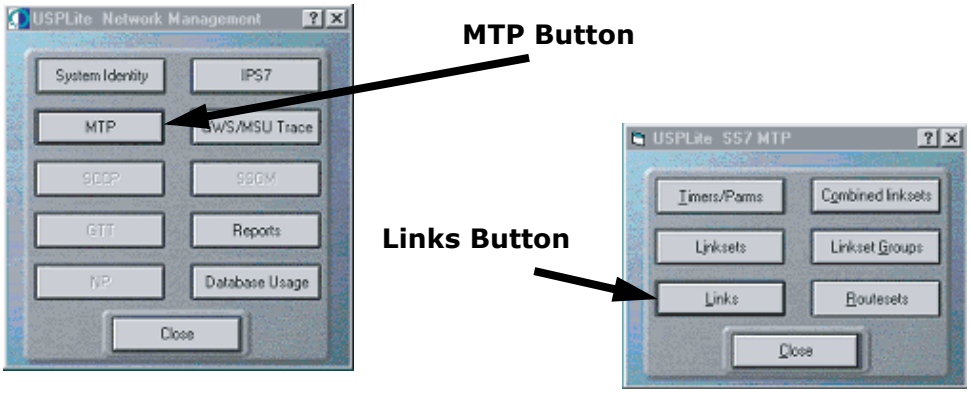



**Network Management**

*The Network Configuration window appears.*

**47** Click the MTP button in the Network Management window.

*The SS7 MTP window appears (see figure below).*

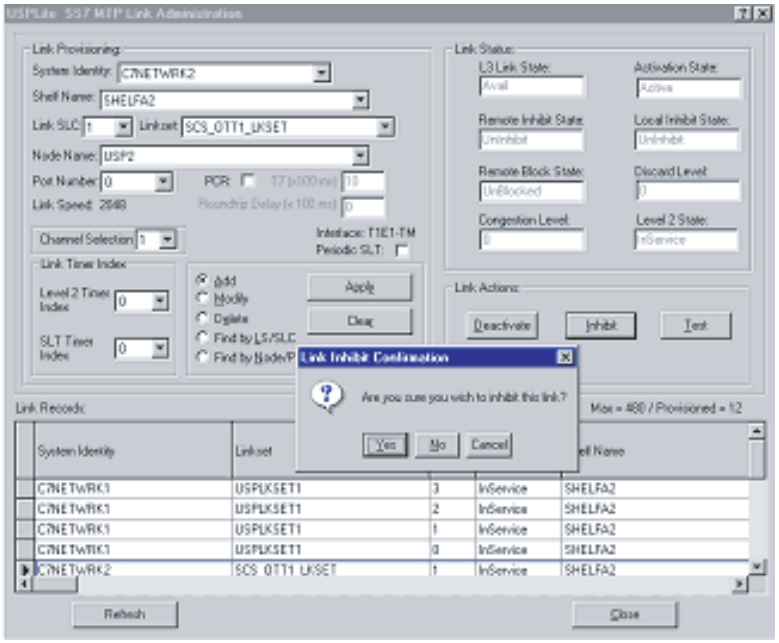



**48** Click the Links button in the SS7 MTP window.

*The Link Management window appears.*

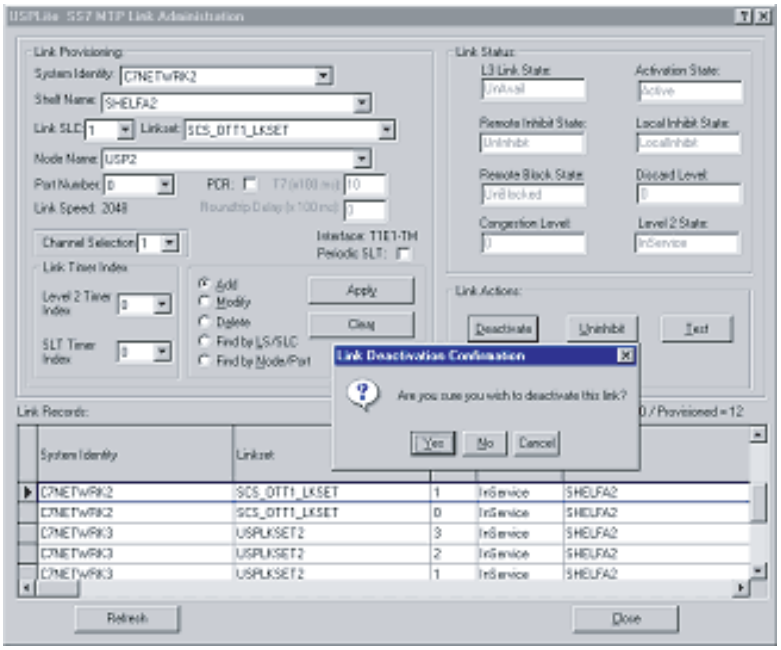
**49** Click the Inhibit button for the slave USPc links.

***Note:*** At least one linkset must be available on the master.



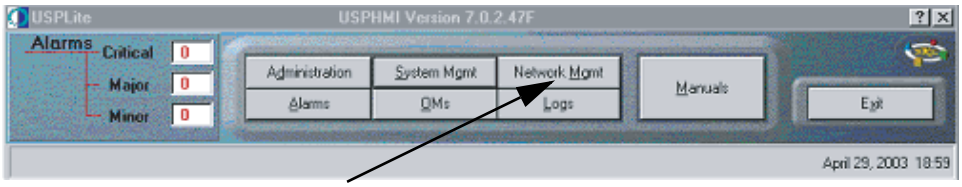

*A confirmation window appears. Select OK to continue.*

**50** Click the Deactivate button for the slave USPc links.




*A confirmation window appears. Select OK to continue.*

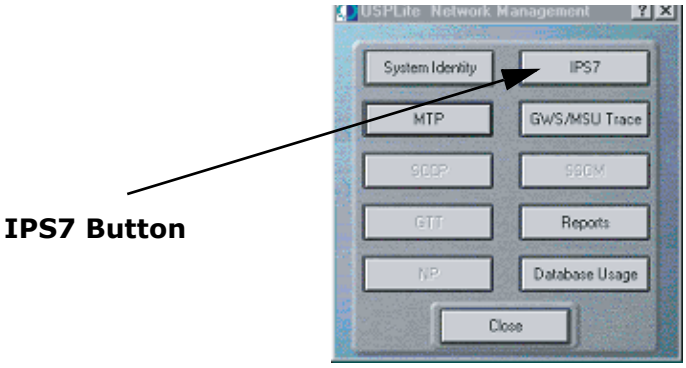
**51** Click the Network Management button on the Main Toolbar.




**Network Management Button**

*The Network Configuration window appears.*

**52** Click the ISP7 button in the Network Management window.



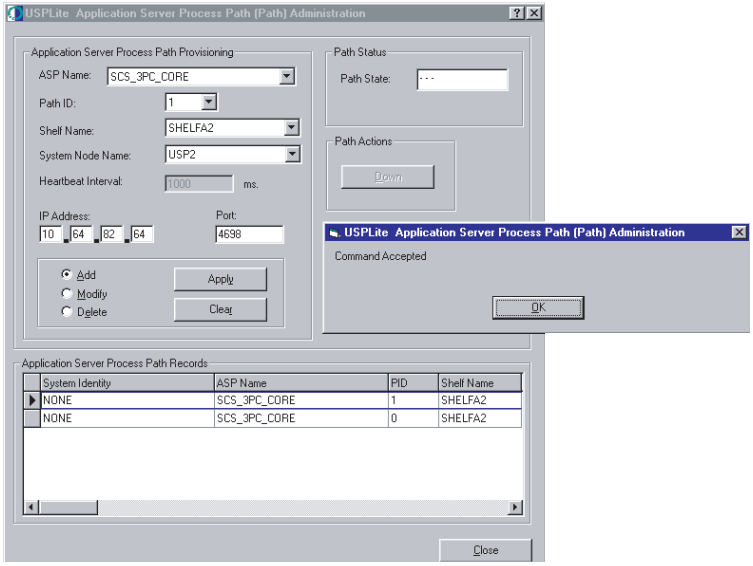

**IPS7 Button**

**53** Click on the ASP Paths button in the USP Compact ISP7 window.

*The USP Compact Application Server Process Path window appears.*

**54** Click the Path Actions button for all Application Server Process (ASP) paths on the slave USPc.

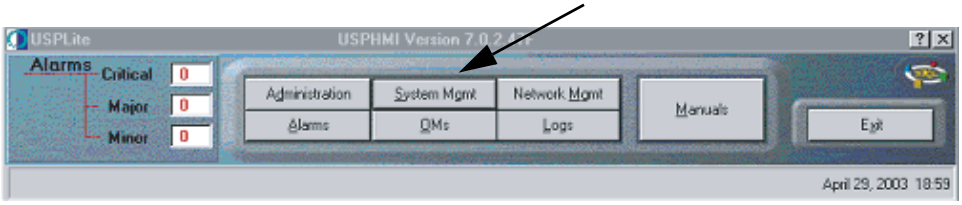
***Note:*** At least one ASP path must be available on the master.



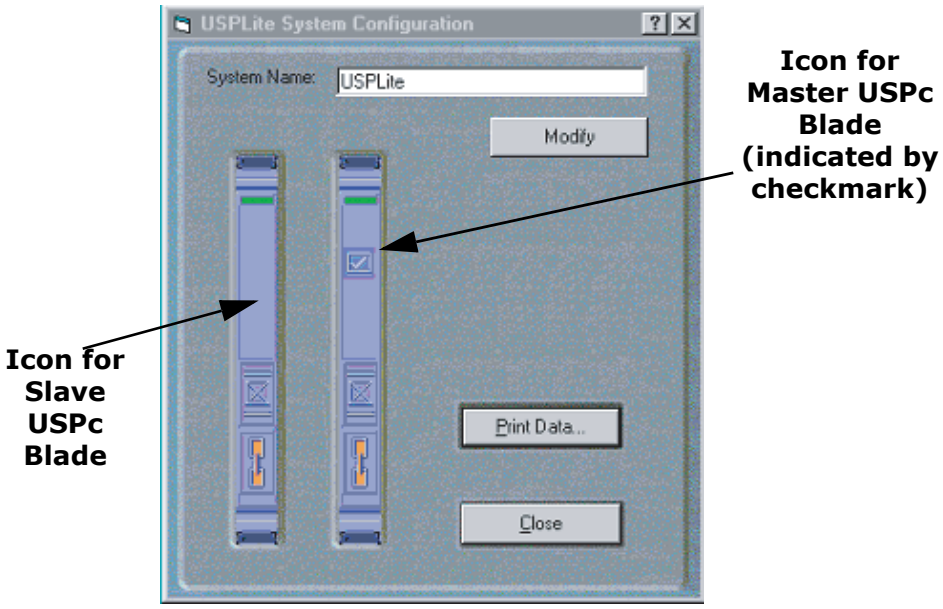

*Click OK in the Path Deactivation confirmation window to continue.*

**55** Click the System Management button on the USPc GUI Main Toolbar to start the System Configuration GUI.

**System Management Button**



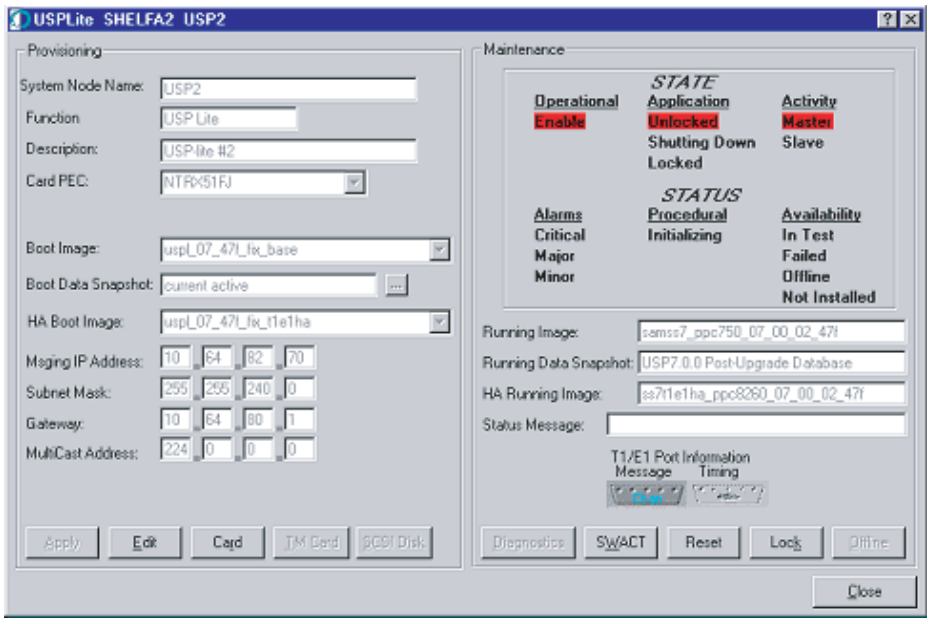

*The System Configuration window appears.*




**56** Click on the icon for the slave USPc blade.

***Note:*** Both USPc blades carry traffic and are inservice. The blade icon with no checkmark identifies the slave USPc. The blade icon with a checkmark is the master USPc.

*The GUI for the slave USPc Shelf appears.*




**57** Click Lock to manually busy the slave USPc blade.

*A confirmation window appears. Select OK to continue.*

***Use the SAM21 EM to lock the inactive USPc blade and disable the USPc GUI:***

**58** Lock the inactive USPc blade (disable the USPc GUI) as follows:

**a** activate the GUI for CALL-AGENT-N.

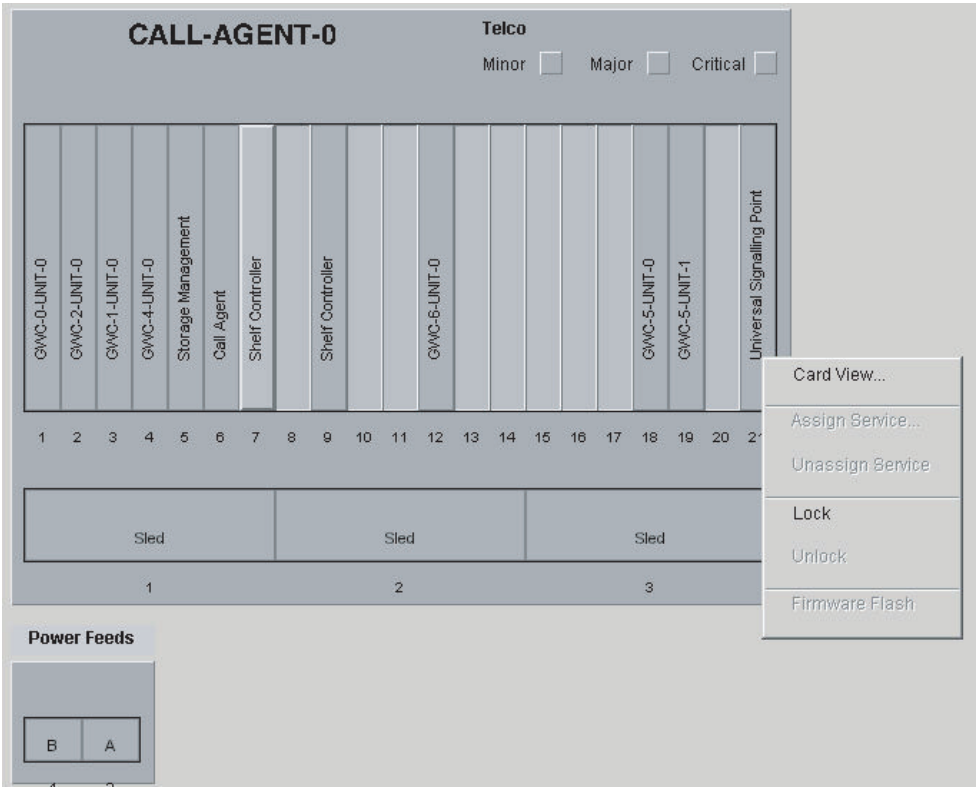
*The GUI for CALL-AGENT-N appears.*

***Note 1:*** *The Universal Signaling Point blade icon must not appear to be raised. A raised icon indicates the blade is active. If the icon appears to be raised consider the recommendation at* step 1 *(unit 0s subtend Passport 8600 Chassis 0, and unit 1s subtend Chassis 1).*

***Note 2:*** *To verify that the Universal Signaling Point blade on the GUI for CALL-AGENT-N is inactive, right-click on the blade icon and select* ***Card View****. From the card view* ***Provisioning*** *tab confirm the status is inactive.*

**b** right-click the Universal Signaling Point icon.

*A sub-window appe.ars with the* ***Card View*** *and* ***Lock*** *selections enabled.*



**c** click the **Lock** option.

***Before rebooting the Passport 8600 that connects the support operating system (SOS) to one of the STORM disks***

**59** Select the next step as follows.

| If | Do |
|---|---|
| the volumes on any STORM disk (for example, sd01) are actively mounted in Device Independent Recording Package (DIRP) | step 60 |
| the volumes on the STORM disk are not actively mounted DIRP, or use a STORM IA configuration | step 67 |

***Note 1:*** Loss of network connectivity between SOS, the call processing application, and the active STORM disk can cause some or all DIRP volumes to be marked “INERROR,” resulting in permanent loss of data.

***Note 2:*** Refer to your network diagram and determine the STORM blade-to-Passport 8600 connectivity as follows.

Volumes prefixed with sd00 reside on STORM device 0, which *must be* connected to Passport 8600 Chassis X. Volumes prefixed with sd01 reside on STORM device 1, which *must be* connected to Passport 8600 Chassis N. Verify this setup in your CS 2000 - Compact. Adjust this procedure, if necessary.

For the first iteration (where N=0), all actions are performed for volumes prefixed with sd01. For the second iteration (where N=1), all actions are performed for volumes prefixed with sd00.

**60** From the Core MAP command line, list all available DIRP subsystems (field SYSSNAME in table DIRPSSYS) for the Core.

**>table dirpssys; lis all**

**61** Access the DIRP level in SOS by typing:

**>mapci nodisp;mtc;iod;dirp**

**62** Query all volumes associated with the subsystem.

**>query <subsystem> all**

where:
**<subsystem>** is from the list of available subsystems executed in step 60.

*The following figure shows an example of this command for the dlog subsystem with an active file highlighted.*

```
>query dlog all
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
DLOG      1     1       3      7  NONE     ***YES***

REGULAR
FILE(S)   STATE VOLUME   RECCOUNT BLOCK E  V V_B VLID FNUM FRN#
ACTIVE    AVAIL SD01DLG1         1     1 0 71 NO  8448 000D 1014
STANDBY1 AVAIL SD00DLG1          0     0 0 70 NO  8408 0015 3012

PARALLEL
FILE               STATE VOLUME   BLOCK E  V V_B VLID FNUM FRN#
                    NONE

REGULAR VOLUME(S)
VOL# VOLNAME  STATE          IOC CRD PORT VOL FSEG ROOM VLID FILES
  70 SD00DLG1 READY          N/A N/A N/A    8   10   11 8408 S1
  71 SD01DLG1 READY          N/A N/A N/A    8  112  116 8448 A

REGULAR SPACE
VOL# VOLNAME  STATE          SEGS   EXP UNEXP TOTAL
  70 SD00DLG1 READY            10     1     0    11
  71 SD01DLG1 READY           112     4     0   116
```

**63** Only rotate the active volume for each subsystem if it is located on a STORM blade connected to the router being upgraded for this iteration. Manually rotate all subsystems until the active files reside on STORM volumes connected to the Passport 8600 chassis that is not to be upgraded for this iteration.

***Note:*** To minimize the risk, rotate and demount the AMA subsystem last. Then restore the AMA subsystem first.

**>rotate <subsystem> <variable>**

where:
**<variable>** is *regular*, *paralel*, or both (Enter *regular* to rotate regular volumes. Enter *paralel* to rotate parallel volumes. Enter *both* to rotate both volumes.)

***Note:*** Parallel is intentionally misspelled.

*The following figure shows example of input for variable regular.*

```
>rotate dlog REGULAR
ACTIVE FILE WILL BE CLOSED IF POSSIBLE (ROTACLOS).
SENDING REQUEST TO SUBSYSTEM
Please confirm ("YES", "Y", "NO", or "N"):
>y
REQUEST SENT TO SUBSYSTEM, CHECK DIRP LOG FOR DETAILS
```

**64** Repeat step 62 to ensure that all volumes have been successfully rotated.

**65** Demount all DIRP volumes connected to the Passport 8600 chassis that is to be upgraded.

**>dmnt <subsystem> <volume> <variable>**

where:
**<volume>** is the volume on the device (prefixed with sd01 for iteration N=0, and prefixed with sd00 for iteration N=1)

**<variable>** is *regular* or *paralel*

***Note 1:*** The **<variable>** parameter is not required when mounting and demounting regular DIRP volumes.

***Note 2:*** Nortel Networks recommends recording all subsystems, volume, and variable information for each volume being demounted in this step.

**66** Busy all STORM volumes connected to the Passport 8600 chassis to be upgraded.

**>diskadm sdXX; bsy all**

where:
**XX**=01 for iteration N=0
**XX**=00 for iteration N=1

***Note 1:*** Nortel Networks does not recommend using option *bsy all force*.

***Note 2:*** Issuing a bsy all command affects all volumes serviced by that STORM blade, not just those used by DIRP.

**67** Select the next step as follows:

| If the CS-LAN is used with: | Do |
|---|---|
| an ATM-based solution | step 68 |
| an IP-based solution | step 70 |

***Use the SAM21 EM to lock the inactive Shelf Controller blade:***

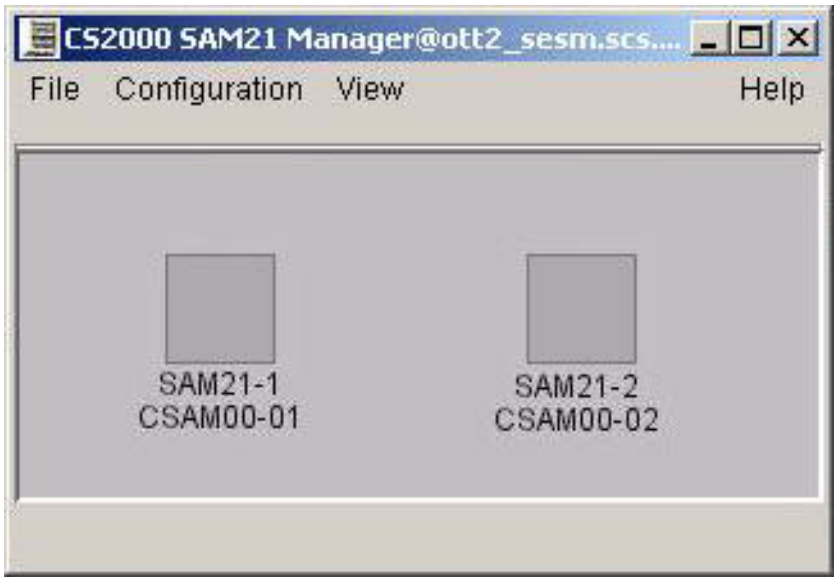
**68** Confirm that Shelf Controller (SC) blade connectivity complies with the recommendation at step 1 for all SAM21 shelves.

***Note:*** The recommendation at step 1 requires SC unit 0s (in slot 7) subtend Passport 8600 Chassis 0, and SC unit 1s (in slot 9) subtend Passport 8600 Chassis 1. If the SAM21 shelf varies from this recommendation, adjust this procedure accordingly.

**69** Lock the inactive SAM21 SC blade for each SAM21 shelf in turn as follows:

**a** launch the SAM21 Element Manager

*The SAM21 EM GUI appears with the related shelf icons displayed.*

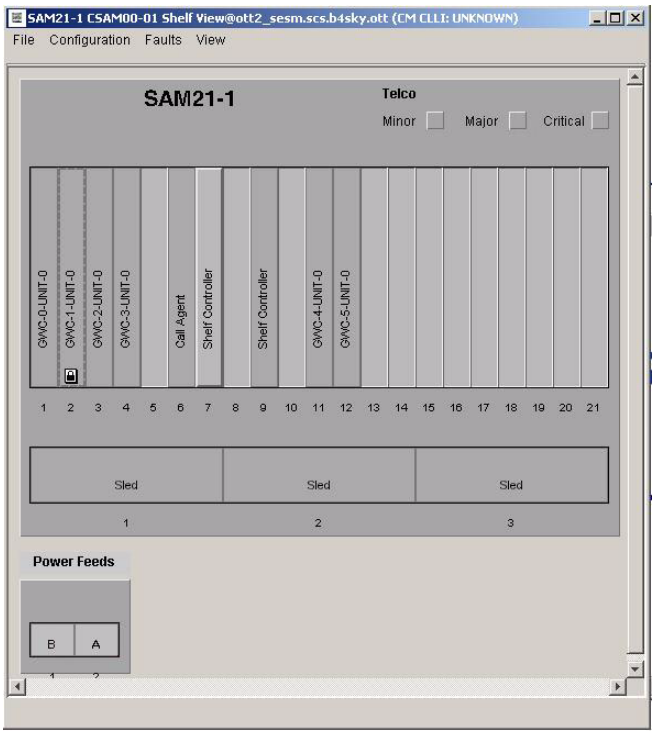



**b** use the cursor to select the shelf icon for the first SAM21 shelf displayed

**Example**
The first shelf in the figure above is SAM21-1 CSAM00-01

**c** double-click the selected shelf icon.

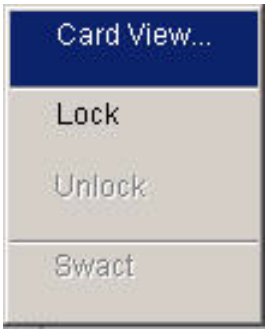
*The SAM21 EM shelf view for the selected shelf appears.*




**d** right-click on the icon for the SC blade associated with the inactive Passport 8600 Chassis.

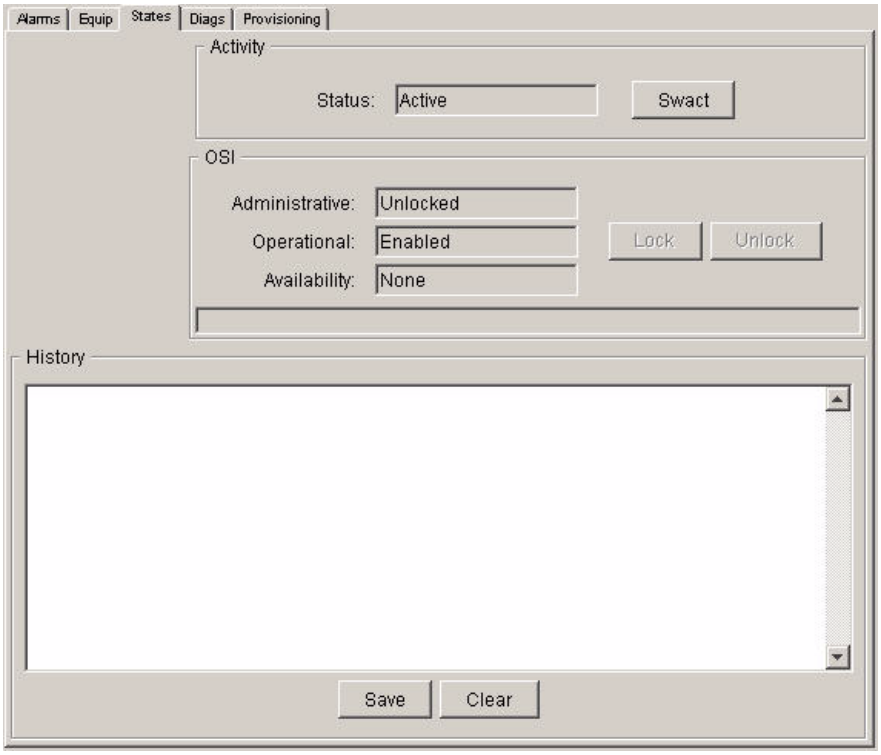
***Note:*** The SC blade in slot 7 subtends Passport 8600 Chassis 0, slot 9 subtends Chassis 1 (see note to step 68)

*A sub-window appears with the **Card View** and **Lock** selections enabled.*




**e** click **Card View.**

*The SC Card View appears.*




**f** select the **State** tab and make sure the SC is inactive.

*If the SC state is **Active**, press the **SWACT** button to change the activity status to **Inactive**.*

**g** close the **Card View**.

*The **Shelf View** reappears.*

**h** right-click on the icon for the inactive SC blade.

*A sub-window appears with the **Card View** and **Lock** selections enabled.*

**i** click **Lock**.

*The inactive SC blade is locked.*

> ***Note:** This prevents an automatic change of activity from occurring. An automatic SWACT at this point could cause a system outage.*

**j** close the **Shelf View**.

*The SAM21 EM view reappears.*

**k** select the next step as follows

| If the (inactive) SC cards are | Do |
|---|---|
| locked on all SAM21 shelves | step 70 |
| not all locked | select the next SAM21 Shelf and go to sub-step c |

***Note:*** Repeat sub-step c through sub-step j until the inactive SCs are all locked.

***Use the Passport 8600 CLI to make sure devices subtending the Passport 8600 Chassis X are active (Chassis N devices inactive):***

**70** Recheck the address resolution protocol information by typing:

**sho ip arp info**

*The IP ARP file appears. Verify topology complies with the recommendation at step 1. Refer to step 3, sub-step c for information on checking the IP ARP file.*

***Note:*** *If any units do not meet this requirement, redo step 33. If the problem persists, contact your next level of support.*

***Use the Passport 8600 CLI to upgrade the software load on Passport 8600 Chassis N:***

**71** Access the Passport 8600s using the serial (console) port.

***Note 1:*** Use either a serial connection and terminal program from an attached PC or TELNET session to an appropriately configured IP address on a terminal server.

***Note 2:*** If access fails, verify network topology, IP address, and Passport 8600 power supply then try again. If the problem persists contact your next level of support.

**72**

**ATTENTION**

Refer to section Text conventions on page 59 for brief definitions and examples of the software filenames used in the following command lines.

Select the next step as follows

| If your CS-LAN: | Do |
|---|---|
| is a dual CPU configuration | step 73 |
| is a single CPU configuration | step 77 |

**73** For a Passport 8600 with a dual-CPU configuration, TFTP the upgrade software to the flash directory on the master CPU. Then copy it to the standby CPU.

In the following sub-steps, both commands must be executed on the master CPU.

***Note:*** The Passport 8600 automatically copies files to the PCMCIA card using the same name as the current file. Therefore, it is not necessary to enter a new filename for the backup version of this file in step 73a through step 73e.

**a** TFTP the new software image file. Type:

**copy <a.b.c.d>:/swd/pp8600/XXX/<newload> /flash/**

**copy /flash/<newload> peer:/flash/**

where **<a.b.c.d>** is the IP address of the TFTP server, and **<newload>** is the name of the new software image file

**b** TFTP the new boot monitor image file. Type:

**copy <a.b.c.d>:/swd/pp8600/XXX/<newboot> /flash/**

**copy /flash/<newboot> peer:/flash/**

where **<newboot>** is the name of the new boot monitor image file

*The boot flash image and software image is backed up to the PCMCIA card on the Passport 8600 Chassis N.*

***Note 1:*** *If either file transfer fails, verify TFTP server IP address and connectivity with Passport 8600 Chassis N. Confirm Passport 8600 TFTP flag is set to true by typing:*
***config bootconfig flags info***

*If the **tftpd** flag is set to false, reset the flag to true by typing:*
***config bootconfig flags tftpd true***

*Confirm the flag is now set to true, then retry the transfer. If the problem persists, contact your next level of support.*

***Note 2:*** *If the transfer completes but the file is corrupted, verify original file and PCMCIA card and transfer the file again. If the problem persists, contact your next level of support.*

***Note 3:*** *Compare file parameters such as file size to check for possible corruption.*

**c** ***Only*** if Chassis N of Passport 8600 uses an ATM blade, TFTP the ATM Flash image to the Flash card on the Passport 8600 Chassis N by typing (otherwise go to step 74.)

**copy <a.b.c.d>:/swd/pp8600/XXX/<newATM> /flash/**

**copy /flash/<newATM> peer:/flash/**

where **<newATM>** is the name of the new ATM file

***Note:*** Notes 1 and 2 from step 73, sub-step b apply.

**d** If the Passport 8600 uses DES, TFTP the file. Type:

**copy <a.b.c.d>:/swd/pp8600/XXX/<newDES> /flash/**

**copy /flash/<newDES> peer:/flash/**

where **<newDES>** is the name of the new DES file

**e** If the Passport 8600 uses 3DES, TFTP the file. Type:

**copy <a.b.c.d>:/swd/pp8600/XXX/<new3DES> /flash/**

**copy /flash/<new3DES> peer:/flash/**

where **<new3DES>** is the name of the new 3DES file

**74** Verify that the software has been copied to the master and standby CPUs.

**a** In the master CPU session, type

**dir**

**b** In the standby CPU session, type

**dir**

**75** Prepare to boot both CPUs.

***Note:*** There is an intentional space between **image-file** and **/flash** in the syntax for substeps a and b.

**a** type:

**config bootconfig choice primary image-file /flash/<newload>**

**b** type:

**config bootconfig choice secondary image-file /flash/<oldload>**

**c**

**WARNING**

Disable the flag setting before saving the bootconfig file. Failure to observe this step can result in loss of configuration.

**config bootconfig flags verify-config false**

**d** verify the new software image file by typing:

**sho boot config**

***Note:*** Ensure that the result indicates the primary image file is **<newload>**.

**e** save the bootconfig file by typing:

**sav bootconfig**

***Note:*** If the switch response does not show the file being saved to the standby CPU, copy the files to the standby CPU by typing:

**copy /flash/boot.cfg peer:/flash/boot.cfg**

*This prepares Passport 8600 Chassis N to reboot.*

**76**

**WARNING**

When booting the dual CPUs, do ***not*** wait for the standby CPU to complete the boot process before booting the master CPU. Waiting results in different images on each CPU. While in the high-availability (HA) mode, booting the master CPU and the standby CPU with different software images can crash the standby CPU.

Boot both CPUs in rapid sequential order, booting the standby CPU first and ***immediately*** booting the master CPU next.

**a** Boot the standby CPU. In the standby CPU session, type

**boot /flash/<newboot>**

where **<newboot>** is the name for the new monitor image file

**b** Immediately boot the master CPU. In the master CPU session, type

**boot /flash/<newboot>**

**ATTENTION**

This command upgrades the primary-image file (including the ATM-image if present) and boot monitor at the same time.

**ATTENTION**

Do not interrupt the reboot process. The CPU card can be damaged if the reboot is interrupted incorrectly.

Go to step 80.

**77** For a Passport 8600 with a single CPU configuration, TFTP upgrade software to the flash on Chassis N of the Passport 8600, as follows:

**a** type:

**copy <a.b.c.d>:/swd/pp8600/XXX/<newload> /flash/**

where **<a.b.c.d>** is the IP address of the TFTP server, and **<newload>** is the name of the new software image file

***Note:*** The Passport 8600 automatically copies files to the PCMCIA card using the same name as the current file. Therefore, it is not necessary to enter a new filename in the command for the backup version of the files in step 77b through step 77e.

**b** type:

**copy <a.b.c.d>:/swd/pp8600/XXX/<newboot> /flash/**

where **<newboot>** is the name of the new boot monitor image file

*The boot flash image and software image is backed up to the PCMCIA card on the Passport 8600 Chassis N.*

***Note 1:*** *If either file transfer fails, verify TFTP server IP address and connectivity with Passport 8600 Chassis N. Confirm Passport 8600 TFTP flag is set to true by typing:*
***config bootconfig flags info***

*If the **tftpd** flag is set to false, reset the flag to true by typing:*
***config bootconfig flags tftpd true***

*Confirm the flag is now set to true, then retry the transfer. If the problem persists, contact your next level of support.*

***Note 2:*** *If the transfer completes but the file is corrupted, verify original file and PCMCIA card and transfer the file again. If the problem persists, contact your next level of support.*

***Note 3:*** *Compare file parameters such as file size to check for possible corruption.*

**c** ***Only*** *if* Chassis N of Passport 8600 uses an ATM blade, TFTP the ATM Flash image to the Flash card on the Passport 8600 Chassis N by typing (otherwise go to step 78):

**copy <a.b.c.d>:/swd/pp8600/XXX/<newATM> /flash/**

where **<newATM>** is the name of the new ATM file

***Note:*** Notes 1 and 2 from step 77, sub-step b apply.

**d** If the Passport 8600 uses DES, back up the file. Type:

**copy /flash/<oldDES> /pcmia/**

where **<oldDES>** is the original DES filename

**e** If the Passport 8600 uses 3DES, back up the file. Type:

**copy /flash/<old3DES> /pcmia/**

where **<old3DES>** is the original 3DES filename

**78** Prepare to reboot Passport 8600 Chassis N as follows:

***Note:*** There is an intentional space between **image-file** and **/flash** in the syntax for substeps a and b.

**a** type:

**config bootconfig choice primary image-file /flash/<newload>**

**b** type:

**config bootconfig choice secondary image-file /flash/<swloadbkup>**

**c**

**WARNING**

Disable the flag setting before saving the bootconfig file. Failure to observe this step can result in loss of configuration.

**config bootconfig flags verify-config false**

**d** verify the **<newload>** by typing:

**sho boot config**

*Make sure the result indicates the primary image file is **<newload>**.*

**e** save the bootconfig file by typing:

**sav bootconfig**

*This prepares Passport 8600 Chassis N to reboot.*

**79**

**ATTENTION**
This command upgrades the primary-image file (including the ATM-image, if present) and boot monitor at the same time.

**ATTENTION**
Do not interrupt the reboot process. The CPU card can be damaged if the reboot is interrupted incorrectly.

Reboot Passport 8600 Chassis N to upgrade the software image with the new software load as follows:

**boot /flash/<newboot>**



where **<newboot>** is the name for the new monitor image file

*Serial connectivity is maintained between the terminal server and Passport 8600 Chassis N during the 60 to 90 seconds required to load the new software image.*

***Use the Passport 8600 CLI to verify all hardware and software on the Passport 8600 Chassis X:***

**80** Make sure Passport 8600 Chassis X (for N=0, X=1; for N=1, X=0) is still operating correctly as follows:

***Note:*** Refer to step 3 for more information about interpreting the results of sub-step a to sub-step c.

**a** check the log file by typing:

**sho log file**

*Review the info and correct any errors or problems reported.*

**b** check the configuration by typing:

**sho config**

*Output similar to the following appears.*

```
#<output date and time info>
#boxtype : Passport-8010
#software version : W.X.Y.Z
#monitor version : W.X.Y.Z
#<output continues>
```

*where **W.X.Y.Z** represents the release number (Ignore the **NNN**.)*

*Review the configuration file (showing network topology and configuration) and correct any incorrect configurations.*

***Note:*** Software version is the load or image version. Monitor version is the bootflash version.

**c** check the address resolution protocol information by typing:

**sho ip arp info**

*Review the IP ARP info and correct any discrepancies.*

***Note:*** *Refer to step 3, sub-step c for information on checking the IP ARP file.*

**81** Select the next step as follows.

| If | Do |
|---|---|
| an inservice CPU memory upgrade for a Passport 8600 chassis is anticipated for future expansion | refer to document “Installing a CPU Memory Upgrade,” Part No. 314832-B, to upgrade the 8691 CPU to 256MB |
| an inservice CPU memory upgrade for a Passport 8600 is not anticipated | step 82 |

**82** Select the next step as follows.

| If | Do |
|---|---|
| the volumes on any STORM disk (for example, sd01) were mounted in DIRP | step 83 |
| the volumes on the STORM disk are not actively mounted in DIRP, or use a STORM IA configuration | step 85 |
| using an XA-Core | step 85 |

**83** At the Core, return to service all disk volumes connected to the Passport 8600 chassis that was upgraded.

**>diskadm sdXX; rts all**

where:
**XX**=01 for iteration N=0
**XX**=00 for iteration N=1

**84** Individually remount all volumes in DIRP. (Ensure you are at the nodisp;mtc;iod;dirp level of the MAPCI for this step.)

**>mnt <subsystem> <volume> <variable>**

***Note 1:*** The **<variable>** parameter is not required when mounting and demounting regular DIRP volumes.

***Note 2:*** Nortel Networks recommends recording all subsystems, volume, and variable information for each volume demounted in step 65.

***Use the SAM21 EM to unlock the inactive GWCs and SCs:***

**85** Launch the SAM21EM client.

*The SAM21 EM GUI appears.*

**86** Select the next step as follows:

| If upgrading to SN07 from | Do |
|---|---|
| release *lower than* SN06 | step 87 |
| release SN06 (or greater) | step 88 |

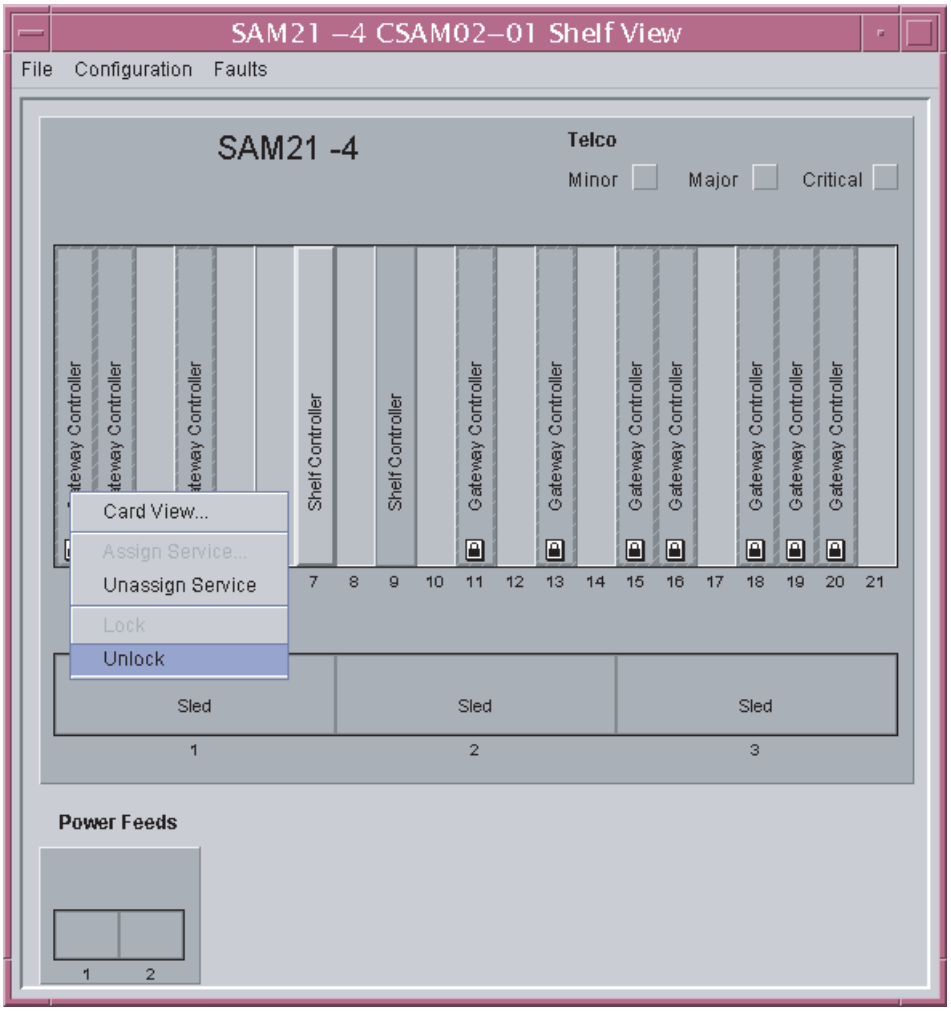
**87** Unlock each locked Gateway Controller unit as follows:

**a** right click on a locked Gateway Controller Unit

**b** select **Unlock** from the drop-down menu that appears

**c** repeat sub-step a and sub-step b until all units are unlocked.

***Note:*** A padlock icon identifies locked GWC units.




**88** Select the next step as follows:

| If upgrading with an | Do |
|---|---|
| ATM solution | step 89 |
| IP solution | just step 89d |

**89** Unlock each locked Shelf Controller blade as follows:

**a** right click on each locked SC blade

**b** select **Unlock** from the drop-down menu that appears

**c** repeat sub-step a and sub-step b until all units are unlocked.

***Note:*** A padlock icon identifies locked SC blades.

**d** continue as follows:

| If USP Compact is | Do |
|---|---|
| used | step 90 |
| not used | step 95 |

***Use the SAM21 Element Manager to unlock the inactive USPc:***

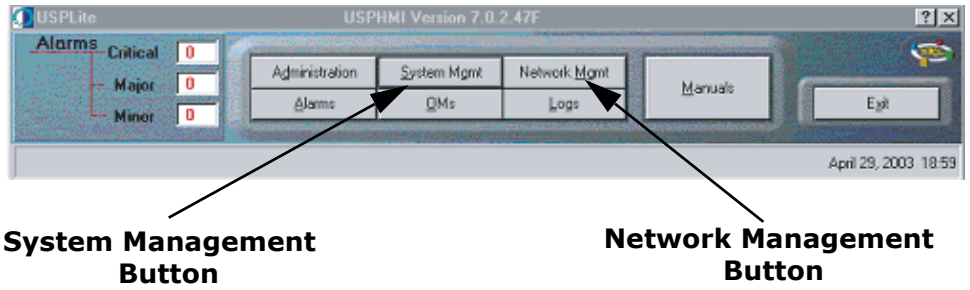
**90** Using the SAM21 EM unlock the slave USPc.

***Note:*** Unlocking the slave USPc from the SAM21 EM enables the USPc GUI.

***Use the USPc GUI to perform the following additional steps:***

**91** Unlock the slave USPc Blade as follows:

**a** click the System Management button on the Main Toolbar




**b** click on the slave USPc blade icon to start the GUI for Shelf management

***Note:*** The blade icon with no checkmark identifies the slave USPc. The blade icon with a checkmark is the master USPc).

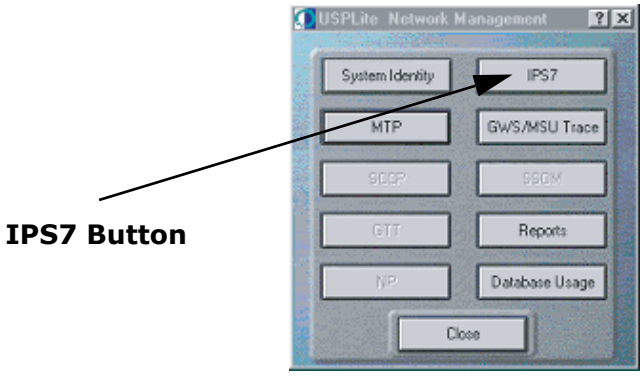
**c** click Unlock to return the slave USPc blade to service.

*A confirmation window appears. Select OK to continue.*

**92** Activate all paths on the slave USPc as follows:

**a** click the Network Management button on the Main Toolbar.

**b** click the ISP7 button in the Network Management window.




*The USP Compact IPS7 window appears.*

**c** click ASP Paths button in the USP Compact IPS7 window.

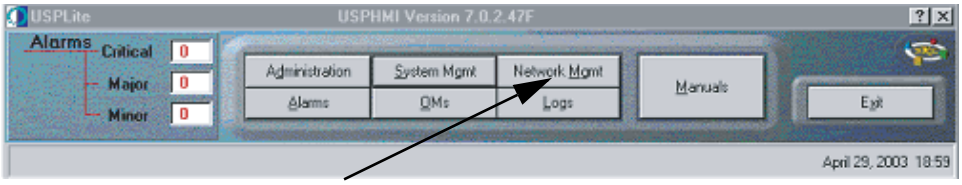
*The USP Compact Application Server Process Path Administration window appears.*

**d** click the Path Actions button in the USP Compact Application Server Process Path window.

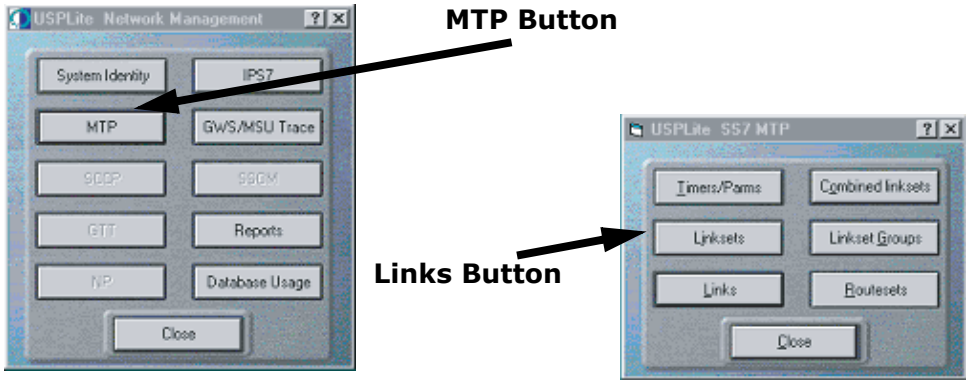
*A confirmation window appears. Select OK to continue.*

**93** Activate all links on the slave USPc as follows:

**a** click the Network Management button on the Main Toolbar.



**b** click the MTP button in the Network Management window.



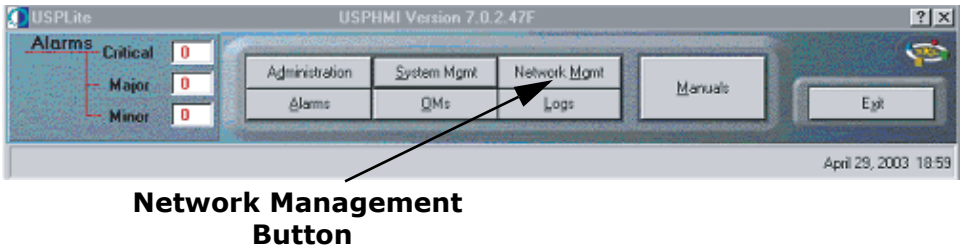

*The USP Compact SS7 MTP window appears.*

**c** click the Links button for the slave USPc links.

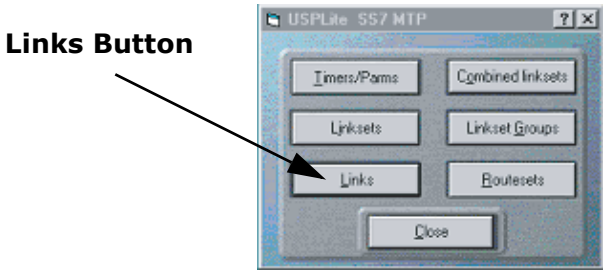
*A confirmation window appears. Select OK to continue.*

**94** Uninhibit all links on the slave USPc as follows:

**a** click the Network Management button on the Main Toolbar.




**b** click the Links button in the SS7 MTP window.




*The Link Management window appears.*

**c** click the Uninhibit button for the slave USPc links

*A confirmation window appears. Select OK to continue.*

**95** Select the next step as follows:

| If the Communication Server uses: | Do |
|---|---|
| an XA-Core | step 96 |
| a Compact chassis | step 98 |

***Use the XA-Core MAP terminal to enable Ethernet links with the Passport 8600:***

**96** Access the ETHR level of the MAP display by typing:

**>MAPCI;MTC;XAC;ETHR**

**97** Refer to the tables below and enable the Ethernet link between the XA-Core and Passport 8600 Chassis N by doing either sub-step a or sub-step b as appropriate.



**a** if the XA-Core uses HIOPs or HCMICs, type (otherwise do sub-step b):

**rts <slot> r link**

| HIOPs/HCMICs | N = 0 | N = 1 |
|---|---|---|
| **<slot>** | 5 | 14 |

go to step 98



**b** if the XA-Core uses IOPs with ETHR packlets, type:

**rts <slot1> r l link**

wait for the command to complete then type:

**rts <slot2> r l link**

| IOP with ETHRs | N = 0 | N = 1 |
|---|---|---|
| **<slot1>** | 5 | 6 |
| **<slot2>** | 13 | 14 |

***Use the Passport 8600 CLI to reset VRRP priority settings and OSPF cost metrics:***

**98** Make sure Passport 8600 Chassis N is in service as follows:

**a** check the IP route information by typing:

**sho ip route info**

*The IP route information file appears. Review the file and verify that the route information is correct.*

**b** check the IP VRRP information by typing:

**sho ip vrrp info**

*The IP VRRP information file appears. Review the file and verify that the information is correct.*

**99** Reset the VRRP priority and OSPF metrics for Chassis N as follows:

**a** type:

**config vlan <vid> ip vrrp <vrid> prio <setting>**

***Note:*** See step 5 for <vid> and <vrid> values for Chassis N. The **PRIO** value for the Chassis N <setting> is also recorded step 5.

*The VRRP priority metric is reset to its operational value.*

**b** type:

**config vlan <vid> ip ospf metric <value>**

***Note:*** See step 10 for the OSPF metric for <value>.

*The OSPF metrics reset to their original value.*

**c** Save the new Passport 8600 configuration by typing:

**sav config**

*This updates the new Passport 8600 configuration so that VRRP settings are maintained after any subsequent reboot.*

**d** Re-enable the flag settings and save the bootconfig file.

**config bootconfig flags verify-config true**

**sav bootconfig**

**100** Increment the iteration index (N = N+1), and select the next step as follows:

| If | Do |
|---|---|
| N=1 | step 10 (for second pass) |
| N=2 | step 101 |

***Note:*** In the second iteration (where N=1) when repeating steps step 10 through step 100, use Chassis X in place of Chassis N. Passport 8600 Chassis 1 (identified as Chassis N) is the slave and Passport 8600 Chassis 0 (identified as Chassis X) is the master.

**101** The procedure is complete.

## What's new in this release

This section highlights the functionality introduced in this release.

- Beginning with SN07, these upgrade and rollback procedures address Passport 8600 configurations with dual CPUs. However, a Passport 8600 must be running with a v3.7.0.0 software load or greater *before* a dual CPU with a high-availability (HA) mode is configured for it.
- Added section Text conventions at beginning of this document that briefly defines and gives examples of filenames that appear in dual- and single-CPU configuration commands in the Passport 8600 Upgrade and Rollback procedures.
- Because former Simple Network Management Protocol (SNMP) settings for the CS-LAN have changed with the release of v3.7.0.0 software load, adhere to a warning to disable flag setting when preparing to reboot the CPUs. Failure to observe this warning can result in no configuration. Also if rolling back to pre-v3.7.0.0 software version after having attempted a v3.7.0.0 or later software upgrade for a dual CPU configuration, users must disable the dual CPU HA flag setting *before* the rollback begins.

  Warning messages indicating these conditions at the appropriate steps are included in the procedures.
- Added warning to rollback section that manual configuration changes executed since the completion of a CS-LAN upgrade are lost when rolling back to a pre-v3.7.0.0 software load. Therefore, Nortel Networks strongly recommends re-entering configuration changes at the completion of the rollback.
- Added notes when to skip designated steps when upgrading the Passport 8600 in a PT-AAL1 solution.
- Added notes when to skip designated steps involving GWCs when upgrading from an SN06 (or greater) to SN07 load.
- Added section Acquiring Passport 8600 software for the CS-LAN, which describes how to prepare the Passport 8600 software for an upgrade.
- Deleted steps at end of upgrade procedure to re-establish OSI Level 2 load sharing between master and slave Passport 8600s.
- Added caution note at beginning of section Upgrade considerations when to upgrade the CPU memory, if required, during this procedure.

- Deleted information about downloading Passport 8600 software from external Nortel Networks website. Beginning with SN07, software is vaulted in the Nortel Networks Software Vault and delivered through ESD or on a CD.



Copyright © 2005, Nortel Networks 

# Preparing to upgrade Preside MDM in Succession SN07

**ATTENTION**
Direct upgrade from SN05 to SN07 is not supported for Multiservice Switch 15000 nodes. Upgrade to (i)SN06.2 first and then upgrade from (i)SN06.2 to (i)SN07. Refer to your (i)SN06.2 Helmsman collection for the upgrade to (i)SN06.2 and use this document to complete the upgrade to (i)SN07.

This document is intended for people who are upgrading Nortel Networks Preside Multiservice Data Manager (MDM) servers from software release 14.2 or 14.3 to 15.1 in a SN06/SN06.2 to SN07 upgrade. If you are installing Preside MDM server for the first time, see 241-6001-100 *Preside MDM Installation*.

The upgrade of other components within Succession solutions is not within the scope of this document. For more information about the solution level upgrades, see NN10320-100 *ATM Solutions Basics* and NN10300-100 *IP Solutions Basics*.

During an upgrade of Succession solutions components, Preside MDM servers must be upgraded so that you have access to the functionality provided by a newer version of the software. This is required to support communication with Nortel Networks Multiservice Switch nodes. Earlier Preside MDM releases cannot support newer Multiservice Switch 15000 releases.

## What you need to know

Before you upgrade Nortel Networks Multiservice Switch nodes you must clearly understand the impact of upgrading Preside Multiservice Data Manager (MDM) servers within the Succession portfolio architecture. In addition, review the solution level upgrade strategies in NN10320-100 *ATM Solutions Basics* and NN10300-100 *IP Solutions Basics*.

You must also have an extensive knowledge of Unix and the Preside MDM toolset.

## What's new in this document

### Branding Changes

The terms Passport 15000 and PVG have been rebranded in conjunction with the new Nortel Networks' brand simplified naming format:

- The Passport 15000 is now referred to as the Nortel Networks Multiservice Switch 15000.
- The packet voice gateway (PVG) is now referred to as the Media Gateway 15000.

The Multiservice Switch 15000 and Media Gateway 15000 network elements continue to share common hardware and software aspects. Hybrid systems can combine these network elements' capabilities, despite the fact that no specific brand exists for such hybrids.

For more information on the product rebranding, refer to NN10600-000 *Nortel Networks Multiservice Switch 7400/15000/20000 What's New in PCR6.1*.

## MDM 15.1 new features

The following features are new in SN07:

### MDP Administration enhancements

This feature simplifies Management Data Provider (MDP) administration by capitalizing on existing Nortel Networks Preside Multiservice Data Manager (MDM) services (Server Administration, Host Group directory server, Multi-nodal name server agent). Configuring the MDP servers is simpler. The following servers are now managed by the Server Administration tool:

- MDP Disk Manager (mdpdiskmgr)
- MDP File Mover Manager (mdpfmmgr)
- MDP Passport Data Model Manager (mdpdmm)

- MDP Passport File Manager (mdppmgr)
- MDP File Prober Manager (mdpfpmgr)

***Note:*** MDP servers can now be installed and started using the Server Administration tool. The servers must be started in a specific order taking into account server dependencies. See the Activating new features for Preside MDM SN07 on page 509 before starting servers.

### Shelf view enhancements

This feature enhances the Nortel Networks Preside Multiservice Data Manager (MDM) Shelf View nodal troubleshooting tool by providing:

- a card inventory for non-Wireless Nortel Networks Multiservice Switch cards for PCR 5.2
- sparing indications for LAPS/APS, DLEP (non-Wireless), PBG
- a maintenance state that can be set to on or, off
- ports that can be set to Lock or, Unlock

This feature also makes the Shelf View agent a full-time server with integrated Command Console (CC agent) functionality.

### Server Administration enhancements

The Server Administration (SVM) tool enhancement simplifies Nortel Networks Preside Multiservice Data Manager (MDM) server administration and configuration by allowing users to add or delete servers from a server list. Context-sensitive help is now available on the servers, and servers can be re-ordered in the list by selecting and moving the server to a new location in the list.



**CAUTION**
**Use caution when re-ordering a server sequence**
Only an expert Preside MDM administrator should re-order servers. Consult the 241-6001-310 *Preside MDM Server Reference Guide*.

This feature also provides a launch point for configuration editors associated with servers.

### Configuring the Succession Release name

This feature adds two utilities to the Nortel Networks Preside Multiservice Data Manager (MDM) toolset. It allows operators to set the Succession release name on Preside MDM (visible in the tool

launcher), and to modify the *CommentText* attribute of the Multiservice Switch node. After an upgrade has been successfully completed, this tool can be used to change the software release number. If a software rollback is necessary, the tool should be used to change the Release number after the rollback is successfully completed.

## Upgrade overview

This document provides detailed procedures on how to upgrade Nortel Networks Preside Multiservice Data Manager (MDM) servers. It also provides procedures to verify the success of the upgrade and to configure security on the servers.

This following sections of this document were modified:

- Preside MDM server upgrade overview on page 139
- Preparing for Preside MDM software migration on page 149
- Pre-migration checks for upgrading Preside MDM servers on page 160
- Preside MDM software installation on page 489
- Post-migration checks on page 1389
- Activating new features for Preside MDM SN07 on page 509
- Preside MDM rollback on page 77

# Preside MDM server upgrade overview

This section describes the:

- pre-requisites to performing an upgrade on Nortel Networks Preside Multiservice Data Manager (MDM) servers
- Preside MDM deployment considerations
- Solution level migration logistics
- Preside MDM Succession feature baseline
  - new Preside MDM features in SN07
- Preside MDM server upgrade task flow

## Prerequisites to performing a server upgrade

Before undertaking the upgrade, confirm that you have met the following pre-requisites.

- Upgrade Preside MDM servers before upgrading the Nortel Networks Multiservice Switch nodes they manage. Preside MDM software is backwards compatible and can manage the current and previous releases of Multiservice Switch, however it is not necessarily forward compatible. To upgrade Multiservice Switch 15000 nodes, see NN10070-461 *Upgrading Nortel Networks Multiservice Switch 15000 in Succession Networks PT-AAL1/UA-AAL1* and NN10419-461 *Upgrading Nortel Networks Multiservice Switch 15000 and Media Gateway 15000/20000 in Succession IP Solutions*.
- To ensure that one Preside MDM server remains in contact with the CS2000 Core Manager, IEMS, or the OSS at all times and continues to provide OAM&P information, isolate and completely upgrade one server while the other server remains fully operational. Following the successful upgrade of the first server, isolate and upgrade the second server using the same procedure.
- Both Preside MDM servers must be sane and operating without any errors:
  - Both servers must be in service, operating in a redundant capacity, and capable of supporting traffic and network management functions with no major alarms.
  - Check the Alarm Display and the System Log Display tools and ensure there are no serious or unexplained logs or alarms.

— Ensure that the second server (the one not being upgraded) is sane before proceeding with the upgrade.

— If using disk mirroring, it must be enabled on both servers and operating without any errors.

- This document describes the upgrade of servers from a baseline Preside MDM deployment within Succession, which involves the configuration of a Sun Fire ™ V480 servers located in the Network Operation Center.

  In SN07, Preside MDM, Multiservice Switch 15000 and Media Gateway releases for VoA and VoIP are aligned and a Preside MDM Succession baseline configuration has been defined to achieve a consistent deployment. The following baseline configuration must be achieved before performing a Preside MDM 14.2 or 14.3 upgrade to 15.1 in SN07:

  — standalone/server and client-sets (optional)

  — SUN workstation configuration

  — Preside MDM Succession feature baseline

  See Preside MDM deployment considerations on page 142 and Solution level migration logistics on page 143 for information regarding standalone/server and client-sets baseline configuration. The SUN workstation configuration is covered in other points in this section.

  See the Preside MDM Succession feature baseline on page 144 for a list of features that must be activated before you upgrade from 14.2 or 14.3 to Preside MDM 15.1.

- If you have deployed client-sets, upgrade them before completing the upgrade task flow described in Preside MDM server upgrade task flow on page 148. See Activating new features for Preside MDM SN07 on page 509.

- If you have not deployed Preside MDM servers according to the standard deployment, follow the upgrade task flow described in Preside MDM server upgrade task flow on page 148 as a guideline, but selected steps may be different. Refer to the Preside Multiservice Data Manager (MDM) base documentation and release notes for additional information.

- The Sun Fire ™ V480 server hardware does not change during the upgrade to SN07. The Solaris 8 operating system does not change but there are new patches identified. Please review *Preside Multiservice Data Manager Release 15.1 Supplement* to determine the latest set of patches.

- If you are upgrading Preside MDM servers from CD-ROM, you must have an X11 terminal with IP connectivity to the Sun Fire ™ V480 server that you are upgrading. If are using a Windows PC, you can use X11 terminal emulation software. If you are using a CD to perform the upgrade, you must have access to the CD ROM drive. If you are upgrading from software downloaded from Nortel Networks Electronic Software Distribution (ESD) page, you must have access to the downloaded file. You must also have access to a text editor so that you can edit various files during the upgrade. We recommend using the UNIX VI text editor.
- Review the *Preside Multiservice Data Manager Release 15.1 Supplement*. If you are migrating from Preside MDM release 14.2, then also review the *Preside Multiservice Data Manager Release 14.3 Supplement*. The release supplement describes the features that are new to the software release and includes information on differences in functionality and capability from the old release to the new release. It is essential that you understand the potential impacts before beginning the upgrade.
- You must have extensive knowledge of Unix and Preside MDM tools and software.
- If you have deployed firewalls in your network, you need to understand which sockets the firewalls have been deployed on. For more information, see NN10225-512 *Nortel Networks Multiservice Switch 15000 and Media Gateway 15000 in Succession Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP*.
- Nortel Networks strongly recommends that you perform a full backup of the Preside MDM workstation as instructed in 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*. Backup and restore (rollback) instructions are also provided in 241-6001-100 *Preside MDM Installation*.

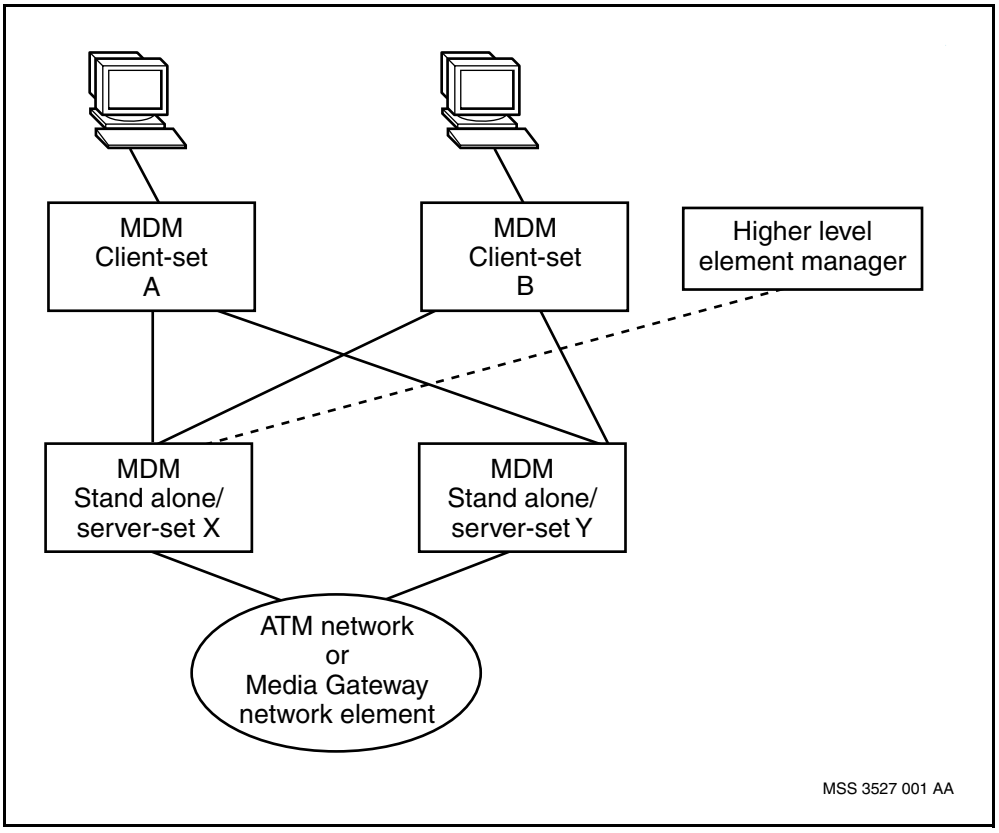
# Preside MDM deployment considerations

Since Nortel Networks Preside MDM can be deployed in many ways, upgrading cannot be viewed simply from the perspective of upgrading a single server but must be viewed from the perspective of upgrading Preside MDM in a Succession deployment. Some common Succession deployment options are:

- stand-alone/server-set (combined server and client)
- separate client sets
- distributed server and client sets

Typical client/standalone/server-set deployment on page 142 illustrates the common deployments. Note that the server and client-sets are deployed as a redundant pair.

**Typical client/standalone/server-set deployment**




## Standalone/server-sets

Standalone/server-sets support the main server processes that allow Preside MDM to perform surveillance and gather network data (fault and/or performance). They are usually run without a monitor and keyboard.

Standalone/server-sets support the main server processes that allow Preside MDM to perform surveillance and gather network data (fault and/or performance).

**Client-sets**

Client-sets host the servers that allow operators to view the surveillance information and network data, and perform provisioning. They are dependent on the standalone/server-sets for the acquisition of surveillance, network data and communication to Preside MDM nodes. Client-sets may host operator desk tops (remote users) as indicated in Typical client/standalone/server-set deployment on page 142.

**Separate standalone/server and client-sets**

While separate server and client-sets are not mandatory to Nortel Networks Preside MDM deployment, they do optimize performance in a large network.

## Solution level migration logistics

Before performing an upgrade, you must consider:

- redundancy (stand-alone/server-set, client-set)
- impact on the OSS and the higher level element manager (this could be the CS2000 Core Manager, SDM (VoA) or IEMS (VoIP))
- order of migration of the server vs. client-sets

Redundancy ensures that the network can be observed and network data collected. Redundancy is unavoidably lost during an upgrade when the server is rebooted (applies to either the server or client-set). At that point the server is running in simplex mode. To minimize the risk of losing the ability to observer the network and collect data, upgrade one of the redundant servers (both server and client-set) at any given time.

A Nortel Networks Preside MDM feature may possibly impact the OSS and the higher level element manager. Software changes may need to be addressed at the OSS level to ensure that incompatibilities do not exist and prevent the OSS and the higher level element manager from losing network visibility.

The general rule when performing migrations is to migrate the most north-bound system first. Migrate systems in the following order:

- OSS and/or IEMS (VoIP) and/or SDM (VoA)
- Client-set A
- Client-set B

- Standalone/server-set A
- Standalone/server-set B
- Multiservice Switch and/or Media Gateway nodes

***Note:*** For Succession Solution specific requirements, refer to the Solution level upgrade procedures.

Migrate the client-sets before the standalone/server-sets because Preside MDM is backwards compatible but not forwards compatible. Home the operator desk tops to the client that is not being migrated to prevent any loss of visibility to the desk tops. Migrate one client-set at a time.

When migrating a standalone/server-set, ensure that the client-sets are not homed into that server-set, otherwise the operator will see an outage because clients do not dynamically switch from one client-server to another. This way the network operator can service select a client-server that is not actively being migrated. Migrate one standalone/server-set at a time.

## Preside MDM Succession feature baseline

Nortel Networks Preside Multiservice Data Manager (MDM) features can be Succession-specific, or not specific to Succession. This section lists the features that are relevant to Succession. These features are already installed for the current VoA customer base (UA-AAL1/PT-AAL1) who have upgraded to SN06 or SN06.2 for those who have done a greenfield ILEC UA-IP installation in SN07 using the Installation Method.

For VoIP and Media Gateway customers outside these deployments, table Preside MDM In Succession - baseline feature list on page 145:

- lists the features that must be activated (appropriate to individual deployments)
- identifies the applicability of the feature to the server vs. client-set
- identifies the Succession release where the feature was introduced
- identifies the Preside MDM release where the feature was introduced
- identifies where the feature originated from: Preside MDM base or Succession

You must establish this baseline before you can upgrade from 14.2 to 15.1, or 14.3 to 15.1. (This document does not describe how to achieve the baseline configuration.)

## Preside MDM In Succession - baseline feature list

| Feature Name | Required for Solution? | Server or client-set feature | Succession Release | Preside MDM Release | Originator |
|---|---|---|---|---|---|
| **Core functionality**: | | | | | |
| Network Time Protocol Support | Y Y | both | NA | in 15.1, this feature is not applicable | Preside MDM base |
| Preside MDM Patch | Y Y | both | all | all | Preside MDM base |
| Client-sets | N N | client | SN06.2 | all | Preside MDM base |
| Redundancy (standalone/server-set) | Y Y | both | all | all | Preside MDM base |
| Redundancy (client server-set if deployed) | Y Y | both | SN06.2 | all | Preside MDM base |
| Software Distribution Site | Y Y | server | all | all | Preside MDM base |
| Data Collection (MDP) | Y Y | server | all | all | Preside MDM base |
| Generating and setting secure passwords for Preside MDM servers (FMDR, PMSP) password encryption | Y Y | server | SN05 | 13.4 | Preside MDM base |
| Secure FTP | Y Y | server | SN05 | 13.4 | Preside MDM base |
| Multiservice Switch backup and Restore | Y Y | server | SN06 | all | Preside MDM base |
| Network Model & Viewer configuration | Y Y | server | all | all | Preside MDM base |
| **Additional features:** | | | | | |
| FDTM Succession configuration | Y Y | server | SN02 | 13.1 | Succession |
| Support for Seasonal time change | N N | server | SN06 | 14.2 | Succession |
| pserver process | Y Y | server | SN04 | 13.3 | Preside MDM base |

## Preside MDM In Succession - baseline feature list

| Feature Name | Required for Solution? | | Server or client-set feature | Succession Release | Preside MDM Release | Originator |
|---|---|---|---|---|---|---|
| NP template installation | Y | Y | server | SN04 | 13.3 | Preside MDM base |
| Multiservice Switch 15000 Configuration Model Server | Y | Y | server | SN06 | 14.1 | Preside MDM base |
| MDP to make BDF files accessible | Y | Y | server | SN06 | 14.1 | Preside MDM base |
| MDP file prober collection times | Y | Y | server | SN06 | 14.1 | Preside MDM base |
| Succession Enabling HSM | Y | Y | client | SN06 | 14.1 | Succession |
| PMs (pmsp & supporting directory structures) | Y | Y | server | SN06 | 14.1 | Succession |
| real-time alarm collection (rtac) | Y | Y | server | SN06 | 14.1 | MDM base |
| File mover for BDF files | Y | Y | server | SN06 | 14.1 | MDM base |
| Shared memory and semaphore setting | Y | Y | server | SN06 | 14.1 | MDM base |

## New features in SN07

Nortel Networks Preside Multiservice Data Manager (MDM) base features added in SN07 are froM Preside MDM release 14.3. There are also several Succession specific features added in release 15.1. Table Preside MDM features new in SN07 on page 147 lists all of the new features for SN07.

***Note:*** If you are upgrading from release 14.3 to 15.1, MDP Administration enhancements, Shelf view enhancements, and Server Administration enhancement features are already installed and activated.

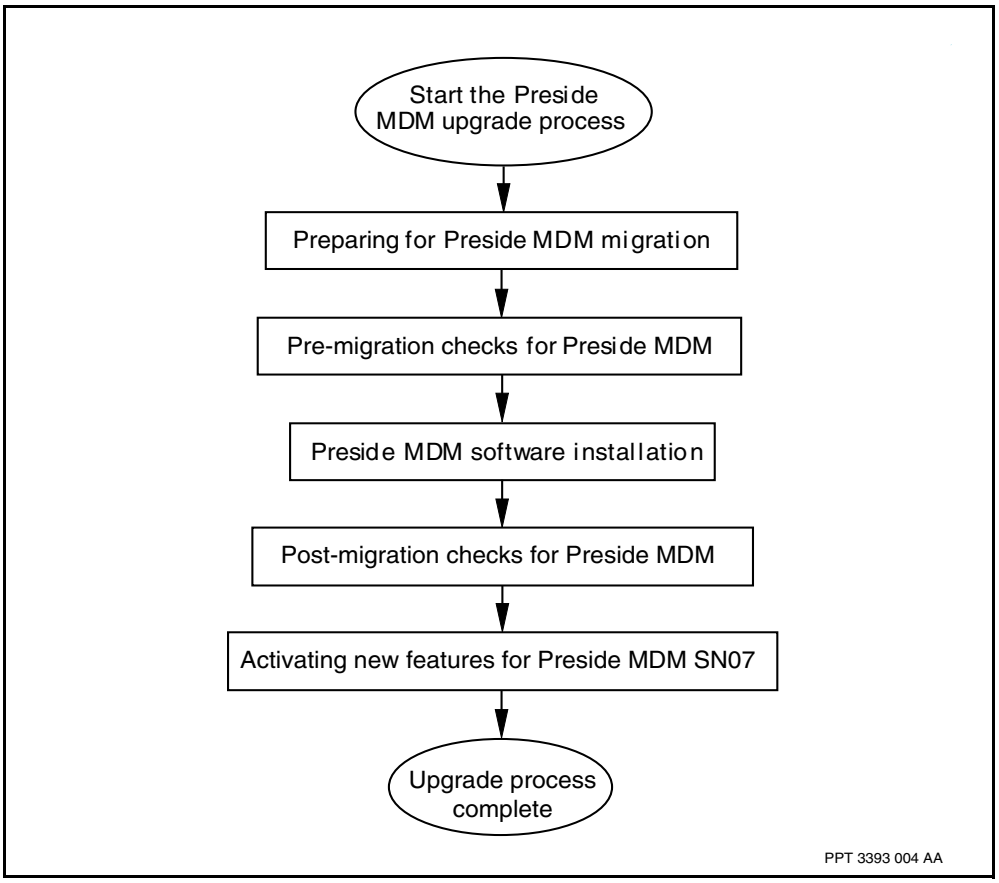
### Preside MDM features new in SN07

| Feature Name | Required for Solution? | | Server or client-set impact | Succession Release | Preside MDM release | Originator |
|---|---|---|---|---|---|---|
| | VoA | VoIP | | | | |
| MDP Administration enhancement | Y | Y | server | SN07 | 14.3 | Preside MDM base |
| Shelf View enhancements | Y | Y | client | SN07 | 14.3 | Preside MDM base |
| Server Administration enhancements | Y | Y | server | SN07 | 14.3 | Preside MDM base |
| Support for 5 min. PMs | Y | N | server | SN07 | 15.1 | Succession |
| SASM Enhancements | Y | N | client | SN07 | 15.1 | Succession |
| Succession Release Name appears in GUI | Y | Y | client | SN07 | 15.1 | Succession |
| XNTP Support | Y | Y | both | SN07 | 15.1 | Preside MDM base |

## Preside MDM server upgrade task flow

The figure Preside MDM server upgrade task flow on page 148 shows the sequence of procedures you must perform to upgrade one Preside MDM server.

**Preside MDM server upgrade task flow**




Repeat the sequence of procedures to upgrade the second server.

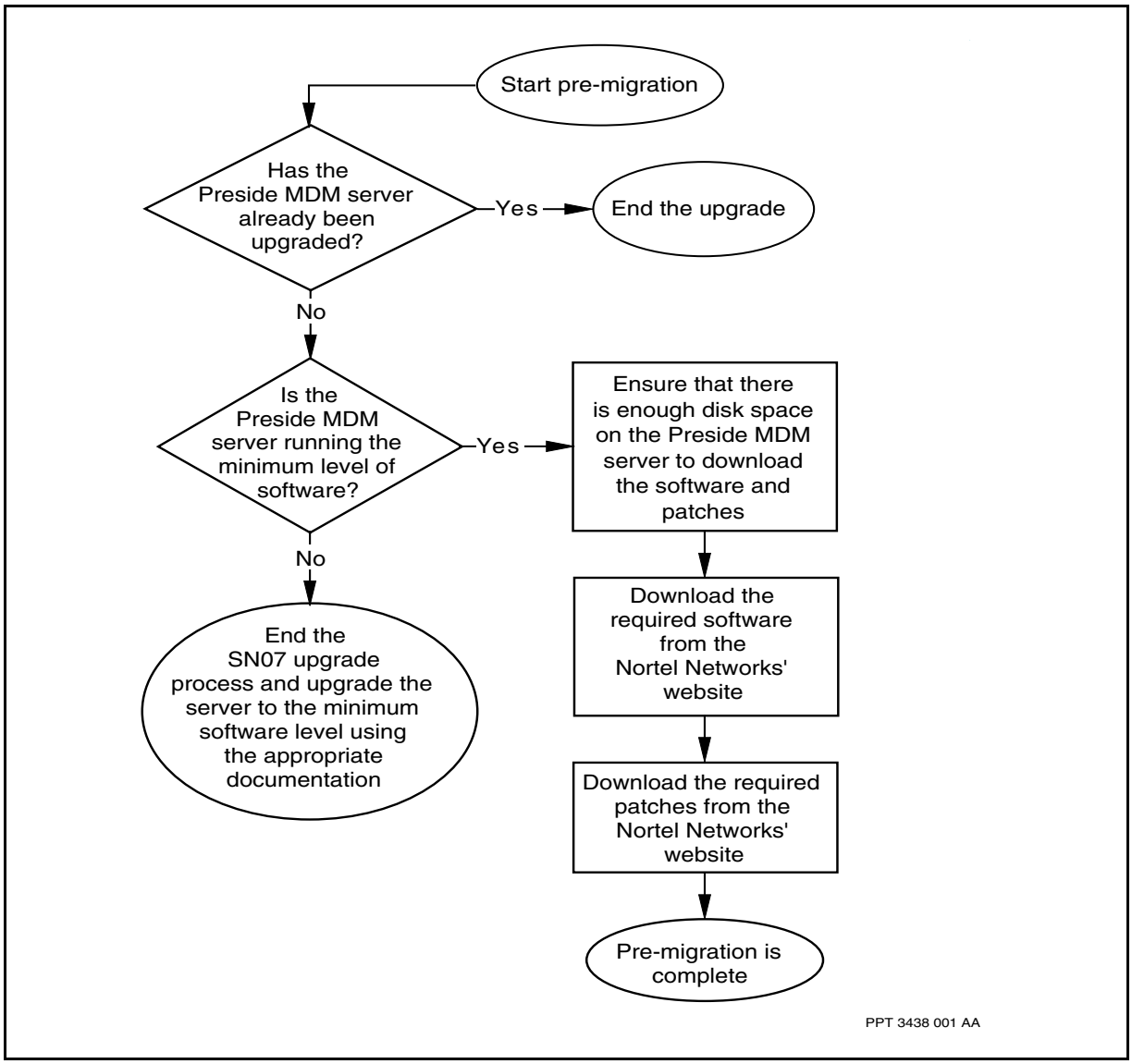
- Preparing for Preside MDM software migration on page 149
- Pre-migration checks for upgrading Preside MDM servers on page 160
- Preside MDM software installation on page 489
- Post-migration checks on page 1389
- Activating new features for Preside MDM SN07 on page 509

After upgrading both servers, upgrade the Nortel Networks Multiservice Switch 15000 nodes. For more information, see NN10070-461 *Upgrading Nortel Networks Multiservice Switch 15000 in Succession Networks PT-AAL1/UA-AAL1*.

# Preparing for Preside MDM software migration

The following figure displays the sequence of procedures you must perform to install Nortel Networks Preside Multiservice Data Manager (MDM) software and patches.

**Preside MDM pre-migration task flow**



Perform the following procedures before installing Preside MDM software and patches:

- Checking the currently active software version on page 151
- Ensuring that there is enough disk space on the servers on page 152
- Downloading Preside MDM software from Nortel Networks website on page 155
- Downloading Preside MDM patches from Nortel Networks website on page 157
- Updating Preside MDM license files on page 159

## Checking the currently active software version

To determine if Nortel Networks Preside Multiservice Data Manager (MDM) has already been upgraded, check the release currently running on the server. Use the command:

```
/opt/MagellanNMS/system/inst/nmsLinks
```

If the response to the command is *MDM142xxx* or *MDM143xxx* proceed with the upgrade.

## Ensuring that there is enough disk space on the servers

If you will be using Nortel Networks ESD page to download the software (not installing it from a CD), ensure that you have sufficient disk space to accommodate the downloaded software.

### Checking server disk space

***From the Preside MDM server***

1 Login — see Logging into Preside MDM servers on page 522.

2 Determine how much disk space is available on each of the servers: **df -k**

The system indicates in kilobytes how much disk space is used in each of the disk partitions.

### Sample response from issuing the df -k command

```
Filesystem   kbytes  used    avail   capacityMounted
on
/proc        0       0       0       0%      /proc
/dev/md/dsk/d0619623418239974310275 30%     /
fd           0       0       0       0%      /dev/fd
/dev/md/dsk/d4018865671782201651750 10%     /var
```

***Note:*** Preside MDM data directories (/opt/MagellanNMS/data/) should not be part of the root (/) partition. A separate/data partition with a soft-link to /opt/MagellanNMS/data/ or an NFS mount to a separate physical medium is recommended.

3 Review *Preside MDM supporting PP15K* entry in *Preside Multiservice Data Manager Release 15.1 Supplement* to determine how much disk space you need. Typically, you need 2000 Mb of disk space.

4 Compare the space available under / with the value in step 3.

5 If you need more disk space on the server, investigate the following strategies:

- Remove older, unwanted Preside MDM software versions
- List the software version currently available:

  **ls /opt/MagellanNMS/loads**
- Select loads that are no longer required and enter the following commands, where <release> is the name of the software load you wish to uninstall:

**cd /opt/MDM<release>_INST**
**./uninstall_mdm<release>**

- remove old CSV files
- remove core files
- remove bdf files
- contact GNTS for alternative strategies

***Note:*** Preside MDM software configuration is persistent. As a result, you will not lose your configuration when you delete Preside MDM packages.

# Retrieving Preside MDM software and patches from a drop box

After verifying that the server has sufficient disk space, you can begin to download Nortel Networks Preside Multiservice Data Manager (MDM) software. Preside MDM patches are jumbo patches that include all previous patches. As a result, you only need to retrieve the most current version of a patch. One method is to retrieve the software from your customer drop box.

## Prerequisites

- You need a dropbox and an account with a user name and password. Contact your Nortel Networks customer representative for more information on accessing Nortel Networks website.
- You must have performed the procedure: Ensuring that there is enough disk space on the servers on page 152.
- Refer to the software downloads area of Nortel Networks website (*www.nortelnetworks.com*) to verify that the drop box contains the software files you need to retrieve. If there are no patches listed for this release, it means that there are no patches currently required for this release.

## Retrieving software from a drop box

### *From the Preside MDM server*

1 Login — see Logging into Preside MDM servers on page 522.

2 Retrieve the required software files and patches according to your retrieval procedure:

- MDM 15.1 Supplement
- MDM 15.1 CD1
- MDM 15.1 CD2
- MDM 15.1 CD3

# Downloading Preside MDM software from Nortel Networks website

After verifying that the server has sufficient disk space, begin downloading software. One method is to download the required software from Nortel Networks website. When you download the software from this website, a copy of the software is placed in the directory you specify.

## Prerequisites

- Refer to the software downloads area of Nortel Networks website *www.nortelnetworks.com* to determine the software load and patches that you need. If there are no patches listed for this release, it means that there are no patches currently required for this release.
- Ensure that you download all software files that belong to the release you require. The software you need to download may be composed of more than one file.
- Download the associated patches after downloading the required software release from the website. For more information, see Downloading Preside MDM patches from Nortel Networks website on page 157.
- Perform the procedure: Ensuring that there is enough disk space on the servers on page 152.

### *From the Preside MDM server*

1. Login — see Logging into Preside MDM servers on page 522.
2. Change directories to the / directory: **cd /**
3. Create a directory to which you can download the software: **mkdir MDM151**

   ***Note:*** Remove this directory at the end of the installation procedure.
4. On the web, go to: *www.nortelnetworks.com*.
5. In the Support section of the window, click *Software Downloads*.
6. Click on *Log In.*
7. When prompted, enter your user name and password for the login.
8. In the Product Family section of the Software Downloads window, click *Preside*.

9 Under the Preside MultiService Data Manager for Succession PT/UA-AAL1 section, click *Software*.

10 The loads and patches for the release are identified at *www.nortelnetworks.com*

***Note:*** Software loads are contained in zip files, while each patch is contained in a single file. The MDM 15.1 Supplement is found under the Documentation tab. The software is found under the Software tab.

11 Download the following software:

- MDM R15.1 Supplement
- MDM 151 CD1
- MDM 151 CD2
- MDM 151 CD3

12 Enter the following directory to indicate where you want the software load files placed: */MDM151*.

13 Click *Save*.

14 On the Preside MDM server, change directories to the directory containing the software:

**cd /MDM151**

15 Uncompress the software load file:

**uncompress <swload_name>.tar.Z**

16 Untar the software load file: **tar xvf <swload_name>.tar**

17 Repeat step 14 through step 16 for every software file you want to download.

18 Delete each tar file: **rm -r <swload_name>.tar**

**Variable values**

| Variable | Value |
|---|---|
| <swload_name> | The name of the software load file that you want to download. |

# Downloading Preside MDM patches from Nortel Networks website

In addition to the main software release, you may need to download patches from Nortel Networks website to the Preside Multiservice Data Manager (MDM) server. When you download the patches from this website, a copy of the patches is placed in the directory you specify.

## Prerequisites

- You need a dropbox and an account with a user name and password. Contact your Nortel Networks customer representative for more information on accessing Nortel Networks website.
- Refer to the software downloads area of the website (to determine which patches you need to download.

  *www.nortelnetworks.com*

  ***Note:*** Consult the Release Notes for this release to identify the most current list of patches you require.

- Preside MDM patches are jumbo patches that include all previous patches. As a result, you only need to download the most current version of a patch.
- You must have performed the procedure: Ensuring that there is enough disk space on the servers on page 152.

### *From the Preside MDM server*

1. Login — see Logging into Preside MDM servers on page 522.
2. Change directories to the / directory: **cd /**
3. Create a directory to download the software to: **mkdir patch151**

   ***Note:*** Remove this directory when the patches are installed.
4. On the web, go to *www.nortelnetworks.com*.
5. In the Support section of the window, click **Software Downloads.**
6. Click on *Log In*.
7. When prompted, enter your user name and password for the login.
8. In the Product Family section of the Software Downloads window, click *Preside*.
9. Under the Preside Multiservice Data Manager for Succession section, click *Software*.

10 Refer to the software downloads area of Nortel Networks website (*www.nortelnetworks.com*) to determine which patches you want to download.

11 Download the following patches if they exist (if the patch does not exist then no patch is required):

- MDM151-xx
- MDP151-xx
- DVR151-xx

12 Click on the file listed beside the File Download heading.

13 Enter the following directory to indicate where you want the patch placed: **/patch151**

14 Click *Save*.

15 Repeat steps 13 through step 14 for the other patches you need.

## Updating Preside MDM license files

Before you can run Nortel Networks Preside Multiservice Data Manager (MDM) server software, you need a license password and a customer identifier. This comes with your Nortel Networks Preside Multiservice Data Manager server upgrade CD. For information on how to upgrade and configure your new server license, see “Software licenses for MDM (mandatory)” in the 241-6001-100 *Preside MDM Installation*. If you do not have the license, you will need to order one. Contact your Nortel Networks Sales Representative for additional information.

# Pre-migration checks for upgrading Preside MDM servers

Before starting to upgrade Nortel Networks Preside Multiservice Data Manager (MDM) servers, you must verify that the servers are in a state that will permit the upgrade.

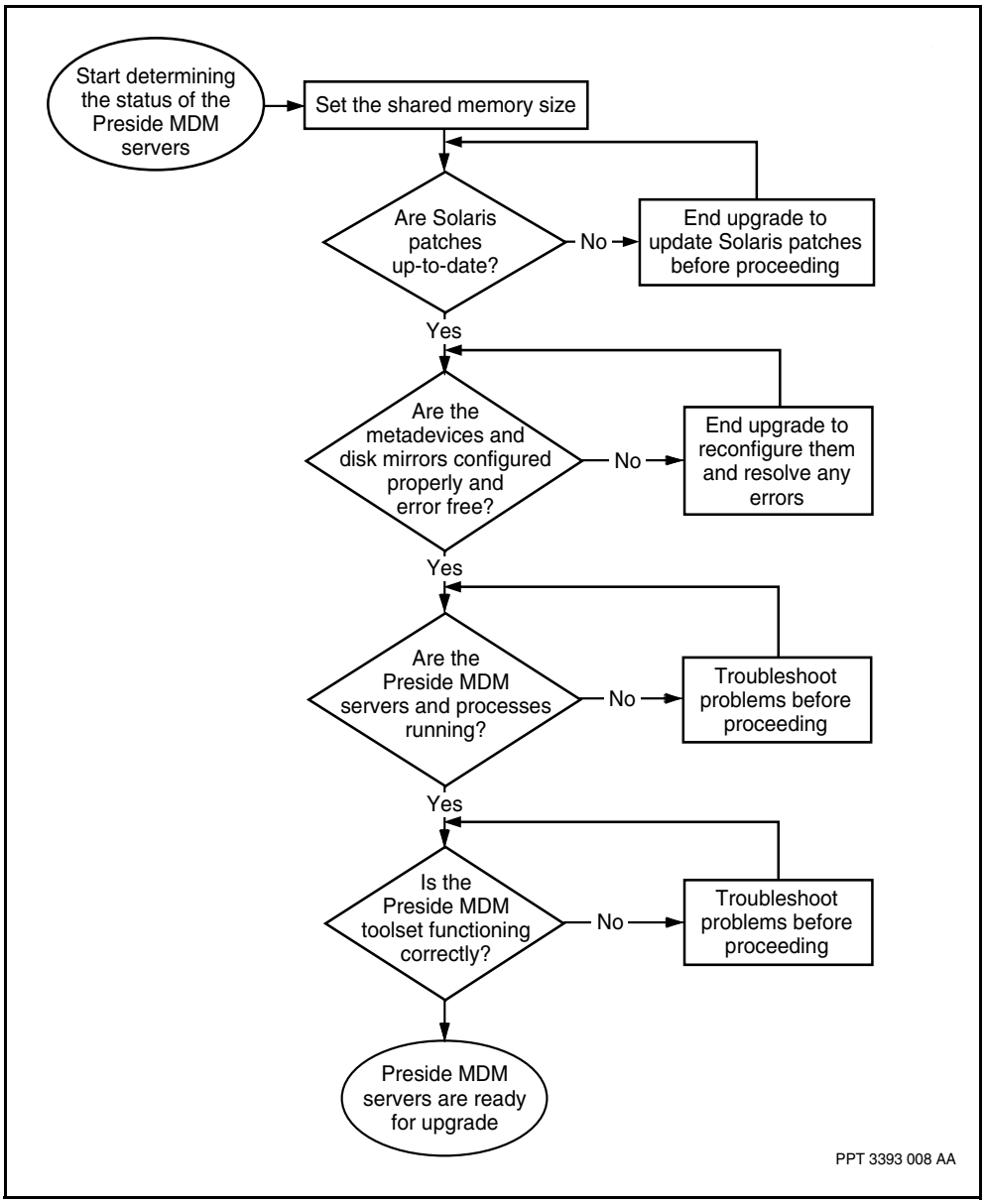
## Prerequisites

You must have:

- access to a text editor on the terminal connected to the servers so that you can open various files. We recommend using the UNIX VI text editor.
- an extensive knowledge of UNIX and Preside MDM tools and software.
- a full backup of the Preside MDM workstation. Refer to 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*. Backup and restore (rollback) instructions are also provided in 241-6001-100 *Preside MDM Installation*.

The figure Preside MDM pre-migration checks task flow on page 161 shows you the sequence of procedures you must perform to determine the status of the servers.

## Preside MDM pre-migration checks task flow



To link to one of the pre-migration procedures, click on one of the following:


- Setting the shared memory size on page 163
- Verifying Solaris and its patch level on page 164
- Verifying the status of the metadevices and disk mirroring on page 165
- Verifying that Preside MDM servers and processes are running on page 166
- Verifying that the Preside MDM toolset is functioning on page 168

# Setting the shared memory size

Before beginning the upgrade, you need to set the shared memory size to the value 256.

### Prerequisites

- Check the *Preside Multiservice Data Manager Release 15.1 Supplement* to determine if the specific value should be other than 256.

.

### Setting the shared memory size

***From the Preside MDM server***

1 Login - see Logging into Preside MDM servers on page 522.

2 Issue the following command:
**/opt/MagellanNMS/system/config/config_sys_shmem 256**

The system prompts you to confirm the change in shared memory size.

3 Confirm the change: **yes**

4 The system may prompt you to reboot. You are required to reboot later during the installation, therefore it is not necessary to reboot at this time. Do not confirm the reboot: **no**

# Verifying Solaris and its patch level

Before beginning the upgrade, determine if the Sun workstation OS is at the right level with the correct patches. Check the *Preside Multiservice Data Manager 15.1 Release Supplement* to determine which SUN OS patches to upgrade. Use the supplement that was obtained from the Electronic Software Distribution (ESD) page (*www.nortelnetworks.com*).

## Verifying Solaris and its patch level

### *From the Preside MDM server*

1. Login - see Logging into Preside MDM servers on page 522.
2. Open an xterm session.
3. Issue the following command: **uname -a**

   The system response indicates that the OS is running at Solaris 8 represented by a 5.8.
4. Check what release of OS is currently running on the workstation:

   **cat /etc/release**

   An example of a Solaris 8 OS output is as follows:

   ```
   Solaris 8 HW 7/03 s28s_hw3wos_05a SPARC
   ```

   In this example the OS version date is 7/03.
5. Compare the output with the Solaris Maintenance Releases as specified in the *Preside Multiservice Data Manager 15.1 Release Supplement*.
6. If the OS version is equal to or greater than the OS version as specified in the *Preside Multiservice Data Manager 15.1 Release Supplement*, an upgrade is not required.

   If the OS version is less than the version specified in the *Preside Multiservice Data Manager 15.1 Release Supplement*, you must upgrade the OS Maintenance release to the correct version of the specified Solaris OS. Refer to the *Preside Multiservice Data Manager 15.1 Release Supplement* for information on where to find the Solaris Maintenance release software.

## Verifying the status of the metadevices and disk mirroring

If you are running disk mirroring on your Sun server, ensure the mirrors are functioning correctly. Consult the SUN documentation for more information.

# Verifying that Preside MDM servers and processes are running

The state of Nortel Networks Preside Multiservice Data Manager (MDM) servers will be one of the following:

- *Not started*, which indicates that the server has not been started since the SVMDMN process was started or since it was added to the list.
- *Running*, which indicates that the server has been started automatically by the SVMDMN process or by an administrator.
- *Exited*, which indicates that the server has exited unexpectedly and is awaiting a restart. When a server is in this state, information about the server is displayed on a yellow background.
- *Quit*, which indicates that the server has shut itself down. No restarts are being attempted. When a server is in this state, information about the server is displayed on a red background.
- *Failed*, which indicates that the server has exceeded all restart limits and that no further attempts to restart it automatically are being made. When a server is in this state, information about the server is displayed on an orange background.

## Verifying the servers and processes are running

### *From the Preside MDM server*

1 Login — see Logging into Preside MDM servers on page 522.

2 Open a Preside MDM window — see Opening the Preside MDM window on page 522.

3 From the Preside MDM window, choose System > Administration > Server Administration.

4 Scan the server list and verify that all of the servers are in a *Running* state.

***Note:*** See the 241-6001-310 *Preside MDM Server Reference Guide* for information on starting a server.

5 To view more detailed information about the server, click on the name of the server whose information you wish to view.

6 From the Edit menu, select *View*.

The server name in the Server Administration dialog indicates the descriptive name assigned to the server.

7 Click *Ok* when you have finished with the dialog.

8 Close the Server Administration tool.

9 From the Preside MDM window choose System -> Administration -> GMDR Administration.

***Note:*** For more information, see Using the GMDR Administration tool in the 241-6001-303 *Preside MDM Administrator Guide*.

10 Ensure that there are two FMDR servers for every distinct Succession office, and two IMDR servers (total) listed. Ensure that each server is associated with a different workstation, and that all are in a connected state.

11 Close the GMDR Administration window.

12 If MDP is running on this system and you are running release MDM 14.2, login as mdpadmin (or the mdpadmin user ID for your system).

From a UNIX window, type: **mdpadm display**

If you are running release MDM 14.3, open and use the Server Administration tool to check that the servers are running.

# Verifying that the Preside MDM toolset is functioning

During a pre-migration check, perform the following procedure to verify that Nortel Networks Preside Multiservice Data Manager (MDM) processes are working correctly.

## Verifying Preside MDM toolset is functioning

### *From the Preside MDM server*

1. Login, see Logging into Preside MDM servers on page 522.
2. Open a Preside MDM window:

   **/opt/MagellanNMS/bin/nmstool &**
3. Click OK to close the copyright dialog.
4. Verify that the Alarm display opens and displays alarms.
   a. From the Preside MDM window, choose Fault>Alarm Display: Active
   b. When the Alarm Display window opens, verify that the alarms are being received.
5. Verify that the Network Viewer opens and displays the nodes. From the Preside MDM window, select Fault > Network Viewer.
   a. From the Preside MDM window, select Fault > Network Viewer.
   b. When the Network Viewer window opens, double-click the group icon to expand it.

      Right-click on the icons to see the node name. Select the node(s) you wish to check.
6. Confirm that the viewer displays the status of the nodes.
7. Verify that the Nodal Provisioning tool opens. From the Preside MDM window, select Configuration > Passport Devices> Nodal Provisioning.
8. If more than one Configuration Manager server is specified in the configuration file, a Select Server dialog box opens. Otherwise, go to step 10.
9. If required, select a valid host in the Select Server dialog and click *OK*.
10. In the Nodal Provisioning Device Selection dialog, select a valid device and click *OK.*
11. In the Authenticating dialog, log on to the network destination by entering a valid user ID and password.

**12** In the Open View dialog, select the Access Mode and the desired View Mode.

The Nodal Provisioning window opens with a component hierarchy displayed by default.

# Preparing to upgrade the CS 2000 Core Manager

## Purpose

Perform the procedures in this section prior to a CS 2000 Core Manager software upgrade. The purpose of these procedures is to ensure that the CS 2000 Core Manager is configured correctly, and that all hardware and software are in good operating condition.

## Prerequisites

This section also includes the procedure Software upgrades from tape on page 196. The purpose of this procedure is to avoid any potential tape problems during the upgrade.

**ATTENTION**

Nortel Networks strongly recommends that you perform this procedure seven days before the start of any software upgrade, to allow time for corrective action if required.

You must successfully complete each pre-check task. Call the Nortel Networks support center for assistance if you cannot successfully complete a pre-check task.

By completing each of the pre-check tasks and submitting a list of any failed pre-check tasks to Nortel Networks, you will minimize potential disruption to the software upgrade, minimize any risk to the switch, and assist Nortel Networks in providing full support on the upgrade, should assistance be required. Nortel Networks will assist in recovering a CS 2000 Core Manager if a problem arises during a software upgrade that was not preceded by this pre-check procedure, but will not provide a root cause analysis of the problem.

## Application

Perform this procedure using a printed copy. A check box is provided at the beginning of each task to help you track your progress through the entire procedure. Whenever you successfully complete a task, put a check mark in the box.

Once you have completed each pre-check task in this procedure, send an email to prodsdm@nortelnetworks.com with the following information:

- Customer name
- CLLI

- Product

  ***Note:*** For Product, specify one of the following values:

  — SDMX for Mobile Telephony Exchange (MTX) applications

  — SDM for SuperNode Data Manager (SDM) base applications

  — GEM (GSM element manager) for UMTS (Universal Mobile Telecommunications System) or GSM (Global System for Mobile-communications) applications

  — CS 2000 Core Manager for Succession applications

- Current load
- Date
- List of any failed pre-check tasks, and a brief description of their solution

# Procedures

## Capturing the pre-check session file

It is recommended that you capture the execution of the pre-check session and store the file on the CS 2000 Core Manager for ten days. Nortel Networks support engineers can use the file to investigate any pre-check step that failed.

To capture the upgrade pre-check session, complete the following steps before starting the pre-check procedure.

### Capturing the pre-check session file

***At the CS 2000 Core Manager VT100 console***

**1** Start the capture of the pre-check session:

```
#script -a sdmprecheck_YYMMDD
```

*where*

**YYMMDD**
is the current year, month, and day that the pre-check procedure is performed

The system creates a file named sdmprecheck_YYMMDD and places it in your current directory.

**2** When you complete all the pre-check tasks, press Ctrl + D to terminate the capture for the sdmprecheck_YYMMDD session file.

**3** You have completed this procedure.

## Pre-check list

Each required pre-check task is listed below. Complete each of the pre-check tasks and indicate whether the task passed or failed for reference purposes.

| Pre-check tasks | Time (min.) | Passed /Failed |
|---|---|---|
| Basic pre-checks | 20 | |
| System audit pre-check | 5 | |
| Hardware baseline pre-check | 5 | |
| CPU Stability pre-check | 5 | |
| DS512 fiber link pre-check | 5 | |
| Application/fileset status and configuration pre-check | 2 | |

| Pre-check tasks | Time (min.) | Passed /Failed |
|---|---|---|
| User configuration pre-check | 2 | |
| Ethernet configuration pre-check | 5 | |

### Basic pre-checks

Before beginning the software upgrade process, ensure that you have completed the following activities.

- Notify the Network Operation Center before you perform this procedure and before you perform the software upgrade procedure, as both procedures may temporarily raise alarms on the Communication Server 2000 core and CS 2000 Core Manager.
- Obtain root and cell_admin passwords.
- Obtain the IP address for the CS 2000 Core Manager, the Communication Server 2000 core, and the operating company gateway and LAN (local area network).
- Ensure you have the latest Maintenance Non-Computing Load (MNCL) release installed on the CS 2000 Core Manager before you upgrade to the new NCL release. Refer to Upgrade guidelines on page 527 for the software baseline.

  ***Note:*** If you need to upgrade to the latest MNCL, refer to the MNCL release notes for instructions.

- Ensure that the modem is configured and operational in the event that Nortel Networks Field Support personnel require remote access to the CS 2000 Core Manager.
- Obtain a 3-gigabyte blank DAT tape to perform a full system backup following the upgrade.

  ***Note:*** Make sure that you have selected one of the brands and lengths approved by Nortel Networks. The approved brands are: Hewlett Packard (HP), Maxell, Verbatim, Imation. The approved lengths (from any of the listed manufacturers) are: 90-meter (90M), 120-meter (120M), or 125-meter (125M). The 125M tape is approved for UMFIOs only, provided that your system is equipped with DDS3-capable devices to read the content of the tape.

- Check your VT100 terminals and cables.
- Clean tape drive 0 (slot 2) and tape drive 1 (slot 13) if you will be upgrading using the procedure Software upgrades from tape on page 196 or directly from tape. Refer to the procedure “Cleaning the DAT drive” in the CS 2000 Core Manager Fault Management document, NN10082-911.

  ***Note:*** Nortel Networks recommends that you upgrade your system directly from tape only if you are unable to complete the procedure Software upgrades from tape on page 196.

- Execute a ‘querysdm config’ command on the CS 2000 Core Manager and record the output for reference purposes.
- Execute a ‘sdmmtc hw’ command on the CS 2000 Core Manager to check if you have X.25 device installed. Record the output for reference purposes.
- Ensure that the following hardware spares are on site (check which versions of these cards you have on your system):
  - CPU controller card
  - DS512 controller card
  - spare hard drive module
  - spare DAT/hard drive module
- Ensure that adequate backup space is available on the Communication Server 2000 core, because the upgrade procedure stops the Billing Application for
  - over 1 hour (OOS Upgrade Procedure)
  - approximately 20 minutes (ESUP)

  To determine the amount of backup space required, refer to “Preparing for SBA installation and configuration” in the Accounting document. To reconfigure backup volumes, refer to “Configuring SBA backup volumes” in the Accounting document.

**System audit pre-check**

The purpose of the system audit pre-check is to execute a sanity check on various components of the CS 2000 Core Manager. For more information on the system audit functionality, refer to the “System audit overview” in the CS 2000 Core Manager Basics document.

***Note:*** Once your system is upgraded to the CS2E0070 software load, the system audit will run automatically on a daily basis at 2 a.m. (default value). However, you are still required to run this pre-check manually before upgrading to CS2E0070.

## Installing the system audit script

### *At the VT100 console*

**1** Determine whether the system audit functionality exists on your CS 2000 Core Manager:

```
# ls -l /sdm/mtce/precheck/sysaudit
```

| If sysaudit script | Do |
|---|---|
| does not exist on your system | step 2 |
| exists on your system | Performing the system audit pre-check on page 178 |

**2** Determine the fileset source.

| If the fileset is | Do |
|---|---|
| on tape | insert the tape labeled CS2E0070.x (1 of 1) in slot 2, and continue with step 3<br>***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed. |
| in a directory | obtain the directory path where the fileset is located, and continue with step 4 |

**3** Install the system audit precheck software from tape:

```
# installp -ad /dev/rmt0 SDM_PRECHECK.sysaudit
```

*Example response:*

```
installp:  Please mount volume 1 on /dev/rmt0.1.
```

Press the Enter to key to continue.

*Example response:*

```
+-----------------------------------------+
     Pre-installation Verification...
+-----------------------------------------+
Verifying selections...done
Verifying requisites...done
Results...

SUCCESSES
---------
Filesets listed in this section passed
pre-installation verification and will be installed.
```

```
Selected Filesets
-----------------
SDM_PRECHECK.sysaudit 1.0.0.0    # System pre-check
                                   tools

  << End of Success Section >>
FILESET STATISTICS
------------------
    1  Selected to be installed, of which:
       1  Passed pre-installation verification
    1  Total to be installed
+-----------------------------------------+
          Installing Software...
+-----------------------------------------+

installp:    APPLYING software for:
           SDM_PRECHECK.sysaudit 1.0.0.0

Finished processing all filesets.  (Total time:
                                    1 mins 44 secs).

+-----------------------------------------+
                 Summaries:
+-----------------------------------------+

Installation Summary
--------------------
Name            Level     Part  Event     Result
-------------------------------------------------
SDM_PRECHECK.   1.0.0.0   USR   APPLY     SUCCESS
sysaudit
```

Once you have completed this step, go to Performing the system audit pre-check on page 178.

**4** Install the system audit precheck software from a directory:

**`# installp -ad <dir> SDM_PRECHECK.sysaudit`**

*where:*

**<dir>**
is the directory where the fileset is located

*Example response:*

```
+-----------------------------------------+
     Pre-installation Verification...
+-----------------------------------------+
Verifying selections...done
Verifying requisites...done
Results...

SUCCESSES
---------
```

```
Filesets listed in this section passed
pre-installation verification and will be installed.

Selected Filesets
  -----------------
SDM_PRECHECK.sysaudit 1.0.0.0     # System pre-check
                                    tools

  << End of Success Section >>
FILESET STATISTICS
------------------
    1  Selected to be installed, of which:
       1  Passed pre-installation verification
    1  Total to be installed
+-----------------------------------------+
          Installing Software...
+-----------------------------------------+

installp:     APPLYING software for:
          SDM_PRECHECK.sysaudit 1.0.0.0

Finished processing all filesets. (Total time:
                                    1 mins 44 secs).

+-----------------------------------------+
                Summaries:
+-----------------------------------------+
Installation Summary
--------------------
Name              Level    Part    Event    Result
-------------------------------------------------
SDM_PRECHECK.     1.0.0.0  USR     APPLY    SUCCESS
sysaudit
```

**5** You have completed this procedure. To perform the pre-check, follow the instructions in Performing the system audit pre-check.

### Performing the system audit pre-check

#### *At the VT100 console*

**1** Access the pre-check directory:

```
# cd /sdm/mtce/precheck
```

**2** Execute the system audit check:

```
#./sysaudit -all
```

*Response*

```
sysaudit command is in progress, please wait a
few minutes for it to complete...
```

3 Display the system audit report:

```
#./sysaudit -report
```

Use the procedure “Viewing the system audit report and taking corrective action” in the CS 2000 Core Manager Fault Management document, NN10082-911 (start at step 2) to analyze the report and take corrective action, if necessary.

4 Return to the default directory:

```
# cd
```

5 You have completed this procedure.

## Hardware baseline pre-check

The purpose of the hardware baseline pre-check is to display the hardware PEC codes and ensure compatibility with the CS2E0070 hardware baseline.

You must upgrade any hardware that does not meet the minimum hardware baseline before you proceed with the software upgrade.

### Performing the hardware baseline pre-check

***At the VT100 console***

1 Display the information for the hardware that is installed on the CS 2000 Core Manager:

```
# locate
```

2 Refer to Hardware baseline on page 528 and verify that the product engineering codes (PECs) on the output meet the minimum hardware baseline.

3 You have completed this procedure.

## CPU stability pre-check

The purpose of the CPU stability pre-check is to ensure that the master and checker CPU is operating as expected. The master CPU will be taken Offline and then returned to service.

> **WARNING**
> Because the master CPU will be Offline, the system will be in a NON-Fault tolerant mode for the duration of the pre-check.

### Performing the CPU stability pre-check

***At the VT100 console***

1 Determine which CPU is currently master:

```
# ftctl -status
```

*Example response:*

```
CPU module CPU-0:
    Current istate      = present
                        powered on
                        significant
                        checker
                        using backplane signals
    Current condition    = online
    Online start date    = Sun Mar 17 12:52:53 CST 2002
    Online duration      = 23 days, 06:52:36
CPU module CPU-1:
    Current istate      = not present
    Current condition    = offline
CPU module CPU-2:
    Current istate      = present
                        powered on
                        significant
                        master
                        using backplane signals
    Current condition    = online
    Master start date    = Sun Mar 17 12:44:37 CST 2002
    Master duration      = 23 days, 07:00:52
    Online start date    = Sun Mar 17 12:44:37 CST 2002
    Online duration      = 23 days, 07:00:52
```

**2** Access the hardware level to determine if the CPU modules are in service:

```
# sdmmtc hw
```

*Example response:*

```
  SDM   CON  512  NET  APPL SYS  HW  CLLI: OTWAONXBEC3
   .     .    ..   .     .    .   .  Host: pcary989
   .          ..   .                  Fault Tolerant
Hw
 0 Quit
 2              I  F  C  D  D  D  E  E  D  5
 3              C  A  P  S  S  S  T  T  A  1
 4 Logs         M  N  U  K  K  K  H  H  T  2
 5                       1  2  3  1  2
 6      Domain 0 .  .  .  .  .  .  .  .  .  .
 7 Bsy  Domain 1 .  .  .  .  .  .  .  .  .  .
 8 RTS
 9
10
11
12
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh
 root
Time 11:15 >
```

**3** Busy the master CPU:

```
> bsy  <domain> cpu
```

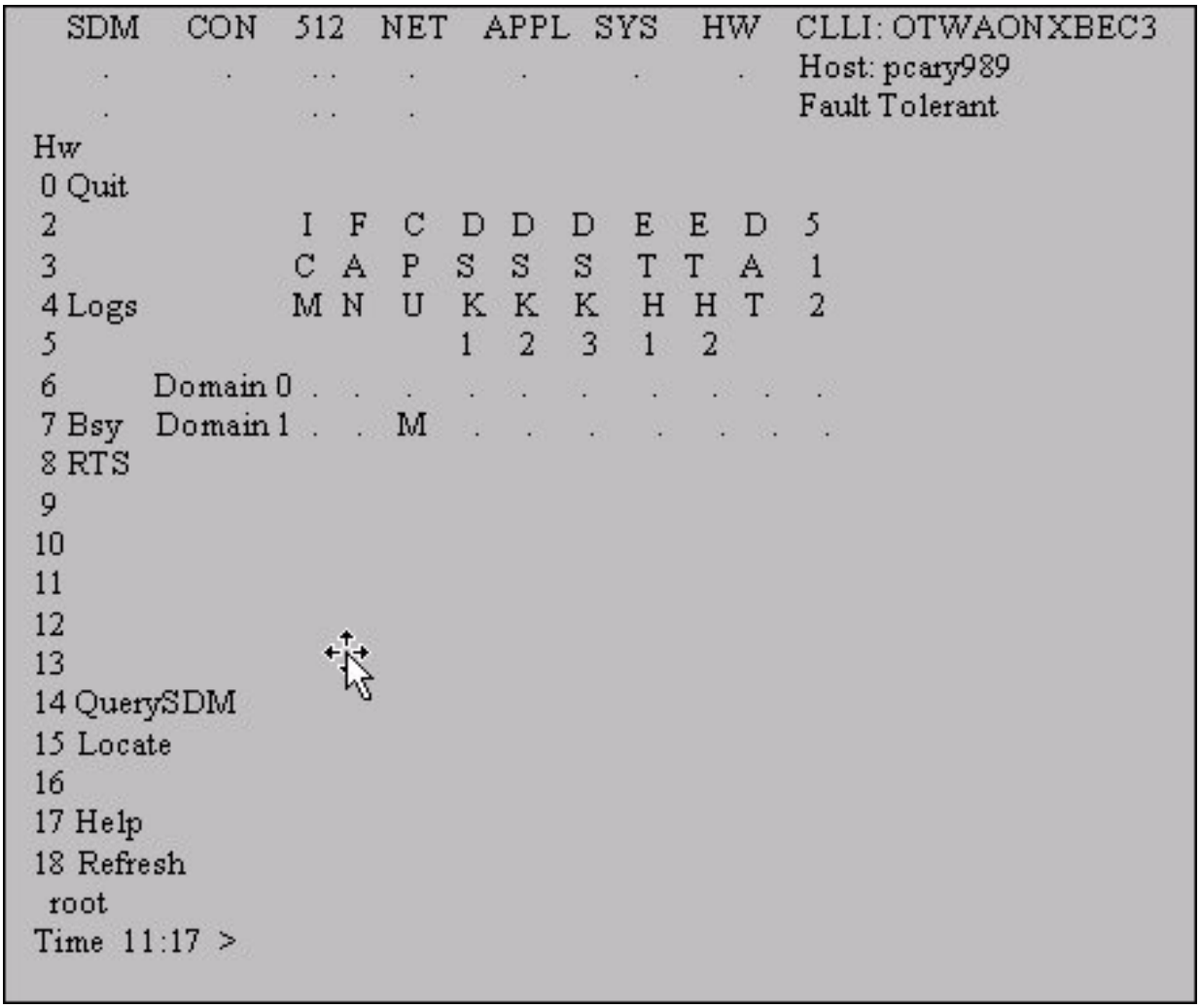
*where*

**<domain>**
is the domain number of the master CPU identified in step 1.

**Example**

```
# bsy 1 cpu
```

*Example response:*




**4** Return the busy CPU to service:

```
> rts  <domain> cpu
```

*where*

**<domain>**
is the domain number of the master CPU you busied in the previous step 3

**Example**

```
# rts 1 cpu
```

| If the rts command | Do |
|---|---|
| succeeds | step 6 |

| If the rts command | Do |
|---|---|
| fails | step 5 |

**5** The CPU reintegration can fail because the system is too busy. To determine that, examine the eeprom on the failing CPU and look for the following message: `PRI: System too busy, PRI could not complete.`

*Example response:*

```
# eeprom -vL CPU-2
.
.

Event    Time - Date          Failure Category & Reason
=====    ===========          =========================

Power on 13:59 Mar 11 2002 EST

Failure  13:59 Mar 11 2002 EST Information report

  PRI: System too busy, PRI could not complete
```

This message does not indicate a faulty CPU (no matter how many times it fails). This message means that the system is presently too busy to reintegrate the CPUs, and the reintegration must be deferred until the system load is reduced. You can attempt the reintegration as many times as necessary, until it succeeds. Once you have successfully reintegrated the CPUs, go to step 6.

***Note:*** To reduce the system load, you may have to busy SBA or the SDM from the core in a maintenance window.

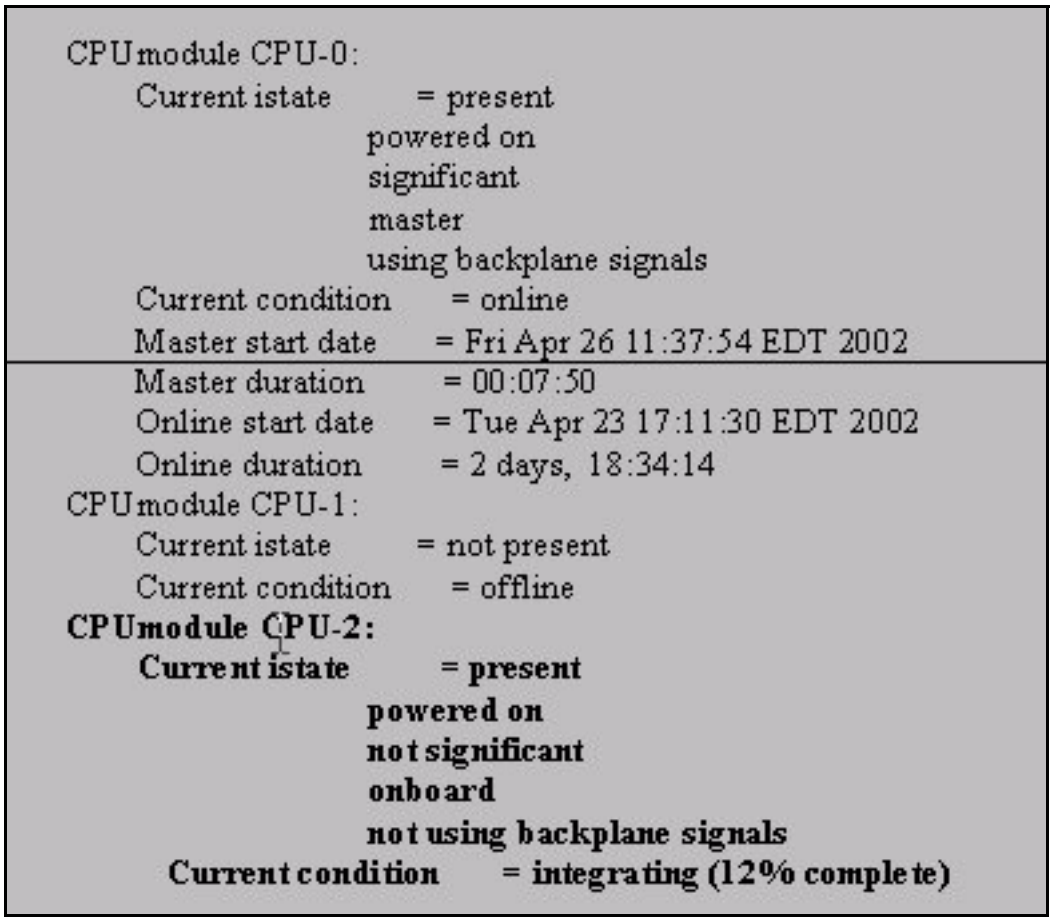
**6** Exit the hardware level:

```
> quit all
```

**7** Monitor the integration status of the CPU:

```
# ftctl -status
```

*Example response:*


CPU module CPU-0:
Current istate = present
powered on
significant
master
using backplane signals
Current condition = online
Master start date = Fri Apr 26 11:37:54 EDT 2002
Master duration = 00:07:50
Online start date = Tue Apr 23 17:11:30 EDT 2002
Online duration = 2 days, 18:34:14
CPU module CPU-1:
Current istate = not present
Current condition = offline
CPU module CPU-2:
Current istate = present
powered on
not significant
onboard
not using backplane signals
Current condition = integrating (12% complete)

**8** Wait until the CPU has been fully integrated, then re-enter the hardware level to ensure that the CPU has returned to service:

```
# sdmmtc hw
```

*Example response:*

```
  SDM   CON  512  NET  APPL SYS   HW  CLLI: OTWAONXBEC3
   .     .    ..   .     .    .    .   Host: pcary989
   .          ..   .                   Fault Tolerant
Hw
0 Quit
2              I  F  C  D  D  D  E  E  D  5
3              C  A  P  S  S  S  T  T  A  1
4 Logs         M  N  U  K  K  K  H  H  T  2
5                       1  2  3  1  2
6       Domain 0 .  .  .  .  .  .  .  .  .  .
7 Bsy   Domain 1 .  .  .  .  .  .  .  .  .  .
8 RTS
9
10
11
12
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh
 root
Time 11:47 >
```

**9** Repeat steps 3 to 8 for the second CPU. For example, if previously you have busied and returned to service CPU 1, repeat steps 3 to 8 for CPU 0.

**10** You have completed this procedure.

## DS512 fiber link pre-check

The purpose of the DS512 fiber link pre-check is to identify potential problems with the DS512 fiber links connected from the core to the DS512 controller modules on the CS 2000 Core Manager. It may also identify problems with DS512 modules.



**CAUTION**
**Possible loss of communication to the core**
The DS512 fiber link pre-check results in a temporary simplex condition on CS 2000 Core Manager links to the Communication Server 2000 core. Therefore, you must perform the DS512 fiber link pre-check during a maintenance shift to ensure that the traffic on the DS512 links does not lead to message overload conditions, which could result in a loss of communication with the Communication Server 2000 core.

***At the MAP terminal***

**1** Access the SDM level of the MAPCI:

```
> mapci;mtc;appl;sdm
```

**2** Identify the message switch (MS) chain cards that are configured with the DS512 controller modules and the associated DS512 fiber links that communicate from the core to the CS 2000 Core Manager:

```
> trnsl
```

*Example response:*

```
XAC    MS   IOD   Net   PM   CCS   Lns   Trks  Ext   APPL
 .      .    .     .     .    .     .     ...   .     .

SDM          OAMAP ATMFW  SDM  SPMCP SWMTC SDMBIL    TOPSIP
0 Quit         .     .     .    .     .     .          .
2
3       SDM 0 InSv    Links_OOS: .
4
5 Trnsl
6          Trnsl
7 Bsy        SDM 0 DOMAIN 0 PORT 0 (MS 0:05:0) OK    MsgCnd:Open
8 RTS        SDM 0 DOMAIN 0 PORT 1 (MS 1:05:0) OK    MsgCnd:Open
9 OffL       SDM 0 DOMAIN 1 PORT 0 (MS 0:05:1) OK    MsgCnd:Open
10           SDM 0 DOMAIN 1 PORT 1 (MS 1:05:1) OK    MsgCnd:Open
11
12
13
14 QuerySDM
15 Locate
16
17
18 Platform
 ADMIN
Time 11:28 >
```

**3** Post the chain card that corresponds to one of the four associated DS512 fiber links that communicate with the CS 2000 Core Manager.

```
# mapci;mtc; ms;shelf;chain <chain_number>
```

*where:*

**<chain_number>**
is the number of the MS chain card

**Example**
# mapci;mtc;ms;shelf;chain 5

*Example response*

```
 XAC    MS   IOD   Net   PM   CCS   Lns   Trks  Ext   APPL
  .     .     .     .     .     .     .     .     .     .

CHAIN       I    Message Switch  Clock  Shelf 0    Inter-MS Link 0 1
 0 Quit     MS 0         .        Master      .                  . .
 2          MS 1         .        Slave       .                  . .
 3
 4          Shelf 0                        1 1  1  1
 5          Card  1 2 3 4 5 6 7 8 9 0 1 2 3
 6 Tst_     Chain          < >    |
 7 Bsy_      MS 0 . . . . . . . . . . . . .
 8 RTS_      MS 1 . . . . . . . . . . . . .
 9 Offl_
10          Chain   05     Range    Link    0 1
11          MS 0     .     05-06    DS512   . .
12 Chain_   MS 1      .    05-06    DS512   . .
13 Card_
14 QueryMS   6
15 Trnsl_
16
17
18
 OPERATOR
Time 11:53 >
```

**4** Busy the DS512 fiber links that correspond to the DS512 card to be busied:

**> bsy 0 link <link_number>**

**> bsy 1 link <link_number>**

*where:*

**<link_number>**
is the number of the DS512 link (0 to 4)

Example
**> bsy 0 link 0**

and

Example
**> bsy 1 link 0**

The examples above will busy MS 0 link 0 and MS 1 link 0 for the DS512 card on domain 0.

***At the VT100 console***

**5** Access the hardware level:

```
# sdmmtc hw
```

**6** Busy the DS512 controller module:

```
> bsy <domain_number> 512
```

*where:*

**<domain_number>**
is the domain number of the DS512 link

**7** Return the DS512 controller module to service:

```
> rts <domain_number> 512
```

*where:*

**<domain_number>**
is the domain number of the DS512 link

| If the DS512 controller module | Do |
|---|---|
| returns to service | step 8 |
| does not return to service | contact your next level of support |

***At the MAP terminal***

**8** Return the DS512 fiber links that correspond to the DS512 card to service:

```
> rts 0 link <link_number>
```

```
> rts 1 link <link_number>
```

*where*

**<link_number>**
is the number of the DS512 link (0 to 4)

Example
**> rts 0 link 0**

and

Example
**> rts 1 link 0**

The examples above will return MS 0 link 0 and MS 1 link 0 for the DS512 card on domain 0 to service.

| If the links | Do |
|---|---|
| return to service | step 9 |
| do not return to service | contact your next level of support |

**9** Repeat the previous steps until each of the DS512 Controller Modules has been busied and returned-to-service successfully.

**10** You have completed this procedure.

**Application/fileset status and configuration pre-check**

The purpose of the application/fileset status and configuration pre-check is to verify that the applications on the CS 2000 Core Manager are in-service and configured.

***At the VT100 console***

**1** Access the application level:

```
# sdmmtc appl
```

*Example response:*

```
  SDM   CON   512   NET   APPL  SYS   HW   CLLI: OTWAONXBEC3
    .     .     ..    .     .     .     .    Host: pcary989
    .           ..    .                      Fault Tolerant
Appl
0 Quit
2             # Application                   State
3             1 SDM Billing Application        .
4 Logs        2 Generic Data Delivery          .
5             3 Log Delivery Service           .
6             4 Image Dump Service             .
7 Bsy         5 Secure File Transfer           .
8 RTS         6 Enhanced Terminal Access       .
9 OffL        7 Table Access Service           .
10            8 OM Access Service              .
11                    Applications showing: 1 to 8 of 8
12 Up
13 Down
14 QuerySDM
15 Locate
16
17 Help
18 Refresh
 root
Time 06:30 >
```

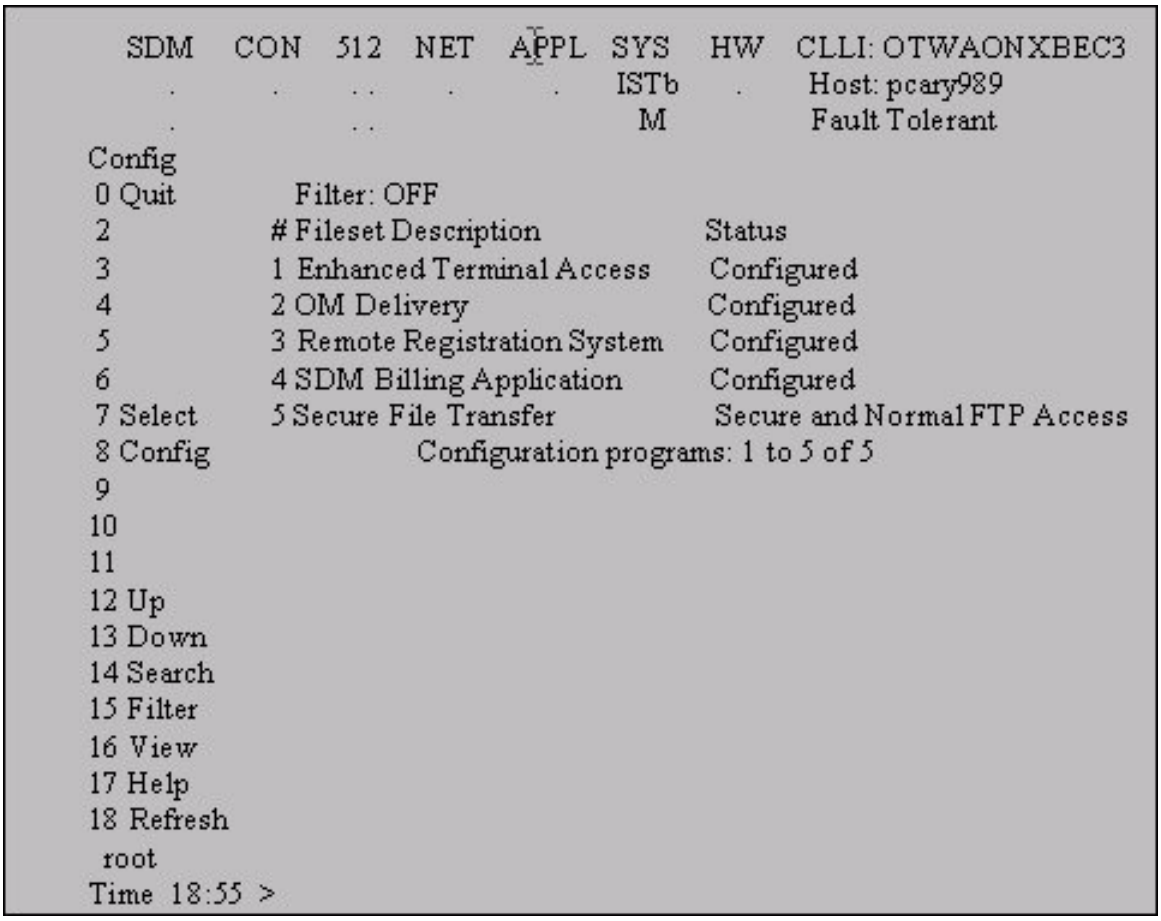
**2** Verify that all applications used are in service (represented by a dot [.] under the “State” header). Use the up/down commands to scroll through the list of applications if necessary.

| If | Do |
|---|---|
| all applications are in service | step 3 |
| one or more applications are not in service | investigate and return to service if required before you proceed |

**3** Access the configuration level:

```
# config
```

*Example response:*




**4** Verify that all required in-service applications are configured. Use the up/down commands to scroll through the list of applications if necessary.

**5** You have completed this procedure.

## User configuration pre-check

The purpose of the user configuration pre-check is to ensure that the CS 2000 Core Manager user attributes are configured correctly.

### Performing the user configuration pre-check

#### *At the VT100 console*

**1** Display the user attributes for the root user:

```
# lsuser root
```

2 Display the user attributes for the maint user:

```
# lsuser maint
```

*Example response*

```
3004-687 User "root" does not exist.
```

| If the user | Do |
|---|---|
| does not exist | contact your next level of support |
| exists | proceed to the next task Ethernet configuration pre-check |

3 You have completed this procedure.

## Ethernet configuration pre-check

The purpose of the Ethernet configuration pre-check is to display the status and configuration of the Ethernet interfaces.

### Performing the Ethernet configuration pre-check

***At the VT100 console***

1 Identify and record the IP address for an external network element than can be used to test network continuity.

```
# hostent -s
```

***Note:*** Select a known functional external network element. Do not use the loopback or proprietary DS512 CM and SDM IPs.

2 Display the configuration and status of the Ethernet interfaces:

```
# dbgent
```

*Example response:*

```
ent0:
    member0 pent0 active (08:00:3e:26:0f:90)   PM: online
    member1 pent2 backup (08:00:3e:26:0f:94)   PM: online
```

3 Verify that the selected external network element can be reached.

```
# ping -c 3 <ip_address>
```

4 Switch the active and backup Ethernet interfaces.

```
#  dbgent -sl ent0
```

5 Verify that the switch occurred.

```
# dbgent
```

*Example response:*

```
ent0:
    member0 pent0 backup (08:00:3e:26:0f:94)  PM: online
    member1 pent2 active (08:00:3e:26:0f:90)  PM: online
```

6 Verify that the selected external network element can still be reached.

```
# ping -c 3 <ip_address>
```

7 Switch the active and backup Ethernet interfaces.

```
#  dbgent -sl ent0
```

8 Verify that the switch occurred.

```
# dbgent
```

9 Verify that the selected external network element can still be reached.

```
# ping -c 3 <ip_address>
```

10 You have completed this procedure.

# Software upgrades from tape

**ATTENTION**
If you are planning to upgrade your system from tape, upload the software from tape to a disk, and then upgrade your system from the directory created during this procedure, in order to avoid any potential tape problems during the upgrade.

The purpose of transferring the upgrade software from tape to a disk is to help ensure a trouble-free upgrade by avoiding tape problems that can occur during the upgrade.

## Installing the UPGRADE Tools fileset

### *At the VT100 console*

1 Log on to the CS 2000 Core Manager using the root user ID and password.

2 Verify that tape drive 0 (slot 2) and tape drive 1 (slot 13) have been cleaned during the Basic pre-checks procedure. If not, clean both tape drives now. Refer to the procedure “Cleaning the DAT drive” in the CS 2000 Core Manager Fault Management document, NN10082-911.

3 Insert the tape labeled “CS2E0070 NCL 7.x (1 of 1)” into the tape drive in slot 2 (DAT0) or slot 13 (DAT1).

4 Install the software that will be used later to copy the content of the tape to a disk, using one of the following commands.

- If the tape is inserted in slot 2:

```
# bffcreate -d /dev/rmt0.1 -t /home/swd -q
SDM_UPGRADE
```

- If the tape is inserted in slot 13:

```
# bffcreate -d /dev/rmt1.1 -t /home/swd -q
SDM_UPGRADE
```

***Note:*** Ignore the warning message that the system displays. Wait until the command is complete and continue with the procedure.

5 Access the maintenance interface:

```
# sdmmtc
```

6 List the filesets in directory /home/swd:

```
> apply /home/swd
```

7 Select the UPGRADE Tools fileset:

```
> select <x>
```

*where*

**<x>**
is the number next to the UPGRADE Tools fileset

8 Install the UPGRADE Tools fileset:

```
> apply
```

9 If prompted, confirm the apply command:

```
> y
```

10 Exit the sdmmtc interface:

```
> quit all
```

### Uploading the software from tape to a disk

#### *At the VT100 console*

1 Start the process of transferring the software load from tape to a disk:

```
# unpacktape
```

2 When prompted, select automatic or interactive method for creating the logical volume where the tape content will be transferred. Enter one of the following values:

- `1` - if you want the system to create the logical volume
- `2` - if you want to create the logical volume or select an existing logical volume

***Note:*** If there is not enough disk space on your system, the procedure will automatically abort. Contact your next level of support for further instructions.

3 When prompted, enter the location of the tape:

- **0**
  if the tape is inserted in slot 2
- **1**
  if the tape is inserted in slot 13

| If in step 2 you have selected option | Do |
|---|---|
| automatic | the system provides the location of the directory where the tape load is being transferred. ***Record the directory path for reference***, then go to step 8. |
| interactive | continue with step 4 |

4 When prompted, specify whether you want to transfer the tape load to an existing logical volume. Enter one of the following values:

- **yes** - if you want to transfer the load to an existing logical volume

  ***Note:*** Make sure that you have at least 1400 Mbytes of free space in the existing logical volume.

- **no** - if you want to create a new logical volume

5 Use the following table to determine your next step.

| If you entered | Do |
|---|---|
| yes | enter the directory path where you want to transfer the load, and press the Enter key. Go to step 8. |
| no | go to step 6 |

6 To continue the procedure, enter:

```
# yes
```

7 When prompted, enter the full path to the new directory where the new logical volume will be mounted.

***Note:*** If there is insufficient free space on datavg and rootvg, the system aborts the procedure. Contact your next level of support for further instructions.

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

| If the system | Do |
|---|---|
| completes the transfer and displays the following message:<br>`Successfully deposited all filesets to <directory name>`<br>**Record the directory path for reference.** | go to step 11 |
| displays a failure message<br>***Note:*** If this is your second attempt to complete the procedure, contact your next level of support. | go to step 9 |

**9** Clean the DAT drive where the tape is inserted. Refer to the procedure “Cleaning the DAT drive” in the CS 2000 Core Manager Fault Management document, NN10082-911.

**10** Once the DAT drive is clean, repeat steps 1 through 8.

**11** You have completed this procedure. You are now ready to upgrade the CS 2000 Core Manager software.

# Preparing your system for upgrade using Electronic Software Delivery

## Purpose

Use this procedure to prepare the CS 2000 Core Manager for an ESD upgrade, which includes the following tasks:

- Preparing the repository server for the CS 2000 Core Manager load on page 202
- Preparing the CS 2000 Core Manager for file transfer from the repository server on page 206

## Prerequisites

If the files already exist in a directory on the CS 2000 Core Manager, proceed with the OOS Upgrade Procedure or ESUP upgrade using the appropriate procedure.

For the network path between the Nortel Networks software vault and a customer's CS 2000 Core Manager, the repository server is the last file transfer point prior to the CS 2000 Core Manager. The server must have enough disk space to hold, uncompress and unarchive the CS 2000 Core Manager load. Once all of the CS 2000 Core Manager filesets are extracted, they are transferred to the CS 2000 Core Manager from the repository server by FTP.

Before you can begin preparing the repository server for the CS 2000 Core Manager load, you will need a decompression tool on the repository server to extract the contents of the CS 2000 Core Manager load. The load transferred is a compressed tar file. If the tar file compression format used is .Z format (as seen by the filename), you will need the *uncompress* tool on the repository server. If the load transferred is in .gz format, you will need either a *gzip* or a *gunzip* tool. These tools and the **tar** command should be in your UNIX PATH environment variable.

**ATTENTION**

Ensure that you have 3 Gbytes of free space available on datavg. To check the free space on datavg, enter the command *sdmmtc storage* at the # command prompt.

This procedure assumes that you are using the FTP tool on the CS 2000 Core Manager to transfer the load from the external repository server to the CS 2000 Core Manager. Alternate transfer methods using

secure CS 2000 Core Manager applications such as Secure File Transfer (SFT) can be available, depending on your site configuration. SFT requires that

- both the CS 2000 Core Manager and repository server be configured as DCE clients within the same distributed computing environment (DCE) cell, and
- the required CS 2000 Core Manager software clients be installed on the repository server.

## Application

Electronic Software Delivery (ESD) uses standard network connectivity methods into the software distribution process for the CS 2000 Core Manager. ESD can be used for both NCL and MNCL upgrades. For more information about ESD, refer to the Electronic Software Delivery Customer Implementation Guide.

## Procedures

### Preparing the repository server for the CS 2000 Core Manager load

***On the client workstation***

**1** Choose a directory location on the repository server to which the CS 2000 Core Manager load can be transferred by FTP. Ensure that this location has sufficient space for the load and its subsequent extraction. To determine space availability on the server, use the **`df -k.`** command:

***Note:*** The uncompressed tar file for a major release of an CS 2000 Core Manager software load usually ranges from 1 to 1.5 gigabytes. You will need this amount of space for the uncompressed tar file, in addition to at least the same amount for the file's extracted content. It is recommended that you have a total of at least 5 gigabytes available.

**2** Change to repository directory:

```
> cd <directory_path_A>
```

*where*

**<directory_path_A>**
is the directory location on the repository server to which the CS 2000 Core Manager load is transferred, uncompressed and untarred before transfer to the CS 2000 Core Manager

*Example command*

```
> cd /local
```

3 Create a directory for the CS 2000 Core Manager product load:

```
> mkdir CS2E0070
```

4 Access the CS2E0070 directory:

```
> cd CS2E0070
```

5 Transfer the CS 2000 Core Manager product load by FTP to the repository server at your current location. After you have completed this step, the CS 2000 Core Manager load (a compressed tar file) appears in your current location

6 Display your directory:

```
> pwd
```

*Example response*:

```
/local/CS2E0070
```

7 List the files in the directory:

```
> ls -al
```

*Example response*

```
total 2333988
drwxr-xr-x    2 root       other        512  Nov  21  01:25  .
drwxr-xr-x   16 root       root        1024 Nov  18  14:48  ..
-rw-r--r--    1 root       other   1194397577   Nov  16 14:02
CS2E0070.7.V.NCL.NAP.VAULT.2.D.tar.gz
```

8 Check the disk space availability on the server:

```
> df -k.
```

The system displays the free unallocated disk space.

9 Unzip the file using one of the following commands (depending on the tool you have available):

```
> gunzip <order_name>.tar.gz
```

or

```
> gzip -d <order_name>.tar.gz
```

*where*

**<order_name>**
is the order name for the current load of this release

*Example command*:

```
> gunzip CS2E0070.7.V.NCL.NAP.VAULT.2.D.tar.gz
```

or

```
> gzip -d CS2E0070.7.V.NCL.NAP.VAULT.2.D.tar.gz
```

***Note:*** Because the size of the load file, the decompression process can take approximately 8 to 10 minutes, depending on the computing capabilities of the repository server.

**10** List the files in the directory:

```
> ls -al
```

*Example response*

```
total 2462180
drwxr-xr-x    2 root       other        512  Nov  21  01:39  .
drwxr-xr-x   16 root       root        1024 Nov  18  14:48  ..
-rw-r--r--    1 root       other   1260001280   Nov  16 14:02
CS2E0070.7.V.NCL.NAP.VAULT.2.D.tar
```

**11** Unarchive (un tar) the filesets:

```
> tar -xvf <order_name>.tar
```

*where*

**<order_name>**
is the order name for the current load of this release

The system creates a subdirectory (for example, CS2E0070.7.V.NCL.NAP.VAULT.2.D) and displays a listing of each file as it is unarchived and placed in this subdirectory.

***Note:*** If errors (such as insufficient disk space) occur during the untarring process, resolve the errors and repeat this step.

**12** Use the following table to determine your next step.

| If you | Do |
|---|---|
| want to delete the tar file to conserve disk space | step 13 |
| do not want to delete the tar file | step 14 |

**13**



**CAUTION**

Be sure that untarring the load file was successful (that is, that the disk did not run out of space during the extraction) or that the load is still available on the server from which you obtained the load.

To conserve disk space, remove the tar file:

```
> rm <order_name>.tar
```

*where*

**<order_name>**
is the order name for the current load of this release

*Example command*:

```
> rm CS2E0070.7.V.NCL.NAP.VAULT.2.D.tar
```

Go to step 15.

**14** Move the tar file to a different directory:

```
> mv <file_name> <directory_path>
```

*where*

**<file name>**
is the name of the tar file

**<directory path>**
is the location of the directory to which you are moving the tar file

***Note:*** Note the path to this directory for later use (when using FTP to transfer files to the CS 2000 Core Manager).

**15** You have completed this procedure.

## Preparing the CS 2000 Core Manager for file transfer from the repository server

### *At the client workstation*

1 Log into the CS 2000 Core Manager using your root user ID and password.

2 If you want to convert an existing logical volume, go to step 3. Otherwise, go to step 6.

3 Access the logical volume directory that you want to convert:

```
# cd <directory_path>
```

*where*

**<directory_path>**
is the logical volume directory that you want to convert

4



**CAUTION**

The **rm** command will remove all files and subdirectories from the current directory. Make sure that you are in the correct directory by typing **pwd**. The system displays the name of the current working directory. If it is the directory that you want to convert, proceed with the **rm** command. Otherwise, repeat step 3 to access the directory that you want to convert.

Remove all files and subdirectories within this logical volume directory:

```
# rm -r *
```

5 Perform a backup using the procedure “Creating system image backup tapes (S-tape) manually” in the Security and Administration document so that you can restore your system at any time if necessary.

If the alarm is enabled, and you choose not to perform a backup, you can force-clear the alarm using the procedure “Clearing a system image backup Required or Failed alarm” in the Fault Management document.

6 Access the storage level:

```
# sdmmtc storage
```

**7** Add a logical volume to store the ESD loads:

```
> esdadd
```

The system prompts you to enter a logical volume to be converted to the /swd/sdm/esd standard.

***Note 1:*** When converting a logical volume to the /swd/sdm/esd standard, no contents are changed in the old logical volume.

***Note 2:*** The CS 2000 Core Manager will go in-service trouble (ISTb) and the status of the Backup Status alarm will be *Required* once you convert a logical volume to the /swd/sdm/esd standard. If the backup Required alarm is disabled, the alarm is not raised

| If you | Do |
|---|---|
| want to convert an existing logical volume | enter the name of the logical volume to be converted (including the leading forward slash ( / ) symbol), press the Enter key, and go to step 9 |
| do not want to convert an existing logical volume | press the Enter key and go to step 8 |

**8** When prompted, enter the size (in MB) of the logical volume, or press the Enter key to accept the default value of 2000 MB.

***Note:*** Select the default size. If you do not enter a large enough size for the logical volume, you cannot put the entire load on the system. If necessary, you can increase the size of a logical volume using the procedure “Increasing the size of a logical volume” in the Security and Administration document.

The logical volume */swd/sdm/esd* is created.

**9** Exit the maintenance interface:

```
> quit all
```

**10** Change to the /swd/sdm/esd upgrade directory:

```
# cd /swd/sdm/esd
```

**11** Use FTP to transfer the files from the repository server to the ESD directory.

*Example of file transfer commands and responses*:

```
# ftp 10.102.128.2 (example IP address)
Connected to 10.102.128.2
220 TimeServer FTP server (SunOS 5.7) ready.
Name (10.102.128.2:root): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /local/CS2E0070/CS2E0070.7.V.NCL.NAP.VAULT.2.D
250 CWD command successful.
ftp> lcd /swd/sdm/esd
Local directory now /swd/sdm/esd
ftp> bin
200 Type set to I.
ftp> prompt off
Interactive mode off.
ftp> mget *
  (files transfer)
ftp> quit
```

**12** You have completed this procedure, and can now proceed to upgrade your system from disk.

# Preparing to upgrade the IW SPM IP

## Upgrade overview

Interworking Spectrum Peripheral Module - Internet Protocol (IW SPM IP) upgrades are performed on a circuit pack by circuit pack basis. Upgrading the software on all the individual circuit packs will upgrade the IW SPM IP.

The upgrade process requires upgrading the software in the IW SPM circuit packs. A separate load exists for each type of circuit pack. Software upgrades require the following sequence:

- SRM
- GEM
- CEM

An IW SPM upgrade involves upgrading circuit pack software loads. The circuit packs are grouped into circuit pack protection groups. A manual upgrade consists of the following phases:

- Check alarms on the IW SPM before starting the upgrade
- Verify the status of the IW SPM carriers before starting the upgrade.
- Update the circuit pack load inventory.
- Upgrade all RM circuit pack protection groups that require an upgrade
- For each RM circuit pack protection group, upgrade all circuit packs in the groups that require an upgrade.
- Upgrade CEMs that require an upgrade.

## Upgrade Methods

An IW SPM upgrade consists of upgrading the software on all of the individual circuit packs on an IW SPM. Two different upgrade methods are available:

- Automated upgrades
- Manual upgrades

The automated method upgrades several circuit pack types at once. The manual method upgrades circuit pack types individually.

The Sync Resource Module (SRM) does not provide sparing therefore offices that use SRMs on an IW SPM IP for office synchronization must upgrade the SRMs prior to using the Automated Upgrade process. All

SRMs must be upgraded manually before beginning the Automated Upgrade procedure. Each office has two IW SPM IPs with an SRM and they which can be located in the SYNCLK table.

## Upgrade Preparation

Before performing an IW SPM upgrade, each of the following requirements should be met:

- an office image was taken in the last 24 hours
- all peripheral module (PM) logs are enabled
- the circuit pack is in-service and the activity state is inactive
- automatic routine exercise (REX) testing is suspended in the office

During upgrade preparation, the new load files are transferred from a tape to a disk drive. An upgrade tape can consist of any of the following:

**Table 1 Upgrade Release Types**

| Release | Explanation |
|---|---|
| milestone | upgrades to the next base software release |
| maintenance or emergency | upgrades to a new release within the current base software release |
| Pre-Patched SPM Load (PPSL) milestone | upgrades to the next base software release with corrective content (patches) included |
| PPSL maintenance | upgrades to a new release within the current base software release and includes patches |

## Software Loads

The IW SPM Load tape contains the IW SPM loads, IW SPM patches, and $XREF file which is identified by “XPMxx” where “xx” refers to the IW SPM load. The automatic upgrade procedure uses $XREF files to apply patches after loading. If the $XREF files are not loaded, then patches must be manually applied.

PrePatched SPM Loads have patches built in as part of the load and are identified by an alpha numeric suffix at the end of the file name. For example:

| Load type | Numbering example |
|---|---|
| PPL | GEM19DE_010082A3 |
| non-PPL | GEM19DI_010086 |

The following table shows an example of load names that might be used in an IW SPM upgrade and the appropriate procedure to follow. In this example, a milestone upgrade would be performed from release16 to release 17. In contrast, a PPSL maintenance release requires only updating the file names in the PMLOADS table and does not require performing upgrade procedures in the last column.

**Table 2 Milestone release load example**

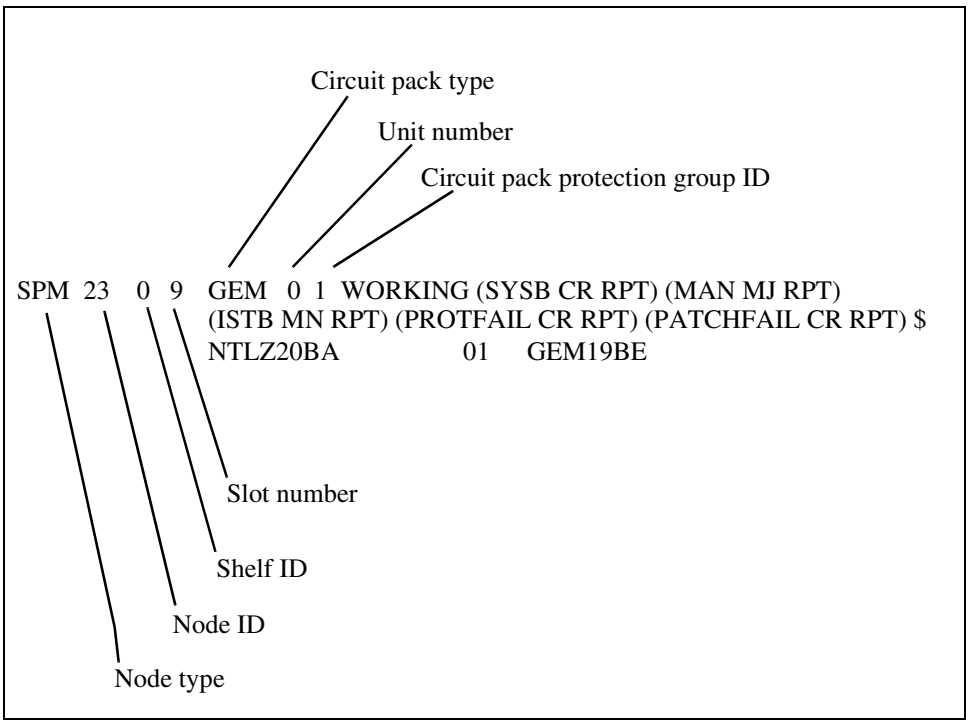
| Current load name in PMLOADS | Current active load file | New load name from SPM load tape contents | New active load file name from SPM load tape contents | Upgrade procedure to perform |
|---|---|---|---|---|
| SYN18BQ | SYN19BQ_010042 | SYN19AE | SYN20AE_010010 | Upgrading or Downgrading an SRM |
| GEM18AF | GEM19AF_010005 | GEM20AE | GEM20AE_010010 | Upgrade or Downgrade a GEM |
| IWS18AF | IWS19AF_010005 | IWS20AE | IWS20AE_010010 | Upgrading a CEM |

## Protection Groups

A protection group consists of multiple circuit packs grouped together for system reliability through sparing. Each protection group has a unique group identification (ID) assigned to it. The CEM does not belong to a protection group, and therefore does not have a circuit pack protection group ID.

The MNCKTPAK table contains a listing of each circuit pack in the IW SPM and associated protection group IDs. The following figure identifies the important fields in the MNCKTPAK table when performing an upgrade.

**Figure 1 Circuit pack upgrade fields**




The circuit pack protection group ID is a subfield of the CPKTYPE field. The following list identifies the subfield name for each RM type.

- GEM: IPGRPID
- SRM: SRMGRPID

The protection group ID in the MNCKTPAK table is defined in the MNPRTGRP table through the GRPKEY field, GRPID subfield. The GRPID subfield values range from1 through 28.

## Upgrade strategies

Nortel Networks strongly recommends completely loading entire IW SPMs with a single maintenance release or milestone upgrade. Failure to load all RMs and CEMs in an IW SPM can result in inadvertently running unsupported mixed load IW SPM configurations. Mixed load configurations can, in turn, result in the reload of modules in an out-of-procedure sequence, which can be potentially service affecting. If unable to complete the loading of all IW SPMs in one session, plan to upgrade a limited number of IW SPMs in multiple sessions.

During the upgrade process IW SPMs not loaded with an upgrade load reflect an ISTB condition caused by a loadname mismatch in the

MNCKTPAK table. The ISTB condition remains in effect until all IW SPMs have been upgraded.

Operating company personnel can upgrade more than one RM and more than one IW SPM at the same time.

To upgrade multiple RMs at the same time on the same IW SPM, open a MAPCI session for each RM type.

To concurrently upgrade multiple IW SPMs, Nortel Networks recommends upgrading up to two IW SPMs at the same time. Open a MAPCI session for each RM type on each IW SPM.

Note that during in-service loading, which involves downloading from the computing module (CM), you can load a maximum of eight RMs at the same time. The restriction of in-service loading no more than eight RMs at the same time also applies to CEMs. During mate loading, up to sixty four RMs can be loaded from the mate at the same time.

Periodically checking the carrier status during the upgrade process provides a method for monitoring the upgrade integrity.

For nonpatchable loads, post-release software updates (PRSU) must be built into the load file.

## PPSL

A Pre-Patched SPM Load (PPSL) is a Spectrum load which includes the released base software content and the corrective content (patches). PPSL advantages include:

- reduce patching effort after reloading
- reduce recovery time
- reduce end to end upgrade time

After loading a PPSL, new patches can be applied using standard tools and procedures through post release software management (PRSM). PRSM can also remove patch files that were built into a PPSL.

A PPSL file is named with the first fourteen characters of the base load plus two additional appended characters to indicate the version number. The two-character appendage uses an alpha numeric format. For example, a PPSL for the base load CEM19AE_010041 could be CEM19AE_010041A3.

The QUERYPM FILES command for a posted IW SPM at the PM MAP level indicates the existence of a PPSL for a CEM through the default filename. For example:

```
CEM 0 InSv Act  Default Loadname: IWS19AE
                  Default Filename: IWS19AE_010041A3
                Running Load:     IWS19AE_010041
                Load in Flash:    IWS19AE_010041
```

A REPORT DEST command through PRSM identifies a PPSL by displaying a PRSU in the SPMLOAD destination with a name comprised of “SPPSL” concatenated with the seven character load name. For example, SPPSLCEM19AE.

A PPSL maintenance release requires datafill changes made only to the PMLOADS table. The file and volume names must be updated to reflect the new PPSL load name and location.

## SPARTS

Patches applied to resource modules initially reside on the DRAM, the memory in which the load is running, of a device. The patched DRAM image does not copy over to the device's Flash memory until after patching activity has ceased on a device for a period of time. The delay between the end of the last patch action on the device and the start of the DRAM-to-Flash image copy varies depending on the load and the device:

- 60 minutes in SP14-16 loads (80 minutes for the inactive CEM in SP15-16)
- 5 minutes in SP17 and later loads (15 minutes for the inactive CEM)

It is possible that this delay could prevent patch updates to the PRSM database which would produce patching mismatches between the PRSM and the device's LPM (local patch manager). SPM Patching after RTS (SPARTS) addresses this issue.

When an RTS is initiated on a device, SPARTS obtains and compares a list of patches actually applied to the device to the patches applied to all other devices in the office that are running the same load. If no patch discrepancies exist, then SPARTS takes no further action. If patch discrepancies exist, SPARTS applies any missing patches to the device and likewise removes any applied patches that are not running on other devices with the same load within the office.

SPARTS raises a PATCHFAIL alarm against the IW SPM node (not the device) if it fails to apply or remove any required patches. SPARTS schedules up to three attempts, each spaced 30 minutes apart, to

correct a patch discrepancy. Once an attempt succeeds any subsequent attempts are cancelled and the PATCHFAIL alarm clears. A PATCHFAIL alarm can be manually cleared by running an ISTBAUDIT command against the device.

Run a DBAUDIT command against a device after loading or patching the first device. A DBAUDIT populates the PRSM database and ensures that SPARTS correctly handles patching on any other device loaded with the same load.

SPARTS does not apply a patch that has not already been applied in an office. SPARTS ensures that previously applied patches are applied every time an RTS is performed on a device.

## Downgrading

Like a software upgrade, a software downgrade loads a different version of software to the SPM components. A downgrade is only performed due to an error condition that necessitates returning to a previous software version.

The downgrade procedure is identical to the upgrade procedure, performed in reverse order, for all components except for the CEM. Those components require different treatment depending on whether the downgrade is to an earlier release or an earlier version within the same release.

Software downgrades cannot span beyond three previous releases. For example, it is possible to downgrade a release 20 to a release 17 but it is not possible to downgrade a release 20 to a release 16.

## Automated Upgrades

An automatic upgrade procedure, known as PANTHER, is designed only for upgrades and does not support software downgrades of any kind.

PANTHER consists of:

- the PMUPGRADE tool
  - — selects and copies the new PM load and patch files from the distribution media to the Core
  - — produces the PM upgrade plan outlining the tasks required to upgrade the PMs with the new loads and patches
- the SWUPGRADE PM tool
  - — automates task execution in the PM upgrade plan to load and patch the necessary PMs

Panther does not support the upgrade of unspared RMs therefore RM spares must be configured before beginning an automated upgrade.

PANTHER makes a set of eight SPMS for upgrade.It constructs an RM list that comprises the RM groups for all eight SPMs. The RM groups list contains RM groups of the first SPM in the current set sequentially followed by RM groups for the remaining SPMs.

Loading times for similar RM types vary only slightly, therefore PANTHER loads the RMs of similar protection groups concurrently to expedite the process without waiting for the slowest RM type to load. The loading times for the 8 RMs of similar RM protection type usually require the same amount of time and therefore the upgrade process does not wait for the slowest RM in the group to load.

PANTHER can concurrently mate load up to 64 RMs across 8 SPMs in the current upgrade set. The calculation for determining the maximum RMs available for mate loading is:

```
New RM Mate Loading Concurrency limit = 8(SPMs) *
8(Prot group per SPM) = 64
```

### $XREF Patch Control File

The PMUPGRADE tool uses an $XREF patch control file to select the required PRSUs for a load. An XA-Core tape cartridge labeled as *Patches:Yes* should contain the appropriate $XREF file for the corresponding load. If the tape does not contain an $XREF file, then the PMUPGRADE tool bypasses the steps to select or copy PRSUs and generates the following MAP message:

*WARNING: No Patch Control File Found. No patch files selected.*

When an office receives an $XREF file through an X.25 NOP link, the file must be placed on the Patch File Distribution volume and the corresponding PRSU files placed on temporary disk volumes specified

as the ISN Patch Destination volume and the XPM Patch Destination volume. PRSUs cannot reside on the same volume as the $XREF file.

The PMUPGRADE tool communicates the $XREF file name and location to the SWUPGRADE PM tool during the automated PM update. The SWUPGRADE PM tool accesses and automatically applies the PRSUs to any designated PM load files.

When downloading patches and loads through file transfer protocol (FTP) or other electronic methods, an $XREF file automatically generates if the following two conditions are met:

- all PM loads and corresponding patches are on a temporary disk volume
- no other $XREF file is present on the distribution volume

Electronically downloading patches and loads automatically copies the PM loads and their corresponding patches from the disk distribution volume to the selected destination volumes and generates a new $XREF file available for use by the SWUPGRADE tool.

## Tools and utilities

IW SPM IP upgrades are performed using the MAP display commands.

# Prepare an IW SPM IP automated upgrade

Use this procedure to prepare an automated (PANTHER) upgrade.

Before beginning the automated upgrade, ensure that spares are configured for all RMs requiring an upgrade.

Each destination volume must have sufficient free space for the new SPM load or PRSU files and meet all office criteria.

**ATTENTION**

The Sync Resource Module (SRM) in an IW SPM does not provide sparing therefore offices that use SRMs for IW SPM office synchronization must upgrade the SRMs prior to using the Automated Upgrade process. All SRMs must be upgraded manually before beginning the Automated Upgrade procedure. Each office has two IW SPM SRMs which can be located in the SYNCLK table.

Each destination volume must have sufficient free space for the new SPM load or PRSU files and meet all office criteria.

The Variable Abbreviations table defines the variables used in this procedure.

**Variable Abbreviations**

| Abbreviation | Definition |
|---|---|
| printer | the printer name |
| log_name | the name of a log type (PRSM, SPM, NODE, TUPL) |
| log_# | the specific number of a log type |
| spm_no | the number of the SPM (0 through 85) |
| shlf_no | the SPM shelf number |
| slot_no | the slot number of a designated shelf |
| printer | the printer name |
| dist_vol | the name of the new Load File Distribution volume |

### Variable Abbreviations

| Abbreviation | Definition |
|---|---|
| patch_vol | the name of the new Patch Distribution volume |
| load_number | the number of the current load |
| load_name_1 (2) (n) | the names of the loads to be included or excluded (repeat variable as needed) |

Throughout the upgrade procedure, the request to type a command requires pressing the Enter key on the keyboard after the command has been typed.

**ATTENTION**

Before beginning this procedure, update the SPM inventory table to prevent offline SPMs in the process of installation or commissioning from being part of the upgrade report plan.

Change the loadname field for any OFFL SPM to the new loadname.

### Prepare an automated upgrade

***At the CI level of the MAP display***

**1** Send the terminal response to a printer by typing

```
>RECORD START ONTO printer
```

*Example*

```
>RECORD START ONTO PRINTER1
```

**2** Enter the log utility and list devices for log output by typing

```
>LOGUTIL
>LISTDEVS
```

*Example of an active log output device*

```
No.  Device    Status           Rerouted   Format
---- -------   -------          ---------- -------
0    MAP121    Outputting Logs  No         STD
```

*Example of an inactive log output device*

```
No.  Device    Status      Rerouted   Format
---- -------   -------     ----------- -------
1    MAP121    Inactive.       No     STD
- End of devices -
```

| If the device is | Do |
|---|---|
| Inactive | step 3 |
| Active (outputting logs) | step 4 |

**3** Start the device by typing

**>STARTDEV device**

*Example of a MAP display*

```
>startdev map121
Log device MAP121 has been started.
Number of devices started : 1
```

**4** Verify that all reports for the PRSM, SPM, NODE, and TUPL log types are configured for output by typing

**>LISTREPS SPECIAL log_name**

*Examples*

**>LISTREPS SPECIAL PRSM**

**>LISTREPS SPECIAL SPM**

**>LISTREPS SPECIAL NODE**

**>LISTREPS SPECIAL TUPL**

*Example of all log type reports configured for output*

```
Log   Rep.        Event                        Suppressed/
Name  No. Class Type     Event Label          Thresholded       Syslog
-------------------------------------------------------------------------------
67 report(s)  printed
```

*Example of suppressed log type reports*

```
Log   Rep.          Event                        Suppressed/
Name  No. Class     Type    Event Label          Thresholded       Syslog
-------------------------------------------------------------------------------
SPM  650    0       PASS                          *supp*
SPM  651    0       FAIL                          *supp*
SPM  300    0       TBL   Device Fault Report    *supp*
```

| If log reports are | Do |
|---|---|
| suppressed | step 5 |
| not suppressed | step 8 |

**5** Resume any PRSM, SPM, NODE, and TUPL logs that have been suppressed by typing

**>RESUME log_name log_#**

*Example*

```
>resume spm 650
1 report(s) RESUMED
```

**6** Determine if the office uses SRMs for synchronization by typing

**>TABLE SYNCLK**

**>LIST**

*Example*

```
>table synclk
>list
CLKKEY              CLKDATA
                       OFFCDATA
  ------------------------------
 0                     STRAT3
SLAVE    SPM 64 SRM    SPM 68 SRM
```

| If the office | Do |
|---|---|
| contains SRMs | step 7 |
| does not contain SRMs | step 8 |

**7** Manually upgrade all nodes configured with a Sync Resource Module (SRM) by following these procedures:

| Procedure | Applies to the: |
|---|---|
| Prepare an IW SPM IP manual upgrade or downgrade | SRM load only in the procedure |
| Perform an IW SPM IP manual upgrade or downgrade | SRM load only in the procedure |
| Upgrading or Downgrading an SRM | the entire procedure |

When both SRMs have been manually upgraded continue to step 8.

**8** Identify the patch destination volume by typing

**>TABLE PADNDEV;LIST ALL;QUIT**

*Example*

```
TABLE: PADNDEV
```

```
TOP
DEVKEY        DEVICE
-------------------
      1  D030M17PTCH
      2  D030M15PTCH
      3    S01DIMAGE
BOTTOM
```

**9** Access the PMUPGRADE utility by typing

**>PMUPGRADE**

**10** Set confirmation to ON by typing

**>SET CONFIRMATION ON**

**11** Carryover loads are load files on the tape that have the same version of the load currently used in the office. Operating company personnel can issue a SET CARRYOVER ON command to copy all SPM loads for the office. The default carryover setting is OFF.

| If the office | Do |
|---|---|
| requires all SPM loads for the office be copied | step 12 |
| does not require all SPM loads for the office to be copied | step 13 |

**12** Set carryover to ON by typing

**>SET CARRYOVER ON**

**13** Confirm the Load File Distribution setting is correct. If necessary, change the setting by typing

**>SET LOADDISTRIB dist_vol**

*Example*

**>SET LOADDISTRIB F02UTAPE**

**14** Confirm the Load File Destination setting is correct. If necessary, change the setting by typing

**>SET LOADDEST dist_vol**

*Example*

**>SET LOADDEST F02LPMLOADS**

**15** Confirm the Patch File Distribution setting is correct. If necessary, change the setting by typing

**>SET PATCHDISTRIB patch_vol**

*Example*

```
>SET PATCHDISTRIB F02UTAPE
```

**16** The ISN, XPM, and SPM Patch Destination settings must point to the patch file destination volume. Confirm the ISN, XPM, and SPM Patch Destination settings are correct based on the PADNDEV table listing obtained in step 8. If necessary, change the setting by entering the following commands

```
>SET ISNPATCH patch_vol
```

```
>SET XPMPATCH patch_vol
```

```
>SET SPMPATCH patch_vol
```

***Note:*** The SPM patch destination volume should be entered in the PADNDEV table.

*Example*

```
>SET ISNPATCH F02LPMLOADS
```

```
>SET XPMPATCH F02LPMLOADS
```

```
>SET SPMPATCH F02LPMLOADS
```

**17** Generate an office load report by typing

```
>DISPLAY LOADS
```

*Result*

PMUPGRADE compiles the PMUPGRADE Load Report from the PMLOADS table and the SPM inventory tables.

***Note:*** A load can have an empty “Tables Used” column. If office policy requires data in this column, perform the following steps:

- Exit PMUPGRADE
- Delete the out-dated load from the PMLOADS table
- Go to step 9 of this procedure

**18** Generate a node report for the office by typing

```
>DISPLAY NODES
```

*Result*

The PMUPGRADE Node Report is compiled from SPM inventory tables. The node name information for the MNCKTPAK table is obtained from the MNNODE table.

**19** Display the firmware information by typing

```
>DISPLAY FWINFO
```

**20** Set the preferred load to the current load by typing

```
>SET FWPREFERRED load_number CURRENT
```

***Note 1:*** The preferred load must be equal to the current load.

***Note 2:*** Repeat this step for each firmware load listed in step 19.

**21** Start the file copy phase of the utility by typing

```
>START FILECOPY
```

*Time Requirements*

The FILECOPY process copies files to the destination volume and adds new loads to the PMLOADS table. The process requires approximately 40 minutes. The amount of time depends on the number of SPM loads and PRSU files.

**22** When prompted to confirm a tape is in its appropriate drive, confirm the tape is physically inserted in the drive. Do not use the INSERTTAPE or IT commands on the tape.

If the tape cartridge label text indicates “Patches:Yes”, the tape includes the required PRSUs for SPM load files.

**23** At the prompt, continue by typing

```
>Y
```

| If the response indicates | Do |
|---|---|
| that EXT files for datafill in the SPMLDVAL table are not available in the distribution volume | step 24 |
| the replacement load name cannot be found | step 25 |
| multiple replacement load names are found | step 26 |
| ready to continue | step 27 |

**24** Stop the automated upgrade by typing

```
>Q
```

Contact the next level of support to update the SPMLDVAL table.

**25** A response similar to the following example appears if PMUPGRADE cannot locate the replacement load name.

```
No replacement loadname found on distribution volume for SM206BH1.
Please enter replacement loadname, or "S" (Same) or "Q" (Quit FILECOPY)
```

| If | Do |
|---|---|
| A new load type replaces the current load type | Enter the new load name. Ensure the load name is typed accurately<br><br>Go to step 27 |
| The load is manufacture discontinued | Enter "S"<br><br>Go to step 27 |
| The load is a filler RM load name, indicating an RM that does not have a load | Enter "S"<br><br>Go to step 27 |

**26** If a response indicates that multiple replacements are found on the load distribution volume, enter the appropriate replacement listed or just the load name.

The loadname appears before the underscore in the load file name. For example, GEM19DE is the load name for the load file GEM19DE_010082A3.

**27** Review the Load File Selection Report and determine if any loads need to be added or removed from the report.

| If | Do |
|---|---|
| one or more loads need to be added or removed from the report | step 28 |
| the report is complete and no loads need to be added or removed | step 33 |

**28** Stop the file copy process by typing

**>N**

| If | Do |
|---|---|
| one or more loads need to be removed from the report | step 29 |
| one or more loads need to be added to the report | step 30 |

**29** Remove the loads from the report by typing

```
>SET EXCLUDELOADS load_name_1 load_name_2 ...
load_name_n
```

***Note:*** Separate each load name with a space.

*Example*

```
>SET EXCLUDELOADS BTMKA02 ECLI4BC
```

| If | Do |
|---|---|
| one or more loads need to be added to the report | step 30 |
| the report is complete and no loads need to be added or removed | step 31 |

**30** Add the loads to the report by typing

```
>SET INCLUDELOADS load_name_1 load_name_2 ...
load_name_n
```

***Note:*** Separate the load names with a blank space.

*Example*

```
>SET INCLUDELOADS BTMKA02 ECLI4BC
```

| If | Do |
|---|---|
| one or more loads need to be removed from the report | step 29 |
| the report is complete and no loads need to be added or removed | step 31 |

**31** Repeat the file selection phase of the utility by typing

```
>START FILECOPY
```

**32** Confirm that the appropriate load names have been added or removed from the Load File Selection Report.

| If the Load File Selection Report | Do |
|---|---|
| does not show the excluded and/or included load names | step 28 |
| shows the excluded and/or included load names | step 33 |

**33** Accept the Load Selection Report by typing

```
>Y
```

**34** Confirm the patch file selection prompt by typing

```
>Y
```

***Note:*** PMUPGRADE uses the $XREF patch control files to select PRSUs for copying. Depending on the method of PRSU delivery, this file may not be available. If the file is not available, PMUPGRADE generates a warning that no patch control file has been found. Contact your next level of support for instruction on how to proceed with the upgrade and a list of required PRSUs to be manually applied.

**35** Create the list of files to copy by typing

```
>Y
```

*Time Requirements*

This final phase of the FILECOPY process requires approximately 20 minutes to complete adding new loads to the PMLOADS table. The amount of time depends on the number of SPM loads and PRSU files.

**36**

**ATTENTION**
Perform this step only if any offline SPMs are being installed or commissioned in the office.

Open a second window and update the LOAD field in the MNCKTPAK field to reflect the new software load for each RM type in all offline SPMs

**37** Generate a PMUPGRADE load report for the office by typing

```
>DISPLAY LOADS
```

Confirm the selected new loads have been added to the report.

**38** Start the generation of the PM upgrade plan by typing

```
>START PLAN
```

***Note:*** Only one PM upgrade plan can be executed at a time. A new plan cannot be started until an existing plan has been cancelled or completed.

**39** Display the PM upgrade plan by typing

```
>DISPLAY PLAN
```

The PMUPGRADE Plan Report organizes the SPM upgrade by tasks and layers. A task is a set of SPMs of the same type at the

same site with the same load requirements. A layer is a grouping of tasks.

**40** Review the PMUPGRADE report.

- Confirm all SPMs that require upgrading are included in the plan report

  ***Note:*** For loads added to the Loadfile Selection Report with the SET INCLUDELOADS command, the associated SPMs must be manually upgraded.

- Confirm the correct loads are included with each task in the plan report.
- Confirm that the sequence of tasks in the plan report conforms to office policy.

  ***Note:*** If the sequence of tasks does not comply, use the RUNSTEP command during the automated SPM upgrade to change the order of tasks.

- Confirm offline SPMs that are being installed or commissioned in the office are not included in the plan report. If an offline SPM is included in the plan
  - — quit the PMUPGRADE process
  - — update the appropriate SPM inventory table. Change the loadname field for that SPM to the new loadname from the loadfile selection report.
  - — start this procedure again from step 8

**41** Exit the PMUPGRADE utility by typing

```
>QUIT
```

**42** Stop the terminal responses from printing by typing

```
>RECORD STOP ONTO printer_name
```

**43** Remove the SPM load tape from the tape drive.

Check office policy concerning additional copies of SPM load and PRSU files. Some offices require additional copies of SPM load and PRSU files on a parallel device.

### *At your desk*

**44** Any new hardware, identified by a Product Engineering Code (PEC), required for the software upgrade release must be installed.

| If each node | Do |
|---|---|
| has the required hardware | step 45 |
| does not have the required hardware | Contact your next level of support for more information. |

**45** You have completed this procedure.

# Prepare an IW SPM IP manual upgrade or downgrade

This procedure prepares the disk volume and file names in the PMLOADS and MNCKTPAK tables for a software upgrade. The Variable Abbreviations table defines the variables used in this procedure.

**Variable Abbreviations**

| Abbreviation | Definition |
|---|---|
| printer | the printer name |
| log_name | the name of a log type |
| log_# | the specific number of a log type |
| spm_no | the number of the node (0 through 85) |
| drive_no | the XA-Core tape drive number |
| tape_vol | the name of the tape cartridge volume |
| pc_file | the name of the patch control file |
| load_name | the load name of the new load (as it appears in the PMLOADS table) |
| act_file | the active load file name (as it appears in the PMLOADS table) |
| act_vol | the active volume name (as it appears in the PMLOADS table). The volume identifies the device where the act_ file is stored. |
| bkp_file | the backup load file name (as it appears in the PMLOADS table). The backup load file name should be identical to the act_file name. |
| bkp_vol | the backup volume name (as it appears in the PMLOADS table). The backup volume identifies where the bkp_file is stored. The backup volume name should be identical to the act_vol name. |
| disk_vol | the name of the backup disk volume |

### Variable Abbreviations

| Abbreviation | Definition |
|---|---|
| act_load | the name of the new active load (as it appears in the PMLOADS table) |
| shelf_ID | the shelf number (0 or 1) |
| slot_no | the number of slot location (1 through 14) |
| rm_name | the RM name (CEM, GEM, etc.) |
| rm_no | the RM number |

Throughout the procedure, the request to type a command requires pressing the Enter key on the keyboard after the command has been typed.

**ATTENTION**

Follow your company policy for soaking selected circuit packs before upgrading the rest of your office.

**ATTENTION**

The XA-Core command syntax for drive_no and disk_no correspond to the following identifiers in the XA-Core command examples:

Shelf position is the front (F) or rear (R) shelf position of the input output processor (IOP).

Slot position is the two-digit number of the slot position for the IOP with the tape device.

Packlet position is the upper (U) or lower (L) packlet position of the IOP with the tape device.

In the command example F17UTAPE, F is the shelf position, 17 is the two-digit slot position, U is the packlet position, and TAPE identifies the software delivery medium.

## Prepare a manual upgrade or downgrade

### *At the CI level of the MAP display*

**1** Send the terminal response to a printer by typing

**>RECORD START ONTO printer**

*Example*

**>RECORD START ONTO PRINTER1**

**2** Enter the log utility and list devices by typing

**>LOGUTIL**

**>LISTDEVS**

*Example of a MAP display*

```
No.  Device   Status          Rerouted   Format
---- -------  -------         ---------- -------
0  MAP121     Outputting Logs  No     STD
```

**3** Verify that logs are routed to a printer by typing

**>LISTREPS SPECIAL PRSM**

*Example of a MAP display*

```
Log   Rep.     Event                  Suppressed/
Name  No. Class Type  Event Label      Thresholded      Syslog
-------------------------------------------------------------------------------
16 report(s)  printed
```

**>LISTREPS SPECIAL SPM**

*Example of a MAP display*

```
Log   Rep.     Event                  Suppressed/
Name  No. Class Type  Event Label      Thresholded      Syslog
-------------------------------------------------------------------------------
67 report(s)  printed
```

**>LISTREPS SPECIAL NODE**

*Example of a MAP display*

```
Log   Rep.     Event                  Suppressed/
Name  No. Class Type  Event Label      Thresholded      Syslog
-------------------------------------------------------------------------------
11 report(s)  printed
```

**>LISTREPS SPECIAL TUPL**

*Example of a MAP display*

```
Log   Rep.     Event                  Suppressed/
Name  No. Class Type  Event Label      Thresholded       Syslog
-------------------------------------------------------------------------------
9 report(s)  printed
```

4 Resume any SPM, NODE, and TUPL logs that have been suppressed by typing

**>RESUME log_name log_#**

*Example*

**>RESUME SPM 311**

5 Post each IW SPM scheduled for an upgrade by typing

**>MAPC NODISP;MTC;PM;POST SPM spm_no**

6 List and print the loads on the SPM by typing

**>QUERYPM FILES**

7 Exit the SPM screen by typing

**>QUIT ALL**

8 Identify the patch destination volume by typing

**>TABLE PADNDEV;LIST ALL;QUIT**

*Example*

```
TABLE: PADNDEV
TOP
DEVKEY        DEVICE
------------------
     1 SFDEV
     2 F17LPTCH_CM
BOTTOM
```

9 Place the load tape into the tape drive of the selected disk volume.

10 Access the disk utility by typing

**>DISKUT**

*Response*

```
Disk utility is now active
```

11 Identify the PMLOADS volume by typing

**>LV**

*MAP Example*

```
Volumes found on the node CM:
```

```
-----------------------------
NAME                    TYPE      TOTAL       FREE
TOTAL   OPEN   ITOC     LARGEST
                                  BLOCKS      BLOCKS
FILES FILES FILES   FREE SEGMENT
-----------------------------------------------
--------------------------------
F17LIMAGE1           FTFS    2048000     305152
13      0      4     129024
F17LIMAGE2           FTFS    2048000     376832
12      0      0     169984
F17LIMAGE3           FTFS    2048000     362496
14      0      4     229376
F17LPMLOADS          FTFS     614400     409440
39      0      0     259904
F17LSPMLOADS         FTFS     819200     648544
15      0      0     464224
F17LPATCH             FTFS     81920      39264
318      0      0      39264
```

**12** Insert the load tape into the tape drive by typing

**`IT drive_no`**

*Example*

**`IT F02UTAPE`**

**13** List the load file contents of the tape by typing

**`LF drive_no`**

*Example*

**`>LF F02PMLOADS`**

**14** Identify the load files required for upgrading by comparing the load files on the tape to the load files currently on the IW SPM (determined in step 6).

**15** Determine if the tape contains patch control files.

| If the tape cartridge label text indicates | Do |
|---|---|
| "Patches: Yes" | step 16 |
| "Patches: No" | step 18 |

**16** Without changing the load file names, copy the patch control file to the PMLOADS volume determined in step 11 by typing

**`>RE FILE  act_vol  drive_no pc_file`**

*Example*

```
>RE FILE F02LPMLOADS F02UTAPE XPM35RTP$XREF
```

**17** Print the patch content of the patch control file by typing

```
>PRINT pc_file
```

*Example*

```
>PRINT XPM35RTP$XREF
```

**18** Copy each load/patch file individually from the tape to a disk volume by typing

*For loads:*

```
>SCANF tape_vol  COPY act_vol load_name
```

*Example*

```
>SCANF  SPM00035 COPY F02LPMLOADS
CEM15CV_010073F
```

*For patches:*

```
>SCANF tape_vol  COPY act_vol NAME *PATCH
```

*Example*

```
>SCANF  SPM00035 COPY F17LPMLOADS NAME
TLC75S0Q$PATCH
```

***Note 1:*** The disk (destination device) and the tape cartridge (origination device) must be in the same tape unit.

***Note 2:*** The patch volume was determined in step 8. A patch volume that begins with the letter “D” is located on an IOM disk and must be copied to the Store File Device (SFDEV). From SFDEV, copy the patches to the IOM disk.

**19** List the load and patch file disk volume, and verify that all required files have been correctly copied to the disk volume, by typing

```
>LF load_vol
```

```
>LF patch_vol
```

*Example*

```
>LF F02PMLOADS
```

```
>LF F17LPTCH
```

***Note:*** If a load or patch volume begins with the letter “D”, it must be listed through disk utility.

*Example*

```
>DSKUT
```

```
>LIV D030PM17PTCH ALL
```

**20** If a load and patch update worksheet has been completed, compare the results of step 19 to the worksheet.

| If | Do |
|---|---|
| you discover required load files that were not copied on the disk volume | step 18 |
| all required load files have been copied onto the disk volume | step 21 |

**21** Steps 21 through 26 copy the upgrade load and PRSU patch files identified in step 19 to their respective back up volumes.

Eject the load tape by typing

```
>ET drive_no
```

*Example*

```
>ET F02UTAPE
```

**22** List the active load file contents on the disk volume by typing

```
>LF disk_vol
```

*Example*

```
>LF F0LPMLOADS
```

**23** Copy each load file from the active disk volume to a backup disk volume by typing

```
>COPY  act_load  disk_vol
```

*Example*

```
>COPY CEM18CB F02LPMLOADS
```

**24** List the loads on the backup volume to ensure that all loads have been copied by typing

```
>LF disk_vol
```

*Example*

```
>LF F0LPMLOADS
```

**25** Review the listing and verify that all of the load files have been copied to the backup volume.

| If all load files | Do |
|---|---|
| are not in the backup volume | step 23 |
| are in the backup volume | step 27 |

**26** Continue based on the patch status.

| If PRSUs | Do |
|---|---|
| were in the PMLOADS volume | repeat step 22 through step 25 for the patch volume |
| are in a separate volume | step 27 |

**27** Remove the SPM load tape from the tape drive and quit the disk utility by typing

```
>QUIT
```

Store the load tape in an available on-site location for future use.

**28** Access the PMLOADS table by typing

```
>TABLE PMLOADS
```

**29** Steps vary based on the upgrade release type.

| If the release type is | Do |
|---|---|
| a milestone (new release) | step 30 |
| a maintenance or emergency (same release) | step 31 |

**30** For each required load, add a new load name by typing

```
>ADD load_name  act_file  act_vol  bkp_file
bkp_vol  N
```

*Example*

```
>ADD CEM19AF CEM19AF_010005 S00DPMLOADS
CEM19AF_010005 S00DPMLOADS N
```

**31** For each new load file, update the file name to reflect the new load values

**Example**

The following example changes the load file name and backup load file name from CEM19DI_010086A1 to CEM19DI_010086A2.

```
>POS CEM17DI

      CEM19DI

CEM19DI_010086A1        S00DPMLOADS
CEM19DI_010086A1        S00DPMLOADS

>CHA

ACTFILE: CEM19DI_010086A1
```

```
>CEM19DI_010086A2
ACTVOL: S00DPMLOADS
>
BKPFILE: CEM19DI_010086A1
>CEM19DI_010086A2
BKPVOL: S00DPMLOADS
>
UPDACT: N
>
TUPLE TO BE CHANGED:
      CEM19DI
CEM19DI_010086A2       S00DPMLOADS
CEM19DI_010086A2       S00DPMLOADS          N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE CHANGED
```

**32** The MNCKTPAK table requires updating only when the load changes for a milestone release. If only changing the load file in the PMLOADS table, no changes are required for the MNCKTPAK table.

***Note:*** Prior to making changes to the MNCKTPAK table, post the SPM to be upgraded and check for and clear any alarms.

| If this is | Do |
|---|---|
| a milestone release | step 33 |
| not a milestone release | step 38 |

**33** Access the MNCKTPAK table by typing

```
>TABLE MNCKTPAK
```

**34** List the contents of the table by typing

```
>LIST ALL
```

**35** Update the circuit pack load inventory for each IW SPM scheduled for an upgrade during the maintenance window by typing

```
>POS SPM spm_no shelf_ID slot_no
```

*Example*

**>POS SPM 23 0 9**

*Response*

```
SPM 23 0 9 GEM 0 1 WORKING(SYSB CR RPT)(MANB MJ
RPT) (ISTB MN RPT)(PROTFAIL CR RPT)(PATCHFAIL MJ
RPT) $ NTLZ20BA     01    GEM19BE
```

**36** Update the appropriate circuit pack load names to match the new loads in the upgrade by typing

**>CHA LOAD load_name**

*Example*

**>CHA LOAD GEM19A0**

**37** Confirm the system prompt by typing

**>Y**

**38** Stop the terminal response from printing by typing

**>RECORD STOP ONTO printer**

**39** You have successfully completed this procedure. Go to the procedure Perform an IW SPM IP manual upgrade or downgrade.

# Preparing to upgrade the CS 2000 Management Tools software

**ATTENTION**
Prior to the upgrade, verify your system has a minimum of 1.074 gigabytes of available disk space on the “/opt” file system, and a minimum of 1.077 gigabytes of available disk space on the “/var” file system. Refer to procedure “Verifying disk utilization on an SSPFS-based server” in the ATM/IP Security and Administration document, NN10402-600, if required.

The supported upgrade paths to the (I)SN07 release are listed below. Follow the link associated with the release you are upgrading from.

- Preparing to upgrade from (I)SN05 to (I)SN07 on page 240
- Preparing to upgrade from (I)SN06 to (I)SN07 on page 242
- Preparing to upgrade from (I)SN06.2 to (I)SN07 on page 244

## Preparing to upgrade from (I)SN05 to (I)SN07

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

**ATTENTION**
If you are upgrading from (I)SN05 and you have the Audio Provisioning Server (APS) on a separate server from the CS 2000 Management Tools, you need to combine the servers prior to upgrading the office to the (I)SN07 release. This procedure assumes that APS is on the same server as the CS 2000 Management Tools for an (I)SN05 to an (I)SN07 upgrade.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

## (I)SN05 to (I)SN07 Preparation checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Install an HTTPS certificate.<br><br>***Note:*** Only perform this activity if HTTPS was not previously installed. An existing HTTPS certificate is maintained over the upgrade.<br><br>Installing an HTTPS certificate requires that Domain Name Service (DNS) be turned on (refer to procedure "Configuring Domain Name Service" in the ATM/IP Solution-level Configuration Management document, NN10409-500, if required). | | Perform procedure Installing an HTTPS certificate on an SSPFS-based server on page 249. |
| 2 | Back up the Oracle data on the server. | | Perform procedure Performing a full backup of Oracle data on a Sun server - pre-(I)SN06.2 on page 262. |
| 3 | Back up the file systems on the server. | | Perform procedure Performing a full backup of file systems - pre-(I)SN06.2 on page 269. |
| 4 | Back up the Network Patch Manager (NPM) data. | | Perform procedure Saving user-defined NPM data using the NPM on page 274. |
| | | | Perform procedure Saving the NPM patch files on page 283. |
| 5 | Back up the Audio Provisioning Server (APS) audio files. | | Perform procedure Performing a backup of APS audio files to tape - Sun t1400 on page 289. |
| 6 | Back up the Audio Provisioning Server (APS) oracle data. | | Perform procedure Performing a backup of APS oracle data to tape on page 293. |
| 7 | Prepare for the CS 2000 SAM21 Manager data migration.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Preparing for the CS 2000 SAM21 Manager data migration on page 297. |

# Preparing to upgrade from (I)SN06 to (I)SN07

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN06 to (I)SN07 Preparation checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Install an HTTPS certificate.<br><br>***Note:*** Only perform this activity if HTTPS was not previously installed. An existing HTTPS certificate is maintained over the upgrade.<br><br>Installing an HTTPS certificate requires that Domain Name Service (DNS) be turned on (refer to procedure "Configuring Domain Name Service" in the ATM/IP Solution-level Configuration Management document, NN10409-500, if required). | | Perform procedure Installing an HTTPS certificate on an SSPFS-based server on page 249. |
| 2 | Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade. | | Perform procedure Verifying group IDs and user IDs on an SSPFS-based server on page 259. |
| 3 | Back up the Oracle data on the server. | | Perform procedure Performing a full backup of Oracle data on a Sun server - pre-(I)SN06.2 on page 262. |
| 4 | Back up the file systems on the server. | | Perform procedure Performing a full backup of file systems - pre-(I)SN06.2 on page 269. |
| 5 | Back up the Network Patch Manager (NPM) data. | | Perform procedure Saving user-defined NPM data using the NPM on page 274. |
| | | | Perform procedure Saving the NPM patch files on page 283. |

## (I)SN06 to (I)SN07 Preparation checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 6 | Back up the Audio Provisioning Server (APS) audio files. | | Perform procedure Performing a backup of APS audio files to tape - Sun t1400 on page 289. |
| 7 | Back up the Audio Provisioning Server (APS) oracle data. | | Perform procedure Performing a backup of APS oracle data to tape on page 293. |

# Preparing to upgrade from (I)SN06.2 to (I)SN07

The configurations that support an upgrade from (I)SN06.2 to(I) SN07 are listed below. Follow the link associated with your configuration.

- Sun Netra t1400 to Sun Netra t1400 on page 244
- Sun Netra 240 to Sun Netra 240 one-server configuration on page 246
- Sun Netra 240 to Sun Netra 240 two-server configuration on page 247

## Sun Netra t1400 to Sun Netra t1400

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

### (I)SN06.2 to (I)SN07 (Sun Netra t1400 to Sun Netra t1400) Preparation checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Install an HTTPS certificate.<br><br>***Note:*** Only perform this activity if HTTPS was not previously installed. An existing HTTPS certificate is maintained over the upgrade.<br><br>Installing an HTTPS certificate requires that Domain Name Service (DNS) be turned on (refer to procedure "Configuring Domain Name Service" in the ATM/IP Solution-level Configuration Management document, NN10409-500, if required). | | Perform procedure Installing an HTTPS certificate on an SSPFS-based server on page 249. |
| 2 | Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade. | | Perform procedure Verifying group IDs and user IDs on an SSPFS-based server on page 259. |
| 3 | Back up the Oracle data on the server. | | Perform procedure Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater on page 265. |

## (I)SN06.2 to (I)SN07 (Sun Netra t1400 to Sun Netra t1400) Preparation checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 4 | Back up the file systems on the server. | | Perform procedure Performing a full backup of file systems - (I)SN06.2 or greater on page 271. |
| 5 | Back up the Network Patch Manager (NPM) data. | | Perform procedure Saving user-defined NPM data using the NPM on page 274. |
| | | | Perform procedure Saving the NPM patch files on page 283. |
| 6 | Back up the Audio Provisioning Server (APS) audio files. | | Perform procedure Performing a backup of APS audio files to tape - Sun t1400 on page 289. |
| 7 | Back up the Audio Provisioning Server (APS) oracle data. | | Perform procedure Performing a backup of APS oracle data to tape on page 293. |

### Sun Netra 240 to Sun Netra 240 one-server configuration

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist , and place a check (√) in the √column as you complete each procedure.

### (I)SN06.2 to (I)SN07 (Sun Netra 240 to Sun Netra 240 one-server) Preparation checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Install an HTTPS certificate.<br><br>***Note:*** Only perform this activity if HTTPS was not previously installed. An existing HTTPS certificate is maintained over the upgrade.<br><br>Installing an HTTPS certificate requires that Domain Name Service (DNS) be turned on (refer to procedure "Configuring Domain Name Service" in the ATM/IP Solution-level Configuration Management document, NN10409-500, if required). | | Perform procedure Installing an HTTPS certificate on an SSPFS-based server on page 249. |
| 2 | Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade. | | Perform procedure Verifying group IDs and user IDs on an SSPFS-based server on page 259. |
| 3 | Back up the Oracle data on the server. | | Perform procedure Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater on page 265. |
| 4 | Back up the file systems on the server. | | Perform procedure Performing a full backup of file systems - (I)SN06.2 or greater on page 271. |
| 5 | Back up the Network Patch Manager (NPM) data. | | Perform procedure Saving user-defined NPM data using the NPM on page 274. |
| | | | Perform procedure Saving the NPM patch files on page 283. |

### (I)SN06.2 to (I)SN07 (Sun Netra 240 to Sun Netra 240 one-server) Preparation checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 6 | Back up the Audio Provisioning Server (APS) audio files. | | Perform procedure Performing a backup of APS audio files to CD/DVD - Sun Netra 240 on page 291. |
| 7 | Back up the Audio Provisioning Server (APS) oracle data. | | Perform procedure Performing a backup of APS oracle data to CD or DVD on page 295. |

### Sun Netra 240 to Sun Netra 240 two-server configuration

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

**ATTENTION**

Although a backup is not normally required in a cluster configuration, it is highly recommended that one be performed in the event you need or want to revert to a previous release after both servers have been upgraded. Refer to procedures Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater on page 265, Performing a full backup of file systems - (I)SN06.2 or greater on page 271, and if APS is present, Performing a backup of APS audio files to CD/DVD - Sun Netra 240 on page 291, and Performing a backup of APS oracle data to CD or DVD on page 295.

Use this table as a checklist , and place a check (√) in the √column as you complete each procedure.

**(I)SN06.2 to (I)SN07 (Sun Netra 240 to Sun Netra 240 two-server) Preparation checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| **On the ACTIVE node** | | | |
| 1 | Install an HTTPS certificate.<br><br>***Note:*** Only perform this activity if HTTPS was not previously installed. An existing HTTPS certificate is maintained over the upgrade.<br><br>Installing an HTTPS certificate requires that Domain Name Service (DNS) be turned on (refer to procedure "Configuring Domain Name Service" in the ATM/IP Solution-level Configuration Management document, NN10409-500, if required). | | Perform procedure Installing an HTTPS certificate on an SSPFS-based server on page 249. |
| 2 | Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade. | | Perform procedure Verifying group IDs and user IDs on an SSPFS-based server on page 259. |
| **On the INACTIVE node** | | | |
| 3 | Verify the state of the cluster. | | Perform procedure Verifying the state of a cluster on page 300. |
| **On the ACTIVE node** | | | |
| 4 | Obtain any patches applicable to components on the CS 2000 Management Tools server (PSE, CS 2000 SAM21 Manager, NPM, SESM, QCA, SSPFS) | | Perform procedure Transferring patches to the NPM database manually on page 1664. |

# 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 below).

**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 250
- High-availability configuration (two servers) on page 254

## Prerequisites

This procedure has the following prerequisites:

- The domain name service (DNS) must be enabled on the server to allow the security certificate to work, and must be enabled prior to the installation of the certificate. Refer to procedure “Configuring Domain Name Service” in the ATM/IP Solution-level Configuration Management document, NN10409-500.
- If purchasing a certificate from a third-party certificate authority (CA), such as VeriSign, obtain a PEM-encoded X.509 certificate, but without a passcode.

  ***Note:*** The name of the certificate should match the host name of the server. Nortel Networks recommends the installation of a unique certificate for each host. A separate file contains the key, and should not have an associated password.

- Make sure all GUI screens are closed before you install the certificate.
- The RSA key for the HTTPS certificate must not have a password.
- The certificate must be created with the fully qualified domain name (FQDN) of the server on which the certificate will be installed.
- Sub-directories “ssl.crt” and “ssl.key” must already exist in the “/opt/apache/conf” directory.

## Action

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:*

```
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.

**16** 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:*

```
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 734.

**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.

# Verifying group IDs and user IDs on an SSPFS-based server

## Application

Use this procedure to verify the group identifiers (GID) and user identifiers (UID) defined on a Succession Server Platform Foundation Software (SSPFS)-based server, to ensure that none of the user-defined GIDs or UIDs conflict with GIDs and UIDs that the SSPFS requires during an upgrade.

**ATTENTION**
It is necessary to perform this procedure prior to upgrading the SSPFS, as the SSPFS upgrade expects certain GIDs and UIDs to be free. If those GIDs and UIDs are not free, the SSPFS upgrade will fail.

## Prerequisites

None

## Action

Perform the following steps to complete this procedure.

**ATTENTION**
In a two-server configuration, perform this procedure on the Active server.

***At your workstation***

**1** Log in to the server by typing

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

and pressing the Enter key.

where

**IP address**
is the IP address or host name of the SSPFS-based server

**2** When prompted, enter your user ID and password.

3 Display the GIDs that exist on the system by typing

```
# cut -f1,3 -d':' /etc/group
```

and pressing the Enter key.

4 Compare the groups you obtained in the system response with the following groups:

root, other, bin, sys, adm, uucp, mail, tty, lp, nuucp, staff, daemon, sysadmin, oinstall, dba, data, maint, succssn, sshd, maint2, trkadm, trkrw, trksprov, trkmtc, trkro, lnadm, lnrw, lnsprov, lnmtc, lnro, mgcadm, mgcrw, mgcsprov, mgcmtc, mgcro, mgadm, mgrw, mgsprov, mgmtc, mgro, emsadm, emsrw, emssprov, emsmtc, emsro, nobody, noaccess, nogroup, and passthru

***Note:*** The passthru group is only applicable to SN07.

5 Note any groups displayed in the system response that are not in the above list. These are user-defined groups.

6 Note any user-defined groups that have a GID number in the 10, 100, or 1000 range.

User-defined groups that have a GID number in the 10, 100, or 1000 range need to be moved to a different GID value before starting the SSPFS upgrade.

7 Report any user-defined groups that have a GID number in the 10, 100, or 1000 range to your next level of support, who will assist in moving each group to a different GID, and updating the impacted file systems to reflect the new GID.

8 Display the users that exist on the system by typing

```
# cut -f1,3 -d':' /etc/passwd
```

and pressing the Enter key.

9 Compare the users you obtained in the system response with the following users:

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, nortel, oracle, and Administrator

10 Note any users displayed in the system response that are not in the above list. These are user-defined users.

**11** Note any user-defined users that have a UID number below 50000.

User-defined users that have a UID number below 50000 need to be moved to a different UID value before starting the SSPFS upgrade.

**12** Report any user-defined users that have a UID number below 50000 to your next level of support, who will assist in moving each user to a different UID, and updating the impacted file systems to reflect the new UID.

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 265 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 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 262 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 1909 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 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 271 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.

# 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 269 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 265 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 1909 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.

# Saving user-defined NPM data using the NPM

## Application

Before performing an upgrade of the Network Patch Manager (NPM) to a new release, it is recommended that you preserve any user-defined data in the current release. Examples would be user-defined sets, reports, alarms, tasks, etc. This does not include system defined data, which will be re-created during the NPM upgrade. All user-defined information will be removed during the NPM upgrade. This procedure contains the steps necessary to preserve this data so it will be available to the new NPM release once the upgrade is completed. You can save user-defined NPM data using one of the following two NPM interfaces:

- Using the NPM CLUI on page 274
- Using the NPM GUI on page 278

## Prerequisites

The SSPFS software has not been upgraded yet.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

**1** Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

**2** Display all the set names present on the NPM by typing

```
npm> qsets
```

and pressing the Enter key.

***Note:*** Ignore the following system-defined sets: ALLPATCHES, AUTOAPPLY, NOSPAPP, ALLDEVICES, OAMDEVICES, AUTORESTARTDEVICES, MG9KDEVICES, and GWCDEVICES.

3 Display the definition details for any user-defined sets that should be propagated to the new release by typing

npm> **viewset SET <set_name>**

and pressing the Enter key.

where

**set_name**
is the name of the user-defined set.

4 Record the details of the set.

5 Repeat steps 3 and 4 for each user-defined set.

6 Display the list of all reports by typing

npm> **qreps**

and pressing the Enter key.

***Note:*** Ignore the following system defined reports: ACTLIST, CALCLIST, DEVICE, DEVICELIST, DISABLEDAPPLIED, DISABLEDREMOVED, ENABLEDAPPLIED, ENABLEDREMOVED, FULLDEVICELIST, LOADLIST, PATCH, PATCHES_SINCE, PATCHINFO, PATCHLIST, DEVICE_ACTIVITY, DEVICE_ACTLEVEL, DEVICE_APPLEVEL, and INVALID_LOADNAME.

7 View the details of the user-defined reports by typing

npm> **viewset REPORT <report_name>**

and pressing the Enter key.

where

**report_name**
is the name of a user-defined report

8 Record the details of the report.

9 Repeat steps 7 and 8 for each user-defined report.

10 Display all defined alarms by typing

```
npm> alarminfo all
```

and pressing the Enter key.

***Note:*** Ignore the following system-defined alarms: ACT_NOT_APP, ACT_NOT_ACT, DEBUG_APP, DNR_NOT_APP, EMG_NOT_APP, GEN_NOT_APP, LTD_NOT_APP, OBS_NOT_REMOVED, OBE_NOT_REMOVED, REMOVED_PATCHES, PATCH_ONHOLD, DEVCIE_ONLHOLD, DEVICE_AUDITFAIL, DISABLED_APPLIED, and ENABLED_REMOVED.

11 Display the details of the user-defined alarms by typing

```
npm> alarminfo <alarm_name>
```

and pressing the Enter key.

where

**alarm_name**
is the name of the user-defined alarm

12 Record the details of the alarm.

13 Repeat steps 11 and 12 for each user-defined alarm.

14 List all the task names by typing

```
npm> qtask all
```

and pressing the Enter key.

***Note:*** Ignore the following system-defined tasks: AUTOAPPLY, AUTORESTART, and AUDIT.

15 Display the details of the user-defined tasks by typing

```
npm> qtask <task_name>
```

and pressing the Enter key.

where

**task_name**
is the name of a user-defined task

16 Record the details of the task.

17 Repeat steps 15 and 16 for each user-defined task.

18 Display the System Plan by typing

```
npm> getplan
```

and pressing the Enter key.

**19** If the System Plan has been modified from its original version, record the changes at this time.

***Note:*** The original version should only show the AUTOAPPLY and AUTORESTART tasks.

**20** Display the patchlist report by typing

```
npm> query PATCHLIST
```

and pressing the Enter key.

**21** Save a copy of the PATCHLIST report for later reference.

**22** You have completed this procedure.

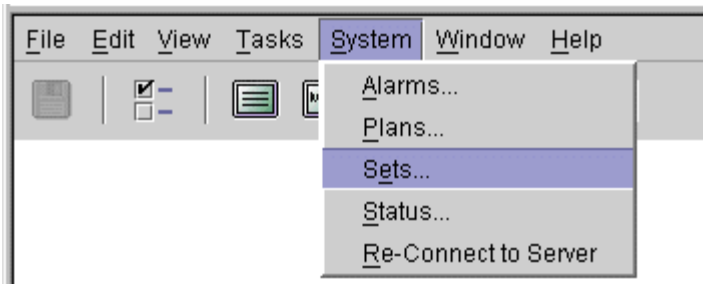
## Using the NPM GUI

### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

### *At the NPM GUI*

2 On the **System** menu, click **Sets...**.




The **Sets** window is displayed.

3 Click the **Set List** tab to display the list of defined sets.

4 Click one of the user-defined sets, then click **Edit** to display its details.

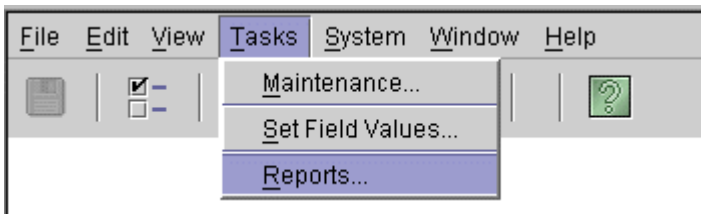
***Note:*** Ignore the following system-defined sets: ALLPATCHES, AUTOAPPLY, NOSPAPP, ALLDEVICES, OAMDEVICES, AUTORESTARTDEVICES, MG9KDEVICES, and GWCDEVICES.

5 Record the details of the set.

6 Repeat steps 3 through 5 for each user-defined set.

7 Click **Close** to close the Sets window.

8 On the **Tasks** menu, click **Reports...**.




9 Click the **Report List** tab to display the list of defined reports.

10 Click one of the user-defined reports, then click **Edit** to display the details.

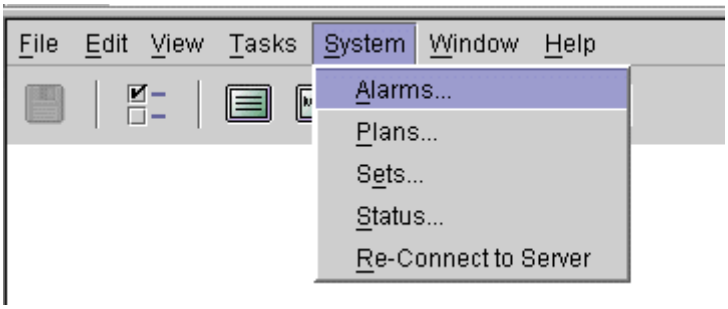
***Note:*** Ignore the following system defined reports: ACTLIST, CALCLIST, DEVICE, DEVICELIST, DISABLEDAPPLIED, DISABLEDREMOVED, ENABLEDAPPLIED, ENABLEDREMOVED, FULLDEVICELIST, LOADLIST, PATCH, PATCHES_SINCE, PATCHINFO, PATCHLIST, DEVICE_ACTIVITY, DEVICE_ACTLEVEL, DEVICE_APPLEVEL, and INVALID_LOADNAME.

11 Record the details of the report.

12 Repeat steps 9 through 11 for each user-defined report.

13 Click **Close** to close the Reports window.

14 On the **System** menu, click **Alarms...**.




15 Click the **Alarm List** tab to display the list of defined alarms.

16 Click one of the user-defined alarms, then click **Edit** to display its details.

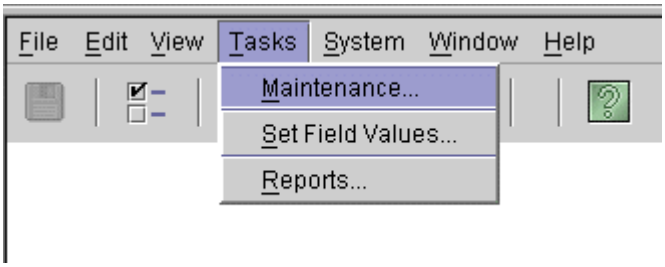
***Note:*** Ignore the following system-defined alarms: ACT_NOT_APP, ACT_NOT_ACT, DEBUG_APP, DNR_NOT_APP, EMG_NOT_APP, GEN_NOT_APP, LTD_NOT_APP, OBS_NOT_REMOVED, OBE_NOT_REMOVED, REMOVED_PATCHES, PATCH_ONHOLD, DEVCIE_ONLHOLD, DEVICE_AUDITFAIL, DISABLED_APPLIED, and ENABLED_REMOVED.

17 Record the details of the alarm.

18 Repeat steps 15 through 17 for each user-defined alarm.

19 Click **Close** to close the Alarms window.

20 On the **Tasks** menu, click **Maintenance...**.




21 Click the **Task List** tab to display the list of defined tasks.

22 Click one of the user-defined tasks, then click **Edit** to display its details.

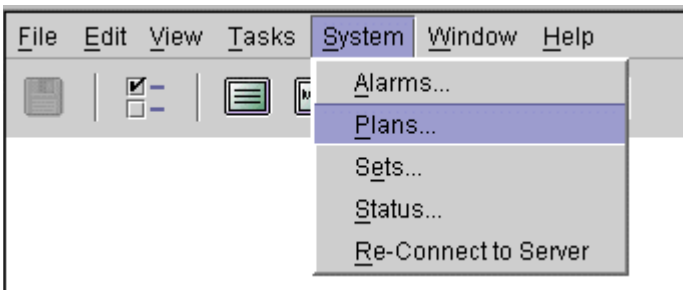
***Note:*** Ignore the following system-defined tasks: AUTOAPPLY, AUTORESTART, and AUDIT.

23 Record the details of the task.

24 Repeat steps 21 through 23 for each user-defined task.

25 Click **Close** to close the Tasks window.

26 On the **System** menu, click **Plans...**.




27 Click the **Plan List** tab.

28 Click the **SYSTEMPLAN**, then click **Edit** to display its details.

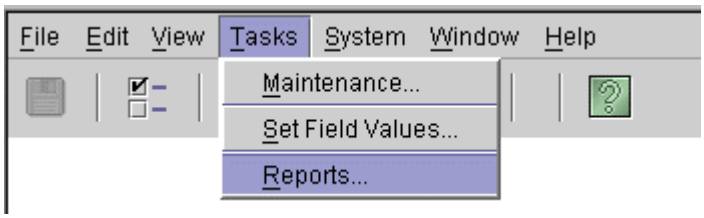
29 If either (or both) are present, open the Tasks and/or Reports folders.

30 If the System Plan has been modified from its original version, record the changes at this time.

***Note:*** The original version should only show the AUTOAPPLY and AUTORESTART tasks.

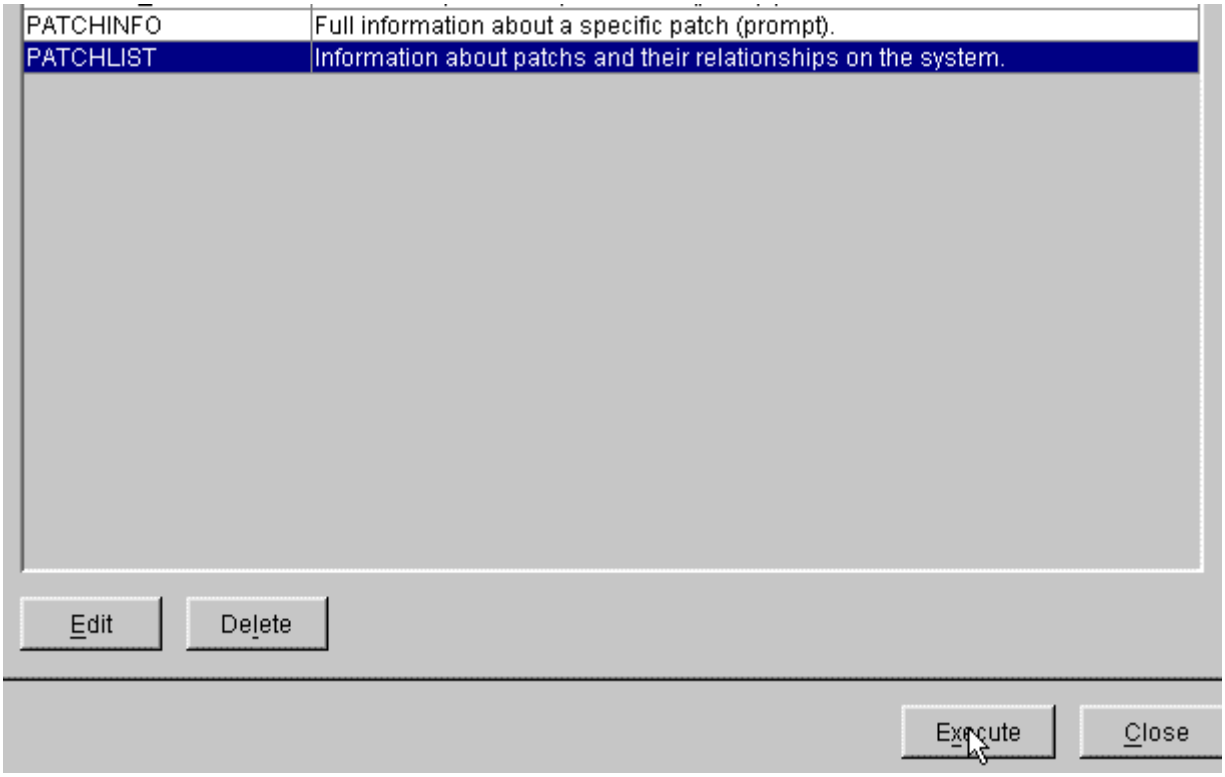
31 Click **Close** to close the Plans window.

32 On the **Tasks** menu, click **Reports...**.

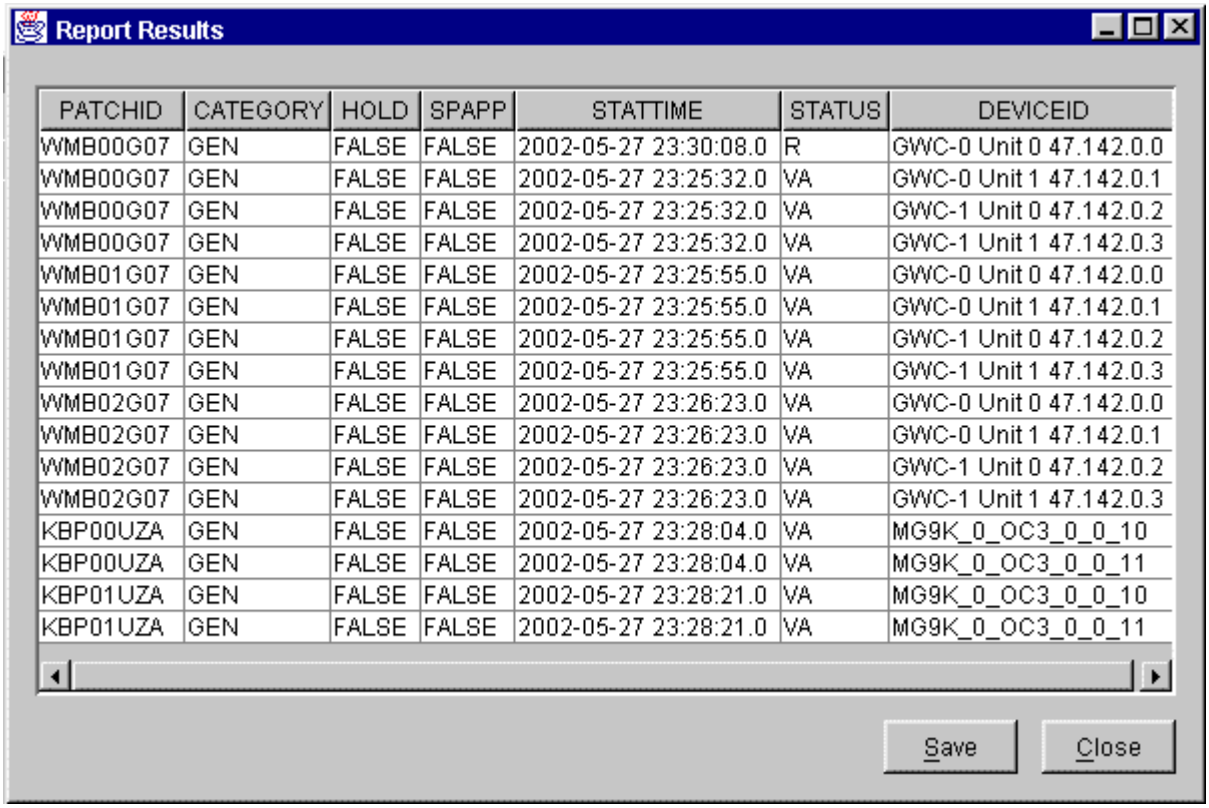



33 Click the **Reports List** tab to display the list of all reports.

34 Select **PATCHLIST**, then click **Execute** to run the PATCHLIST report.




The **Reports Results** window is displayed.




**35** Click **Save** to save the results of the PATCHLIST report.

**36** In the **Filename** box enter a name for the saved report, then click **Save**.




**37** You have completed this procedure.

# Saving the NPM patch files

## Application

Use this procedure prior to upgrading the Network Patch Manager (NPM) software. This procedure provides instructions on how to copy patch files information to one of the following locations:

- Saving NPM patch files to disk on page 284
- Saving NPM patch files to tape (Sun Netra t1400 only) on page 287
- Saving NPM patch files to CD (Sun Netra 240 only) on page 288

***Note:*** NPM patch files saved to a location on disk are preserved over an upgrade. However, if for some reason you need to restore those patch files, contact your next level of support. If you save the NPM patch files on tape (Sun Netra t1400) or CD/DVD (Sun Netra 240), you can restore them using procedure Restoring NPM patch files on page 1586 in this document.

## Prerequisites

This procedure has the following prerequisites if you are saving the NPM patch files to tape or CD/DVD:

- you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data (Sun Netra t1400 only)
- you need one or more blank CD-R, CD-RW, DVD-R or DVD-RW of 4.7 GB to store the data (Sun Netra 240 only) - backup on CD-R completes sooner than on other media types, and DVD-R does not require formatting

***Note:*** To re-use a CD or DVD, refer to procedure Erasing the contents of a CD/DVD on a Sun server on page 1909 in this document.

## Action

Perform the steps using one of the following methods to complete this procedure:

- Saving NPM patch files to disk
- Saving NPM patch files to tape (Sun Netra t1400 only)
- Saving NPM patch files to CD (Sun Netra 240 only)

## Saving NPM patch files to disk

### *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 hostname 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 Verify whether any NPM patch files exist as follows:

**a** Change directory to the NPM's patch file directory by typing

```
# cd /data/npm/Au
```

and pressing the Enter key.

**b** List the content of the directory by typing

```
# ls
```

and pressing the Enter key.

| If patch files | Do |
|---|---|
| exist | step 6 |
| do not exist | you have completed this procedure |

6 Access the data directory by typing

```
# cd /data
```

and pressing the Enter key.

**7** Make a directory to store the old NPM files by typing

```
# mkdir <npm_old>
```

where

**npm_old**
is a valid Unix directory name

**8** Change directory to the directory you just created by typing

```
# cd <npm_old>
```

where

**npm_old**
is a valid Unix directory name

**9** Create a temporary directory to hold the NPM backup data by typing

```
# mkdir <directory_name>
```

and pressing the Enter key.

where

**directory_name**
is a valid UNIX directory name

Example

```
# mkdir patch_data
```

**10**

**ATTENTION**
This step copies all or selected NPM patch files to a temporary location. If it is preferable to download the required patch files after the upgrade, this step may be skipped.

Save a copy of the needed patch files by performing the following steps.

***Note:*** The NPM upgrade process normally does not remove the patch files present in the patch file repository. However, the NPM server may not be able to locate and utilize all the files. The NPM server and database will remain unaware of any patches present that are not yet applied to any working device.

**a** Change directory to the NPM's patch file directory by typing

```
# cd /data/npm/Au
```

and pressing the Enter key.

**b** Copy all patch files to the backup directory by typing

```
# cp *.ptch* <directory_path>
```

and pressing the Enter key.

where

**directory_path**
is the path to the directory you created in step 9

Example

```
# cp *.ptch* /data/npm_old/patch_data
```

**c** Ensure all patch files were copied to the backup directory by typing

```
# ls -l <directory_path>
```

and pressing the Enter key.

where

**directory_path**
is the path to the directory where you copied the patch files

Example

```
# cd /data/npm_old/patch_data
```

**11** Return to the home directory of the UNIX host by typing

```
# cd
```

and pressing the Enter key.

**12** You have completed this procedure.

## Saving NPM patch files to tape (Sun Netra t1400 only)

***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 hostname 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 Insert a blank tape into the drive.

***Note:*** Ensure the write-protect tab is set to allow writing.

6 Rewind the tape by typing

```
# mt rewind
```

and pressing the Enter key.

7 Copy the patch files to tape by typing

```
# tar cv /data/npm/Au
```

and pressing the Enter key.

8 Rewind and eject the tape by typing

```
# mt offline
```

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.

## Saving NPM patch files to CD (Sun Netra 240 only)

***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 hostname 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 Create a temporary directory by typing

```
# mkdir /tmp/.iso
```

and pressing the Enter key.

***Note:*** The directory may already exist.

6 Insert a blank CD or DVD into the drive.

7 Make an ISO image of the patch files and write this image to the CD or DVD by typing

```
# /opt/nortel/sspfs/bks/cdwrite /data/npm/Au
PATCHES
```

and pressing the Enter key.

***Note:*** The CD or DVD is automatically ejected.

8 Remove the CD or DVD from the drive, label it and store it in a safe place.

9 You have completed this procedure.

# Performing a backup of APS audio files to tape - Sun t1400

## Application

Use this procedure to back up APS audio files to a 4mm Digital Audio Tape (DAT).

**ATTENTION**
This procedure only applies to a Sun t1400 server with a DAT drive. Use procedure Performing a backup of APS audio files to CD/DVD - Sun Netra 240 on page 291 for a Sun Netra 240 server with a CD/DVD drive.

## Prerequisites

None

## Action

Perform the following steps to complete this procedure.

***At the APS server***

1 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides.

***At the APS server console***

2 Log in to the server through the console (port A) using the root user ID and password.

3 Rewind the tape by typing

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

and pressing the Enter key.

4 Change directories to the root filesystem by typing

```
# cd /
```

and pressing the Enter key.

5 Back up the APS application files by typing

```
# /usr/ntdb/uas/scripts/backup_appl_data.sh
```

and pressing the Enter key.

***Note:*** This command backs up file systems /PROV_data, /audio_files, and /user_audio_files.

6 Rewind the backup tape by typing

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

and pressing the Enter key.

7 To ensure that the backup was successful, list the content of the tape by typing

```
# tar tvf /dev/rmt/0c | more
```

and pressing the Enter key.

8 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen) to prevent the data on the tape from being accidentally over-written. Store the tape for later use.

9 You have completed this procedure.

# Performing a backup of APS audio files to CD/DVD - Sun Netra 240

## Application

Use this procedure to back up APS audio files onto a CD/DVD.

**ATTENTION**
This procedure only applies to a Sun Netra 240 server with a CD/DVD drive. Use procedure Performing a backup of APS audio files to tape - Sun t1400 on page 289 for a Sun t1400 server with a DAT drive.

## Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater
- you need one 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 1909 in this document.

## Action

Perform the following steps to complete this procedure.

***At the APS server***

**1** Insert a blank 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.

6 Change directories to the root file system by typing

```
# cd /
```

and pressing the Enter key.

7 Create a “tar” file of the APS audio files by typing

```
# tar cvf AudioFiles.tar /audio_files
/user_audio_files /opt/uas/uas_conf_backup
```

and pressing the Enter key.

***Note:*** The above command is entered on one line, and includes a space between each directory.

8 Verify the size of the “AudioFiles.tar” file by typing

```
# ls -l AudioFiles.tar
```

and pressing the Enter key.

| If the “AudioFiles.tar” file is | Do |
|---|---|
| under 2 GB | step 10 |
| over 2 GB | step 9 only |

9 Move the “AudioFiles.tar” file onto another server using File Transfer Protocol (FTP).

10 Backup the tar file of the APS audio files onto the DVD-RW by typing

```
# /opt/nortel/sspfs/bks/cdwrite AudioFiles.tar
```

and pressing the Enter key.

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

12 You have completed this procedure.

# Performing a backup of APS oracle data to tape

## Application

Use this procedure to back up APS oracle data to a 4mm Digital Audio Tape (DAT).

**ATTENTION**
This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure Performing a backup of APS oracle data to CD or DVD on page 295.

## Prerequisites

You need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the oracle data.

## Action

Perform the following steps to complete this procedure.

***At the server***

1 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides.

***At the server console***

2 Log in to the server through the console (port A) using the root user ID and password.

3 Rewind the tape by typing

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

and pressing the Enter key.

4 Change directories to the root filesystem by typing

```
# cd /
```

and pressing the Enter key.

5 Back up the APS oracle files by typing

```
# ips_export_db.sh -t /dev/rmt/0 | tee
,/export_log
```

and pressing the Enter key.

6 Rewind the backup tape by typing

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

and pressing the Enter key.

7 To ensure the backup was successful, list the content of the tape by typing

```
# tar tvf /dev/rmt/0c | more
```

and pressing the Enter key.

8 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen) to prevent the data on the tape from being accidentally over-written. Store the tape for later use.

You have completed this procedure.

# Performing a backup of APS oracle data to CD or DVD

## Application

Use this procedure to back up APS oracle onto a CD or DVD.

**ATTENTION**
This procedure only applies to a Sun Netra 240 server with a CD/DVD drive. Use procedure Performing a backup of APS oracle data to tape on page 293 for a Sun t1400 server with a DAT drive.

## Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater
- you need one blank CD-R, DVD-R, CD-RW or DVD-RW to store the data

***Note 1:*** The backup utility limits the storage to 2 GB on a DVD-R, or DVD-RW.

***Note 2:*** If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure “Preparing a CD-RW or DVD-RW for use” in the ATM/IP Security and Administration document, NN10402-600.

## Action

Perform the following steps to complete this procedure.

***At the server***

**1** Insert a blank CD or DVD into the drive.

***At your workstation***

**2** Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**
is the IP address or 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 Back up the APS oracle data to hard disk by typing

```
#  ips_export_db.sh -diskonly
```

and pressing the Enter key.

7 Change directories to where the backup is by typing

```
# cd /audio_files/aps_db_backup
```

and pressing the Enter key.

8 Create a tar file of the APS oracle files by typing

```
# tar cvf aps_oracle_bkup.tar *
```

and pressing the Enter key.

9 Verify the size of the “aps_oracle_bkup.tar ” file by typing

```
# ls -l aps_oracle_bkup.tar
```

and pressing the Enter key.

| If the “aps_oracle_bkup.tar” file is | Do |
|---|---|
| under 2 GB | step 11 |
| over 2 GB | step 10 only |

10 Move the “aps_oracle_bkup.tar” file onto another server using File Transfer Protocol (FTP).

You have completed this procedure.

11 Backup the tar file of the APS oracle data onto the CD or DVD by typing

```
# /opt/nortel/sspfs/bks/cdwrite
aps_oracle_bkup.tar
```

and pressing the Enter key.

12 Remove the CD or DVD from the drive, label it, and store it in a safe place.

You have completed this procedure.

# Preparing for the CS 2000 SAM21 Manager data migration

## Application

Use this procedure to prepare for the migration of the CS 2000 SAM21 Manager from the core manager to the CS 2000 Management Tools server, prior to upgrading the CS 2000 Management Tools software to (I)SN07.

**ATTENTION**

Once you prepare for the CS 2000 SAM21 Manager data migration, ensure no SAM21 nodes are added to the network until the entire upgrade of the CS 2000 Management Tools software is complete, and the CS 2000 SAM21 Manager is operating from the CS 2000 Management Tools server.

## Prerequisites

The core manager must be at the CS2E00006 software release or higher.

## Action

Perform the following steps to complete this procedure.

***At the console connect to the core manager***

**1** Log on to the core manager through the console using the root user ID and password.

**2** Verify that the Open SSH fileset is installed as follows:

**a** Access the Details level of the maintenance interface to display a list of the filesets installed on the core manager by typing

```
# sdmmtc details
```

and pressing the Enter key.

**b** Filter the display so that only the filesets with “ssh” in their name are displayed by typing

```
> filter ssh
```

and pressing the Enter key.

**c** Ensure that the OpenSSH fileset is applied.

| If OpenSSH is | Do |
|---|---|
| applied | step 3 |
| not applied | Refer to procedure "Installing or upgrading OpenSSH" in the CS 2000 Core Manager Upgrades section, NN10060-461. When complete, return to this procedure and continue with step 3. |

**3** Busy the CS 2000 SAM21 Manager as follows:

**a** Access the application level of the maintenance interface by typing

> **appl**

and pressing the Enter key.

**b** Busy the Succession SAM21 Manager application by typing

> **bsy <#>**

and pressing the Enter key.

*where*

**#**
is the number next to the Succession SAM21 Manager fileset

**c** Confirm the busy command by typing

> **y**

and pressing the Enter key.

The CS 2000 SAM21 Manager client application on the core manager shuts down after the busy command.

**d** Exit the maintenance interface by typing

> **quit all**

and pressing the Enter key.

**4** Run the pre-migration script to backup persistent data and create an SSPFS persistent data file by typing

# **/sdm/snm/bin/sam21emPreMigration.sh**

and pressing the Enter key.

**5** Return the CS 2000 SAM21 Manager application to service as follows:

**a** Access the application level of the maintenance interface by typing

```
# sdmmtc appl
```

and pressing the Enter key.

**b** Return the Succession SAM21 Manager to service by typing

```
> rts <#>
```

and pressing the Enter key.

*Where:*

**#**
is the number next to the Succession SAM21 Manager fileset

***Note:*** The state changes to ISTb, then to in-service (represented by a dot) after approximately one minute.

**6** You have completed this procedure.

# Verifying the state of a cluster

## Application

Use this procedure to verify the state of a cluster, which involves verifying the status of replicated disk volumes, the cluster indicator, and the cluster configuration. A cluster refers to a Sun Netra 240 server pair.

**ATTENTION**

The “ClusterOutOfSync” file may be present in the root directory, however, it does not give the definitive state of the cluster. It is best that you perform this procedure to determine the state of the cluster rather than rely on the presence of the “ClusterOutOfSync” file.

When a cluster node is out of sync, log SPFS310 is generated.

***Note:*** For more information on logs, refer to the *Succession Networks Fault Management Logs Reference* document, NN10275-909. For information on how to configure log reporting, route customer logs to a remote host, and view customer logs, refer to the *ATM/IP solution-level Fault Management* document, NN10408-900.

## Prerequisites

You need the root user ID and password.

## Action

Perform the following steps to complete this procedure.

***At your workstation***

1 Telnet to the Inactive server of the cluster by typing

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

and pressing the Enter key.

where

**IP address**
is the physical IP address of the Inactive server 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 the status of replicated disk volumes by typing

```
# udstat
```

and pressing the Enter key.

| If the system response | Do |
|---|---|
| contains “nodaemon”, “offline”, “down”, “not mounted” | step 8 |
| is STANDBY normal UP clean | step 6 |

**6** Verify the cluster indicator by typing

```
# ubmstat
```

and pressing the Enter key.

| If the system response | Do |
|---|---|
| is other than “ClusterIndicatorSTBY” | step 8 |
| is “ClusterIndicatorSTBY” | step 7 |

**7** Verify the status of the cluster configuration by typing

```
# CheckConfiguration
```

and pressing the Enter key.

| If the system response | Do |
|---|---|
| is other than “Checking local cluster configuration against <other node> | step 8 |
| is “Checking local cluster configuration against <other node> | the cluster is in a good state and you have completed this procedure |

**8** Reboot the Inactive server by typing

```
# init 6
```

and pressing the Enter key.

| If the problem | Do |
|---|---|
| persists | step 9 |
| is corrected | the cluster is in a good state and you have completed this procedure |

**9** Capture SSPFS file and logs for debugging purposes 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 “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 -
```

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

*Example response*

```
Executing “capt_files”
```

**10** Provide the debugging data to your next level of support for analysis.

**11** You have completed this procedure.

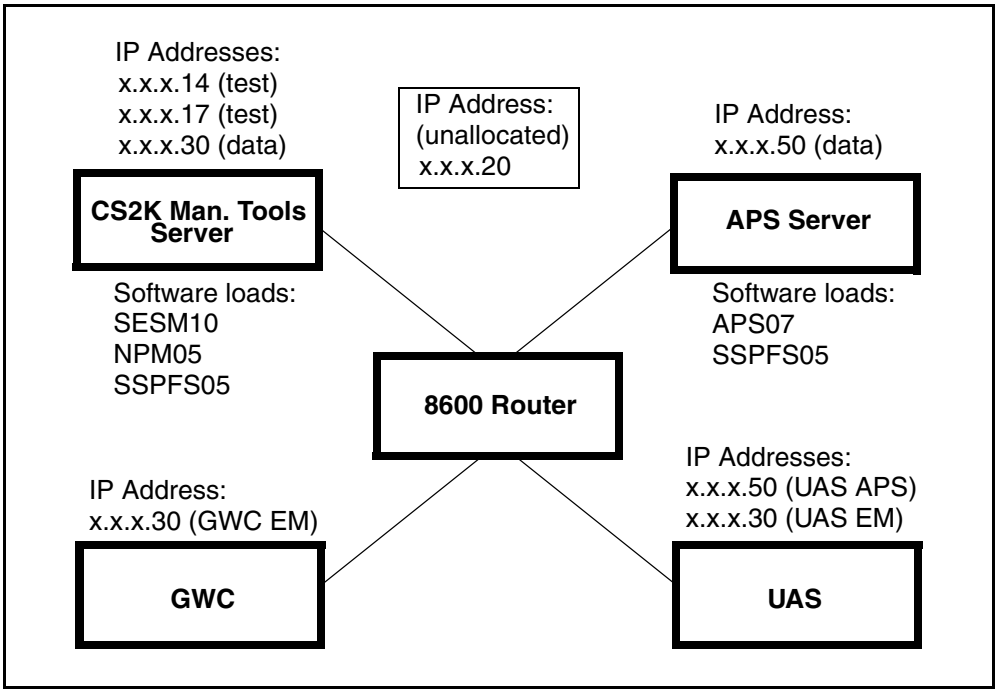
# Combined server upgrade

This document contains the procedure for performing a combined server upgrade, and the procedure for backing out of a combined server upgrade that you have performed, if necessary.

The combined server upgrade procedure enables you to perform a “collapse” of an existing APS system, that resides on a dedicated, “standalone” server, onto a “combined” server that hosts the CS 2000 Management Components (CS2M), called the “CS 2000 Management Tools server.” This is a prerequisite procedure required for standalone APS systems at release level APS07 (SN05) that are being upgraded to release level APS08 (SN06).

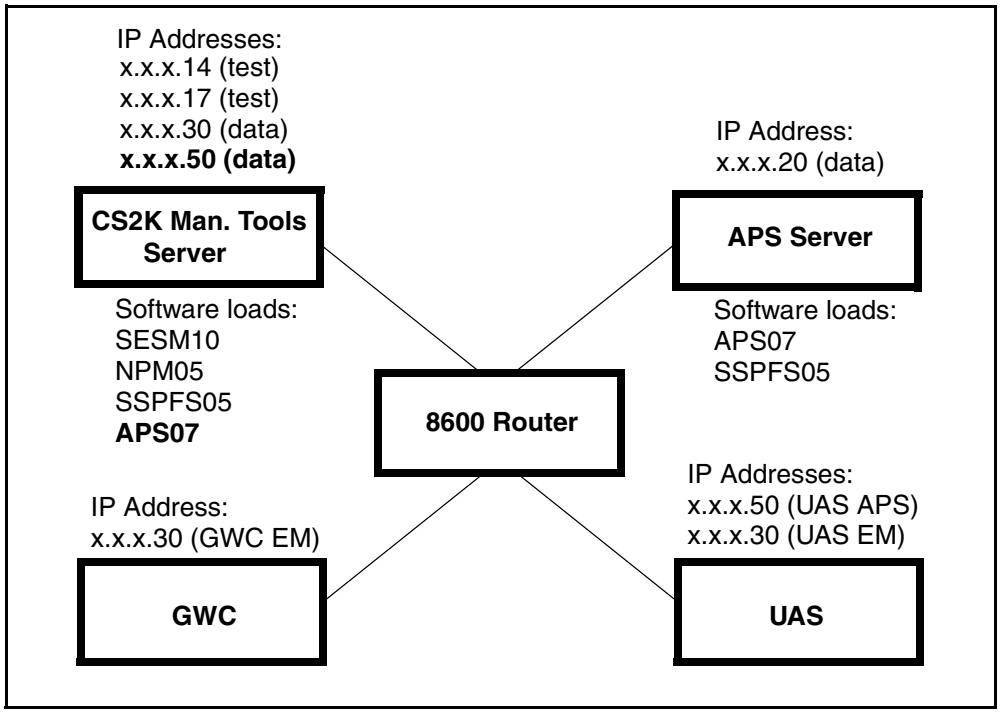
The following illustrations depict the basic impact of the upgrade procedure. In the first illustration, below, the APS is configured on a standalone server, at release level APS07.

**Combined server upgrade impact - before the upgrade**




In the illustration below, which shows the system configuration after the “Combined server upgrade” procedure has been performed, the IP address formerly associated with the standalone APS server has been moved to the CS 2000 Management Tools server.

**Combined server upgrade impact - after the upgrade**




## Upgrade special considerations

The CS 2000 Management Tools server is not available during the upgrade procedure. Thus, visibility into the network through the CS 2000 Management Tools and services to the GWCs are not available during the upgrade.

Safe stopping points in the procedure are so noted.

## Entry criteria before starting the upgrade

The following must be obtained before the procedure can be started:

- the IP addresses and host names of the existing APS and CS 2000 Management Tools servers; this includes the test IP addresses used on the CS 2000 Management Tools server for multipathing
- one additional, unallocated IP address on the same subnet as the CS 2000 Management Tools and APS servers, to be used as a new IP address for the old standalone APS server. This avoids two machines with the same IP address on the network should the old APS server be accidentally switched back on.
- one new host name for the old standalone APS server that does not match any existing hostnames on the subnet
- DDS-3 DAT tapes, for performing backups

# Combined server upgrade procedure

## Combined server upgrade

### *At the Windows desktop interface*

1 Open a telnet connection to the CS 2000 Management Tools server.

2 Log in as the “maint” user.

3 Become the “root” user by entering the following command and then entering the “root” password when prompted:

```
su - root
```

4 Verify that the CS 2000 Management Tools server is equipped with the appropriate baseline hardware by performing the following steps:

**a** type **format** on the command line

*The program displays a list of disk drives. There should be four disk drives, numbered 0 through 3, in the list. If four drives do not display in the list, then the system is not equipped with the appropriate baseline hardware and cannot be upgraded. In that case, abort the procedure, after you exit from the “format” program by entering **quit**.*

**b** In response to the “Specify disk” prompt, enter a disk drive number, starting with drive 0.

**c** In response to the “format” prompt, enter **inquiry**.

*In the resulting display, the last three characters in the “Product:” field indicate the size of the disk. If you see “36G”, which indicates a disk size of 36Gbyte, the disk is at the required baseline size. If a smaller disk size is indicated, this procedure must be aborted, after you exit from the “format” program by entering **quit**.*

**d** Exit from the “format” program by entering **quit**.

**e** Repeat steps a through d for each disk in the system, and then proceed to step 5.

5 Verify the system processors and memory size by performing the following steps:

**a** Type **prtconf | less** on the command line.

*In the resulting display, look for the following line of information: “Memory size: 2048 Megabytes”. The value, 2048 Megabytes, indicates that the memory size is 2Gbyte, which is the baseline size required for performing this*

*upgrade. If a smaller memory size is indicated, this procedure must be aborted, after you exit from the "prtconf | less" command by entering* ***q****.*

**b** Scroll to the end of the display by repeatedly pressing the space bar.

*In the display, look for the following line of information, which should be displayed twice: "SUNW,UltraSPARC-II (driver not attached)". If this line is displayed only once, this procedure must be aborted, after you exit from the "prtconf | less" command by entering* ***q****.*

**c** Type **q** on the command line, to exit from the command.

***Note:*** This is a safe stopping point in this procedure.

**6** Open a telnet connection to the APS server.

**7** Log in as the "maint" user.

**8** Become the "root" user by entering the following command and then entering the "root" password when prompted:

```
su - root
```

**9** At the APS server, 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, and then rewind the tape by entering the following command:

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

**10** Initiate a backup of the database to the tape by entering the following command:

```
ips_export_db.sh -t /dev/rmt/0c
```

*The system displays a log of activity as the database backup proceeds.*

***Note:*** This is a safe stopping point in this procedure.

**11** Rewind the backup tape by performing the following command:

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

**12** List the contents of the tape by entering the following command:

```
tar -tvf /dev/rmt/0c | more
```

*The system displays a listing of the tape contents. You should review this listing to ensure that all of the files were backed up.*

**13** Eject the backup tape, label it as "APS DB backup tape", 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.

***Note:*** This is a safe stopping point in this procedure.

**14** Insert another 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 server, and then rewind the tape by entering the following command:

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

**15** Enter the following commands to back up the APS file systems:

```
cd /
```

```
tar -cvf /dev/rmt/0c /PROV_data /audio_files
/user_audio_files /opt/uas/uas_conf_backup
(this command is entered on one command line)
```

***Note 1:*** When entering the command, you must ensure that a space is placed between the pathnames, "/PROV_data" and "/audio_files", between "/audio_files" and "/user_audio_files", and between "/user_audio_files" and "/opt/uas/uas_conf_backup"

***Note 2:*** This is a safe stopping point in this procedure.

**16** Rewind the backup tape by performing the following command:

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

**17** List the contents of the tape by entering the following command:

```
tar -tvf /dev/rmt/0c | more
```

*The system displays a listing of the tape contents. You should review this listing to ensure that all of the files were backed up.*

**18** Eject the backup tape, label it as "APS application file tape", 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.

***Note:*** This is a safe stopping point in this procedure.

**19** Determine the APS server hostname and IP address by entering the following command:

```
more /etc/inet/hosts
```

Record the APS hostname and IP address that display.

***Note:*** This is a safe stopping point in this procedure.

**20** Change the IP address of the APS server. This will prevent any conflicts when the APS software is installed on the CS 2000 Management Tools server.

**a** Type **cli** on the command line to start the “Command Line Interface” tool.

**b** In response to the “select” prompt, enter the number in the menu that is associated with “Configuration”.

**c** In response to the “select” prompt, enter the number in the menu that is associated with “IP Configuration”.

**d** In response to the “select” prompt, enter the number in the menu that is associated with “config_data”.

**e** In response to the “Primary IP Address” prompt, enter a new IP address that you obtained prior to starting this procedure.

**f** In response to the “Hostname for <IP address>” prompt, enter a new hostname that you obtained prior to starting this procedure.

**g** Type **ok** to commit the new IP address and hostname entries.

**h** After the tool displays a note about the changes you have just made and the need to reboot the system, the “IP Configuration” menu displays. Type **X** (exit) in response to the “select” prompt.

**i** When the “Configuration” menu displays, type **X** (exit) in response to the “select” prompt.

**j** When the “Command Line Interface” menu displays, type **X** (exit) in response to the “select” prompt.

**k** Reboot the APS server, to make the hostname and IP address changes active, by typing the following on the command line:

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

*The server reboots.*

***Note:*** This is a safe stopping point in this procedure.

**21** Open a telnet connection to the CS 2000 Management Tools server.

**22** Log in as the “maint” user.

**23** Become the “root” user by entering the following command and then entering the “root” password when prompted:

```
su - root
```

**24** If you have not already enabled multipathing on the CS 2000 Management Tools server, perform the following steps:

**a** Type **cli** on the command line to start the “Command Line Interface” tool.

**b** In response to the “select” prompt, enter the number in the menu that is associated with “Configuration”.

**c** In response to the “select” prompt, enter the number in the menu that is associated with “IP Configuration”.

**d** In response to the “select” prompt, enter the number in the menu that is associated with “config_test”.

**e** In response to the “Enter test IP address one” prompt, enter a test IP address that you obtained prior to starting this procedure.

**f** In response to the “Enter test IP address two” prompt, enter a test IP address that you obtained prior to starting this procedure.

**g** In response to the “Enter Network Timeout Value in seconds” prompt, enter a network timeout value or press the Return key to enter the default value.

**h** Type **ok** to commit the test IP address and network timeout value entries.

**i** When the “IP Configuration” menu displays, type **X** (exit) in response to the “select” prompt.

**j** When the “Configuration” menu displays, type **X** (exit) in response to the “select” prompt.

**k** When the “Command Line Interface” menu displays, type **X** (exit) in response to the “select” prompt.

***Note:*** This is a safe stopping point in this procedure.

**25** Add the former APS server IP address and hostname, that you recorded in step 19, to the CS 2000 Management Tools server.

**a** Type **cli** on the command line to start the “Command Line Interface” tool.

**b** In response to the “select” prompt, enter the number in the menu that is associated with “Configuration”.

**c** In response to the “select” prompt, enter the number in the menu that is associated with “IP Configuration”.

**d** In response to the “select” prompt, enter the number in the menu that is associated with “config_data”.

**e** In response to the “Primary IP Address” prompt, enter the CS 2000 Management Tools server IP address.

**f** In response to the “Hostname for <IP address>” prompt, enter the CS 2000 Management Tools server hostname.

**g** In response to the “Secondary IP Address” prompt, enter the former APS server IP address.

**h** In response to the “Hostname for <IP address you entered in the previous step>” prompt, enter former APS server hostname.

**i** In response to the “Third IP Address” prompt, press the Return key.

**j** Type **ok** to commit the new IP address and hostname entries.

**k** When the “Configuration IP” menu displays, type **X** (exit) in response to the “select” prompt.

**l** When the “Configuration” menu displays, type **X** (exit) in response to the “select” prompt.

**m** When the “Command Line Interface” menu displays, type **X** (exit) in response to the “select” prompt.

**n** Reboot the CS 2000 Management Tools server, to make the hostname and IP address changes active, by typing the following on the command line:

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

*The server reboots.*

***Note:*** This is a safe stopping point in this procedure.

**26** Install the APS07 load on the CS 2000 Management Tools server.

**a** Insert the APS07 installation CD into the CD-ROM drive of the CS 2000 Management Tools server.

**b** Enter the following command to ensure that the CD has been properly mounted:

```
df
```

In the list that displays, you should see the entry “/cdrom/<*xxx*>/”, where <*xxx*> is the CD volume label name.

**c** Copy the software from the CD to the file system and then list the software you have copied:

```
cp /cdrom/<xxx>/* /
```

```
ls -l *.pkg
```

**d** Install the APS software files by entering the following commands:

```
pkgadd -d NTaps07-xx.y.pkg
```

```
pkgadd -d NORTips07-xx.y.pkg
```

where *xx.y* is the version of the software that was listed above.

***Note:*** If the system prompts you about installing conflicting files, enter **n** (no).

**e** Run the APS software installation script:

```
./start.sh
```

After the installation completes, the system will reboot automatically.

**f** Log back into the CS 2000 Management Tools server as the root user, and remove the CD from the CD-ROM drive:

```
eject
```

**g** Install the APS MNCL (see release notes for instructions).

**27** Restore the APS database, on the CS 2000 Management Tools server.

**a** Insert the “APS DB backup tape” into the DDS-3 tape drive.

**b** Rewind the backup tape by performing the following command:

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

**c** Start the restoration of the APS database from the tape by entering the following command:

```
ips_export_db.sh -t /dev/rmt/0c -restore
```

*Messages logging the progress of the restoration display on the screen.*

***Note:*** When you are prompted about continuing the restoration even if the current database will be destroyed, enter “y” (yes).

**d** After the restoration of the APS database is complete, rewind the backup tape by performing the following command:

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

**e** Eject the backup tape and store it for possible use later.

**28** Restore the APS application files, on the CS 2000 Management Tools server.

**a** Insert the “APS application file tape” into the DDS-3 tape drive.

**b** Change directory to the root directory:

```
cd /
```

**c** Rewind the backup tape by performing the following command:

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

**d** Restore the application files (/PROV_data, /audio_files, /user_audio_files, and uas_conf_backup) by entering the following command:

```
tar xvf /dev/rmt/0c
```

**e** When the restoration of the application files completes, remove the tape from the tape drive and store for possible use later.

**f** 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.*

***Note:*** The “uas_conf_backup” file does not need to be checked. This is only a backup of the UAS configuration file that is backed up automatically to the APS server (or CS 2000 Management Tools server, after this procedure is complete) each morning at 1:00. Unlike the three other “application” files, it has no direct function in the normal operation of the APS.

**29** Configure the APS SNMP agent by performing the procedure, “Configuring the SNMP agent” in the *UAS Configuration module*, NTP NN10095511, in your Succession Solution customer documentation suite.

***Note 1:*** In response to the prompt, “What port does the agent use to receive SNMP messages from the element manager?” enter **5161** or any other un-used port. This same port number must then be used when the APS is added to the network topology of the Call Server Management Tools element manager.

***Note 2:*** This is a safe stopping point in this procedure.

**30** The old APS server can be switched off and removed from the network if required.

**31** You have completed this procedure.

# Combined server upgrade backout procedure

This procedure enables you to back out the combined server upgrade, if necessary.

### Combined server upgrade backout

***At the Windows desktop interface***

1 Open a telnet connection to the CS 2000 Management Tools server.

2 Log in as the “maint” user.

3 Become the “root” user by entering the following command and then entering the “root” password when prompted:

```
su - root
```

4 Remove the APS software by performing the following steps:

**a** Enter the following command on the command line:

```
APSagentctl stop
```

**b** Enter the following command on the command line:

```
pkgrm NTaps07
```

**c** Enter the following command on the command line:

```
drop_user_lion.sh
```

**d** Enter the following command on the command line:

```
remove_aps_package.sh
```

**e** Enter the following command on the command line:

```
pkgrm NORTips
```

***Note:*** This is a safe stopping point in this procedure.

5 Remove the APS server IP address and hostname from the CS 2000 Management Tools server.

**a** Type **cli** on the command line to start the “Command Line Interface” tool.

**b** In response to the “select” prompt, enter the number in the menu that is associated with “Configuration”.

**c** In response to the “select” prompt, enter the number in the menu that is associated with “IP Configuration”.

**d** In response to the “select” prompt, enter the number in the menu that is associated with “config_data”.

e In response to the “Primary IP Address” prompt, enter the CS 2000 Management Tools server IP address.

f In response to the “Hostname for <IP address>” prompt, enter the CS 2000 Management Tools server hostname.

g In response to the “Secondary IP Address” prompt, press the Return key.

h Type **ok** to commit the new IP address and hostname entries.

i Type **quit** to start exiting from the cli tool.

j When the “Configuration IP” menu displays, type **X** (exit) in response to the “select” prompt.

k When the “Configuration” menu displays, type **X** (exit) in response to the “select” prompt.

l When the “Command Line Interface” menu displays, type **X** (exit) in response to the “select” prompt.

6 Open a telnet connection to the standalone APS server.

7 Log in as the “root” user.

8 Change the IP address of the APS server.

a Type **cli** on the command line to start the “Command Line Interface” tool.

b In response to the “select” prompt, enter the number in the menu that is associated with “Configuration”.

c In response to the “select” prompt, enter the number in the menu that is associated with “IP Configuration”.

d In response to the “select” prompt, enter the number in the menu that is associated with “config_data”.

e In response to the “Primary IP Address” prompt, enter the APS IP address that you removed from the CS 2000 Management Tools server in step 5.

f In response to the “Hostname for <IP address>” prompt, enter the APS hostname that you removed from the CS 2000 Management Tools server in step 5.

g Type **ok** to commit the new IP address and hostname entries.

h Type **quit** to start exiting from the cli tool.

i After the tool displays a note about the changes you have just made and the need to reboot the system, the “IP Configuration” menu displays. Type **X** (exit) in response to the “select” prompt.

**j** When the “Configuration” menu displays, type **X** (exit) in response to the “select” prompt.

**k** When the “Command Line Interface” menu displays, type **X** (exit) in response to the “select” prompt.

**l** Reboot the APS server, to make the hostname and IP address changes active, by typing the following on the command line:

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

*The server reboots.*

**9** Perform the procedures for backing out the SSPFS software and the CS 2000 Management Tools software that you upgraded during the “Combined server upgrade” procedure. For the location of these procedures, contact your Nortel Networks service representative.

**10** You have completed this procedure.

# Preparing to upgrade the MG 9000

This document contains upgrade and downgrade information and procedures for the MG 9000 cards and the MG 9000 Manager.

## When to use this document

Use this document when it is necessary to upgrade the MG 9000 Manager and the MG 9000. Separate upgrade procedures are provided in this document that fit different upgrade scenarios as noted below:

- upgrading the MG 9000 Manager and MG 9000 from SN06.2 or SN06 to SN07. Throughout this document, substitute SN06 or SN06.2 for SN06.x as appropriate depending on the release from which you are upgrading.
- downgrading the software in the MG 9000 Manager and MG 9000
- upgrading the MG 9000 Manger software to a maintenance release
- upgrading the MG 9000 cards individually
- upgrading the MG 9000 cards by card type
- upgrading all the MG 9000 cards

When upgrading the MG 9000 Manager and MG 9000 from SN06.x to SN07, the following list provides an overview of upgrade activities which occur in the following order:

- upgrade the MG 9000 Manager master server and mid-tier software
- upgrade the OM Collector
- install the GUI client application
- provision userids
- export SN06.2 data to XML file
- upgrade MTA and xDSL cards
- upgrade software in MG 9000 cards
- import SN06.2 data from XML file
- remove SN06.2 software packages

Before proceeding to the upgrade checklist and any upgrade procedures, ensure all the information in this section is read and understood. The order for upgrading the MG 9000 and the MG 9000 Manager is presented in the MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server) on page 777 or MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)

on page 790. This checklist provides the required order and refers to specific procedures in this document and other documents while also providing simple steps for activities that must be performed at that time.

***Note:*** The above referenced checklist provides a high level procedure that provides the steps required for the upgrade of both the MG 9000 Manager and the MG 9000 from SN06.x to SN07. Specific upgrade procedures are provided for the MG 9000 Manager and the MG 9000 later in this document.

## Upgrade strategy

The following provides a high-level strategy for software upgrades of the MG 9000 Manager and the MG 9000 to SN07 which are accomplished in the following order in relation to other components in the solution:

1. The Communication Server 2000 (CS2000) Management Tools must be upgraded to SN07 to ensure node and line provisioning applications are updated. Refer to *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.
2. The Succession Server Platform Foundation Software (SSPFS) must be upgraded to SN07. Refer to “Upgrading SSPFS Software” in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450. This includes the SSPFS on the MG 9000 Manager master and mid-tier servers.

   ***Note:*** After the SSPFS platform software is upgraded to SN07 and the MG 9000 Manager restarts in SN06.x (step 1), and CS2000 Management Tools have been upgraded to SN07, the MG 9000 Manager server and mid-tier software can be upgraded (step 3).

3. The MG 9000 Manager software must be upgraded in the following order: server, mid-tier.
4. All the MG 9000 intelligent cards are upgraded to SN07 from an image received on CD using the Software Upgrade tool accessible from the Frame View.
5. The newly updated MG 9000 network element must be added to SN07.
6. Delete the MG 9000 network element being updated from SN06.x in the SN06.x Subnet View.
7. Once the MG 9000 is in the SN07 Subnet View, and the network element is deleted from the SN06.x Subnet View, any new hardware can be added into the system.
8. Remove old SN06.x packages.

## Service impacts

The following are the service impacts to consider when proceeding with the upgrade:

- Warnings for all components and services impacted during upgrade
  - — No data provisioning should be performed during upgrades.
  - — PM collection cannot be performed during the time between stopping the mid-tier server and starting the OM Collector. During the time when the DCC cards have been upgraded to SN07 but the NE still resides in the SN06.x Subnet View, the SN06.x OM Collector will not collect any OMs because of security features added in the MG 9000 card software.
  - — During the time when the DCC cards have been upgraded to SN07 but the NE still resides in the SN06.x Subnet View, the node is not being managed. Alarms are going to the SN06.x MG 9000 Manager but any alarms specific to SN07 MG 9000 card loads are being dropped. Once the NE is moved to SN07, all alarms even those dropped, will be shown in SN07.
  - — Call processing should not be impacted during the MG 9000 Manager upgrade.
  - — During the time when the DCC cards have been upgraded to SN07 but the NE still resides in the SN06.x Subnet View, ESA data download should not be performed. ESA data download cannot work because of a security functionality added in the SN07 MG 9000 card load. The SN06.x MG 9000 Manager does not have this security functionality. Once the MG 9000 is imported into SN07, ESA downloads can be performed.
  - — During a downgrade, the GWC cannot be downgraded until all MG 9000s that subtend it are downgraded.
  - — OC3 carriers must not be in split-mode, refer to procedure “Recovery from APS Split-mode” in *MG 9000 Fault Management*, NN10074-911.
  - — Prior to downgrading to SN06.x, the hardware versions should be checked to ensure that the PEC codes are not for the new SN07 hardware. If the new hardware is not removed, the SN06.x loads will be FTP’d to the boards but they will not run. Also, if the OC3 ports have been channelized, they must be manually

provisioned to OC-3 concatenated prior to downgrading. Refer to the following table to identify the PEC codes for SN07 cards.

**Table 1 SN07 upgrade PEC codes**

| Card type | Pre-SN07 PEC codes | SN07 new hardware PEC codes |
|---|---|---|
| ITP | NTNY30AA or NTNY30BA (IP) | NTNY30BA or NTNY30CB |
| ITX | NTNY41AA | NTNY41BA |
| DS-512 ABI | NTNY43AA | NTNY43BA or NTNY43BB |
| DCC-OC3 (SCO) | NTNY45AA | NTNY45CA |
| Hybrid DCC-OC3 (OC3) | NTNY45AA | |
| DCC-DS1IMA (SCI hybrid) | NTNY45BA | NTNY45BA |

- Recommendations for limiting service impact: none

## Upgrade and downgrade time factors

When preparing for an upgrade from SN06.x to SN07, time is a consideration. The factors affecting the upgrade and the amount of time involved are provided in the following table. In addition, formulae for computing upgrade and downgrade times for the MG 9000 Manager are provided in the table.

Upgrade procedure information:

- datafill changes required during upgrade: none required
- recommended soak time: 24 hours
- total upgrade time, high level estimates (worst case):

  ***Note:*** The following estimates are based on MG 9000s with 55,000 lines maximum.

  — upgrade - 182 minutes, 16 NEs

  — downgrade - 160 minutes, 16 NEs

  Use the information in the following table to compute the upgrade and downgrade activities.

**Table 2 Computing upgrade and downgrade times**

| Activity | Variables | Formula | Value (in minutes) |
|---|---|---|---|
| **Upgrade** | | | |
| | MG 9000 Manager upgrade time = | | |
| | (n x X) + ED + ER + EA + EeP + (n x I) + (n x P) | | |
| | where: | | |
| | n | is the number of network elements (assumes worst case of an 8 shelf NE) | |
| | X | is the time to export an 8 shelf NE | 1:20 |
| | I | is the time to import a single 8 shelf NE | 6:30 |
| | ED | is the time to take the MG 9000 Manager down | 1:21 |
| | ER | is the time to perform the SUN package remove | 1:00 |
| | EA | is the time to perform the SUN package add | 4:00 |
| | EeP | is the time to edit the Subnet Persistence file | 1:00 |
| | ES | is the time to start the MG 9000 Manager | 1:21 |
| | P | is the time to persist a single 8 shelf NE | 3:00 |

**Table 2 Computing upgrade and downgrade times**

| Activity | Variables | Formula | Value (in minutes) |
|---|---|---|---|
| | SC | is the static components = sum of ED = ER + EA + EeP + ES | 8:42 |
| | Example computation:<br>MG 9000 Manager upgrade time for 16k line network (all 8 shelves) =<br>(4 x 1:20) + SC + (4 x 6:30) + (4 x 3:00) =<br>(5:20) + (8.42) + (26) + (12:00) = 52 minutes | | |
| **Downgrade** | | | |
| | MG 9000 Manager downgrade time =<br>ED + ER + EA + EeP + ES + (n x I) + (n x P)<br>***Note:*** If an export is performed for one or more NEs between the MG 9000 Manager upgrade and the abort, no data will be available from the MG 9000 Manager for the downgraded NEs. | | |

## Tools and utilities

The MG 9000 and the MG 9000 Manager software support software upgrades and downgrades. Procedures in this document support these activities. The MG 9000 and MG 9000 Manager support patching through the network patch manager (NPM). Procedures for patching the MG 9000 and the MG 9000 Manager are provided in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.

The MG 9000 Manager provides a tool to upgrade the software in the intelligent DCC, ITX, ITP, DS-512 (ABI), and DS1 cards. A single card or multiple cards can be upgraded using this tool.

In addition, the software in the xDSL and MTA cards can be downloaded into the cards using the Software Download tool available from the xDSL and MTA Card Views in the MG 9000 Manager. Procedures for downloading software into the xDSL and MTA cards are provided in this document.

## MG 9000 Manager client system requirements

Recommended minimum configurations for the MG 9000 Manager client are provided in the following table.

**Table 3 MG 9000 Manager client minimum configurations**

| Client platform | Configuration |
|---|---|
| Windows client | • Windows NT 4.0 (SP5 or later), Windows 2000 (SP2 or later), or Windows XP<br>• Pentium III 1 GHz or higher<br>• display resolution of 1280 x 1024 with 256 colors<br>• 256 MB RAM<br>• 200 MB hard drive space<br>• 10BaseT/100BaseT Ethernet network connection<br>• Java Web Start (JWS) 1.2.0_02 and higher<br><br>If the Windows PC supports more Succession client applications than just the MG 9000 Manager client application, the following minimum configuration is required:<br>• Windows 2000 (SP2 or later), or Windows XP<br>• Pentium III 2.5 GHz or higher<br>• display resolution of 1280 x 1024 with 256 colors<br>• 1 Ghz RAM<br>• 30 Gb hard drive space<br>• 10BaseT/100BaseT Ethernet network connection<br>• Java Runtime Environment (JRE) 1.4.1_02 and higher<br>• Java Web Start (JWS) 1.4.2_05 and higher |
| Solaris client | • Solaris 7 or Solaris 8 with Sun recommended patches for Java Runtime Environment (JRE) 1.4.1_02<br>• Ultra 5 400 MHz or higher<br>• display resolution of 1280 x 1024 with 256 colors<br>• 256 MB RAM<br>• 200 MB hard drive space<br>• 10BaseT/100BaseT Ethernet network connection |

**Table 3 MG 9000 Manager client minimum configurations**

| Client platform | Configuration |
|---|---|
| Windows or Solaris client | Third party software<br>• Netscape 6.0 and higher or Internet Explorer 5.5, 6.0 and higher<br>• Java Web Start (JWS) 1.2.0_02 and higher |
| ***Note:*** Access to some functions requires the use of SSH compatible client software for access to secure telnet and ftp services (using SSH standard). SSH clients are supplied bundled with some operating systems, but may need to be obtained separately. Sources for SSH clients include, but are not limited to the following:<br>• PUTTY - freeware<br>• OpenSSH - freeware<br>• SSH Inc. - commercial<br>• Secure CRT - commercial<br>• WinSCP - freeware<br>Nortel Networks does not supply or recommend a particular supplier. | |

## Pre-upgrade requirements

Ensure the CS 2000 Manager has been upgraded to SN07 before upgrading any MG 9000s to SN07.

The MG 9000 Manager must be upgraded to SN07 first. This means the MG 9000 Manager is capable of managing an MG 9000 operating at SN07. However, this does not mean an MG 9000 at the SN06.x release is managed by an MG 9000 Manager at SN07. The MG 9000 is upgraded to SN07 and the network element (NE) representing the MG 9000 is moved from the SN06.x subnet to the SN07 subnet. An SN07 subnet/MG 9000 Manager cannot manage an MG 9000 at SN06.x.

***Note:*** All alarms on the MG 9000 Manager and MG 9000 network element must be cleared prior to proceeding with the SN06.x to SN07 upgrade process.

Do not provision any new data to the NEs during upgrade activities.

### Entry criteria

The following are the criteria for entering the SN06.x to SN07 upgrade process:

- host names and IP addresses required for:
  - the MG 9000 Manager mid-tier server
  - the MG 9000 Manager server
  - the CS 2000 Manager (Oracle database), required
  - the Security Authentication Host, typically the mid-tier IP address
  - the Imaging FTP Server Host, typically the SDM
- user id and password for the Imaging FTP Server Host, must have overwrite privileges
- hardware and software baseline:
  - MG 9000 card loads must be at SN06.x with all patches applied
  - MG 9000 Manager software must be at SN06.x with all patches applied and enabled
- tools required: database browser (optional)
- upgrade interdependency:
  - SSPFS on MG 9000 Manager master and mid-tier servers must be upgraded to SN07. SSPFS upgrades are covered in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.
  - CS 2000 Management Tools must be upgraded to SN07 prior to upgrading the MG 9000 Manager to SN07.

— MG 9000 card upgrades are addressed in Upgrading software in MG 9000 cards on page 921

— ensure MG 9000 PSEs are configured correctly before the upgrade starts. This requires the following steps:

***Note:*** If this is an N240 server, configure PSE on the workstation. If this is a t1400 server, configure PSE on the master and mid-tier servers.

– telnet to the specific machine to be upgraded by typing

```
> telnet <server ip address>
```

– change to the root directory by typing

```
$ su - root
```

– Access the command line interface by typing

```
> cli
```

– To select Configurations, type

```
> 2
```

– To select Succession Element Configuration, type

```
> 14
```

– To select PSE Configurations, type

```
> 1
```

– To select View PSE Configuration, type

```
> 1
```

– Ensure the PSE application is pointing to the CS 2000 Management Tools machine where NPM is running. If it is not configured correctly, reconfigure the PSE to point to the CS 2000 Management Tools machine where the NPM is running. Refer to “Upgrading the SSPFS Software” in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.

- datafill changes required prior to upgrade: All NEs which are being upgraded to SN07 may have their SN06.x data exported prior to upgrading. This is optional. However, no provisioning including OSSGate should occur between the point where the SN06.x data is exported and the node is imported in SN07. If data provisioning does occur, the SN06.x data can be exported again and this will overwrite the old SN06.x data. Refer to step 9 in the MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist

(one-server) on page 777 or step 14 in MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server) on page 790.

- if this is an SN06x to SN07 Sun Netra cluster (two-server) upgrade, run a getpatch to retrieve all SN07 patches before the upgrade starts. Refer to "Transferring patches to the NPM database manually" in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.

**Exit criteria**

The following are the criteria for exiting from the SN06.x to SN07 upgrade process:

- The upgrade was successful
  - — after the MG 9000 Manager mid-tier server and server applications are running in SN07
  - — after the NE is successfully discovered in SN07
- Recommended testing
  - — Make sure alarms are received (temporarily set a cooling unit breaker on the IBIP to off).
  - — Select a VMG from the Switched Line Services View. Select a termination and make sure that the termination properties show correctly.
  - — Select a Private lines service, if provisioned, and get the properties for it. Make sure the Svc OperStatus from the Service Properties View is connected for full and active endpoint services
- Log reports or operational measurements (OM): check the customer logs for audit messages indicate clean up failures.
- Equipment state verification: access the Oracle database and verify the same number of terminations exists (optional).

**Applying software fixes**

When it is necessary to apply software fixes, the following methods are available:

- Maintenance Release upgrade process: refer to the procedure "Upgrading the MG 9000 Manager software to a maintenance release" in Upgrading the MG 9000, NN10048-461
- Patching
  - — SN07 patching of the MG 9000 Manager is handled as noted in Patching MG 9000 Manager software on page 1776

# Preparing to upgrade the UAS

This document contains the following procedures:

- Upgrades
  - — Upgrade from release UAS06 or UAS07 to release UAS08
  - — Upgrade from one version of release UAS08 to a later version of release UAS08
  - — UAS08 ground up installation
- Downgrades
  - — Downgrade from release UAS08 to release UAS07 or UAS06
  - — Downgrade from one version of release UAS08 to a previous version of release UAS08

## Tools and utilities

This section contains the following information, which will help you prepare for an upgrade or downgrade of the system:

- a description of upgrade prerequisites, such as hardware replacements that must be completed before the upgrade is started
- a description of special considerations, such as where the upgrade is performed, impact of the upgrade on office operation, and how datafiles can be backed up for restoration
- information about the media necessary for performing an upgrade
- a description of the UAS database backup and restoration strategy
- information about upgrading the APS, including where the APS upgrade instructions can be found

### UAS Installation prerequisites

Before an upgrade is started, the configuration information outlined in Configuration information on page 336, appropriate for the type of upgrade, should be collected and recorded for quick reference during the upgrade. For additional information about configuration parameter input, see “Customer Questionnaire” in Upgrading the UAS, NN10047-461.

Before installation of the UAS or APS software is performed, the following tasks must be completed:

- installation of the audio management software on the APS node, if the UAS system is connected to its own APS node
- installation of the following third-party hardware necessary for the operation of a specific UAS application
  - — Natural MicroSystems CG6000C card(s) - (VoIP) (For a procedure used to install or reconfigure CG6000 cards, see “Adding a CG6000 card to a UAS node” or “Removing a CG6000 card from a UAS” in the document NN10073-911, entitled “UAS Fault Management.”)
  - — Natural MicroSystems AG4000C card(s) - (VoATM) (For a procedure used to install or reconfigure AG4000 cards, see “Adding an AG4000 card to a UAS node” or “Removing an AG4000 from a UAS node” in the document NN10073-911, entitled “UAS Fault Management.”)
  - — Natural MicroSystems PA200 card - (VoATM-AAL1 and AAL2) (For a procedure used to install a PA200 card, see Replacing a BX4000c (S007) card with a PA200 card on page 934.)

## UAS upgrade special considerations

### Where an installation or upgrade is performed

All steps in the installation and upgrade procedures are performed at the local console.



**CAUTION**

No remote access sessions (telnet, ftp) should be in progress on a unit that is being installed, upgraded, or downgraded.

### Upgrade interdependencies

None.

### Office impact

The following general impact on an office can be expected during a UAS software upgrade:

- A UAS unit must be out of service when it is being upgraded. When the unit is out of service, other UAS units in the cluster continue to process calls.
- While an APS is out of service, audio provisioning cannot be performed; the UAS units in the cluster can, however, continue to process calls.
- During software installation, audio distribution to the UAS unit being upgraded is disabled.
- Multiple UAS units can also be upgraded in parallel as long as the requisite number of units required to handle call processing during the upgrade procedure remain in service.
- When, through the Universal Audio Server Manager, the administrative state of the UAS is set to “lock graceful” in preparation for the upgrade, all active calls in the UAS unit being upgraded complete before the unit goes out of service.

### Software removal

Before an upgraded, or previous, version of the UAS software can be installed, it is necessary to remove the existing UAS software. If a software upgrade or downgrade is attempted when the existing software has not been removed, an error message is issued and the UAS installation program (“setup.exe”) exits.

The procedures used to remove UAS software include steps that save the UAS system configuration parameters before the system configuration files are removed. Thus, during a subsequent re-installation, the configuration parameters can be restored.

### Hardware precautions



**CAUTION**
**Catastrophic Hardware Failures - Please Read**
If, during the Universal Audio Server installation, a catastrophic hardware failure is experienced on the node, it is necessary to terminate the installation at that point and execute a ground up installation. A catastrophic hardware failure is characterized by, but not limited to, loss of power to the node, surprise extraction of a system controller card, or surprise extraction of the hard disk drive. In the event that a catastrophic hardware failure occurs, contact your Nortel Networks service representative for assistance.

**Disk Drive** Under no circumstances should the locking key on the system hard drive be turned while the system is operational. Turning this key while the system is operational can result in false error condition reporting by the system. If a disk becomes faulty during a system upgrade and requires replacement, the procedure, “Replacing a UAS disk drive,” located in the document, NN10047-461, entitled “UAS Fault Management” should be consulted for instructions.

## UAS Installation media

Installation is performed from the Universal Audio Server UAS08.0 Installation CD. This CD contains one folder, named “WINNT.”

### WINNT folder

The WINNT folder contains the callp application software to be installed on the cPCI. Specifically, the folder contains the Setup.exe installation file and its associated files. In addition, the folder contains the sub-folders, “Extras,” “IML,” and “NMS.”

The “NMS” folder contains the self-extracting/self-installing files used for the installation of the Natural MicroSystems Software applications.

The “ATM” folder contains the self-extracting/self-installing file used for the installation of the Natural MicroSystems software application.

The “Extras” folder contains files for the Microsoft tool, “Visual File Information,” which retrieves and generates file information. This tool can be used to uncover differences between two seemingly identical machines. Although the tool is not used during installation, it is available for administrative use.

## UAS system configuration backup/restore strategy

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

### Automatic configuration file back-up

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 associated with the UAS node you are updating, the configuration files for that UAS node, and all UAS nodes in the network, can be backed up to the APS node. This capability is set up by entering the APS node IP address in the "Backup Storage IP" field of the Local Configuration Interface GUI screen, in the Procedure, UAS07 application software installation on page 992972972. 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 capability is established through step 19 of the UAS07 application software installation procedure. The remote server IP address must then be entered 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."

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.

The files that are backed up 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)

### APS installation

Starting with release APS07, the APS server is configured on a server that also hosts the CS 2000 Management Tools, "Succession Element and Sub-Network Manager (SESM)," "CS 2000 GWC Mgr," "UAS Mgr," and "Network Patch Manager (NPM)." For the procedure used to upgrade the APS software when the APS resides on this "CS 2000 Management Tool," see your solution's Upgrades document.

***Note:*** Release APS08 can only be installed on an APS that is configured on the CS 2000 Management Tool (described in the paragraph above). For a procedure used to combine an APS at release level APS06 or APS07 with the CS 2000 Management Tool, see your solution's Upgrades document.

### APS Patching

Patches to the APS software are delivered in the form of patch packages, which replace one or more application files. The procedure, "APS08 maintenance release process" in Upgrading the UAS,

NN10047-461 contains the instructions for applying a patch or "maintenance release." For assistance in performing a maintenance release, contact your Nortel Networks service representative.

## Upgrade procedures

The following tables list the procedures you use to perform upgrades or downgrades.

***Note:*** The procedures in this document are presented in a hierarchical format: top-level procedures consisting of steps that describe the tasks to perform reference sub-procedures that enable you to actually perform the tasks. It is important, therefore, that you use and follow the top-level procedures listed in the following tables. The Bookmarks panel, which displays on the left side of this document, lists the content of the document. Although it can be used for quick access to the procedures in this document, it doesn't show which upgrade or downgrade tasks to perform or the order in which to perform the tasks.

**Table 4 UAS08 upgrade procedures**

| Procedure and page |
|---|
| UAS06 or UAS07 to UAS08 software upgrade procedure on page 930 |
| UAS08 to UAS08 Upgrade on page 966 |
| "UAS08 ground up installation" in Upgrading the UAS, NN10047-461 |

**Table 5 UAS08 downgrade procedures**

| Procedure and page |
|---|
| "UAS08 to UAS07 or UAS06 software downgrade" in Upgrading the UAS, NN10047-461 |
| "UAS08 to UAS08 downgrade" in Upgrading the UAS, NN10047-461 |

**Table 6 Procedure for performing an APS maintenance release**

| Procedure and page |
|---|
| "APS08 maintenance release process" in Upgrading the UAS, NN10047-461 |

## Configuration information

Before an upgrade is started, the configuration information outlined in the tables below should be collected and recorded for quick reference during the upgrade. For additional information about configuration parameter input, see, Customer Questionnaire.

The following table contains the configuration parameters that must be datafilled for an ATM-AAL1 fabric UAS node.

**Configuration information for an ATM-AAL1 fabric UAS**

| Parameter | Entry for this node |
|---|---|
| **General** | |
| ATM companding mode | |
| optical carrier mode | |
| NTP server IP | |
| backup storage IP | |
| ATM Ctone support | |
| **Call Agent** | |
| Primary Call Agent name | |
| Primary Call Agent IP address | |
| Primary Call Agent port | |
| UAS call control port | |
| **Log Levels** | |
| system log level | |
| UAS log level | |
| application log level | |
| security log level | |

The following table contains the configuration parameters that must be datafilled for an ATM-AAL2 fabric UAS node.

**Configuration information for an ATM-AAL2 fabric UAS (Sheet 1 of 2)**

| Parameter | Entry for this node |
|---|---|
| **General** | |
| ATM companding mode | |
| optical carrier mode | |
| Gateway control protocol | |
| IVR support | |
| NTP server IP | |
| primary DBserver host | |
| primary DBserver IP | |
| backup storage IP | |
| audio synch on restart | |
| ATM BCT support | |
| ATM Ctone support | |
| **Call Agent** | |
| Primary Call Agent name | |
| Primary Call Agent IP address | |
| Primary Call Agent port | |
| UAS call control port | |
| legacy announcements | |
| primary language | |
| secondary language | |
| **Log Levels** | |
| system log level | |

**Configuration information for an ATM-AAL2 fabric UAS (Sheet 2 of 2)**

| Parameter | Entry for this node |
|---|---|
| UAS log level | |
| application log level | |
| security log level | |

The following table contains the configuration parameters that must be datafilled for AG4000 cards provisioned in an ATM-AAL2 fabric UAS node that supports trunk testing.

**Configuration information for ATM-AAL2 fabric AG4000 cards**

| Parameter | Entry for this node |
|---|---|
| test trunk support | |
| test trunk config size | |
| Sage box 1 IP | |
| Sage box 2 IP | |

The following table contains the configuration parameters that must be datafilled for an IP fabric UAS node.

**Configuration information for an IP fabric UAS (Sheet 1 of 2)**

| Parameter | Entry for this node |
|---|---|
| **General** | |
| Gateway control protocol | |
| IVR support | |
| conferencing state | |
| conference spanning | |
| conference expansion ports | |
| NTP server IP | |
| primary DBserver host | |
| primary DBserver IP | |
| backup storage IP | |
| audio synch on restart | |
| tone set | |
| **Bearer** | |
| RTP base port | |
| transmit gain | |
| receive gain | |
| default TOS | |
| RFC2833 DTMF | |
| RFC2833 DTMF squelch | |
| G729B | |
| supported codec | |
| **Call Agent** | |

**Configuration information for an IP fabric UAS (Sheet 2 of 2)**

| Parameter | Entry for this node |
|---|---|
| Primary Call Agent name | |
| Primary Call Agent IP address | |
| Primary Call Agent port | |
| UAS call control port | |
| legacy announcements | |
| primary language | |
| secondary language | |
| **Log Levels** | |
| system log level | |
| UAS log level | |
| application log level | |
| security log level | |

The following table contains the configuration parameters that must be datafilled for each CG6000C card provisioned in an IP fabric UAS node.

**Configuration information for IP fabric CG6000C cards**

| Parameter | Entry for this node |
|---|---|
| IP address | |
| router IP address | |
| netmask | |
| BCT support | |
| test trunk support | |
| test trunk config size | |
| Sage box 1 IP | |
| Sage box 2 IP | |

The following table contains the SNMP management configuration parameters that must be datafilled for ATM and IP fabric UAS nodes.

**Configuration information for SNMP management in an ATM or IP fabric UAS**

| Parameter | Entry for this node |
|---|---|
| v2c read-write community | |
| v2c read only community | |
| v3 read/write user | |
| v3 read-only user | |
| trap version | |
| trap destination | |
| trap port | |

# Preparing to upgrade the Gateway Controller

This section provides details on specific items that personnel need to be aware of prior to upgrading GWC nodes in a CS 2000.

Ensure that you research each item in the GWC upgrade preparation list in the following table:

**GWC upgrade preparation list**

| Item | √ | Details |
|---|---|---|
| Upgrade paths supported | | Depends on your solution.<br><br>See the supported upgrade paths in your solution's upgrade NTP, NN10344-450 or NN10261-450. |
| Upgrade order for all GWC card types | | Applicable to all solutions.<br><br>See section Upgrade order for all GWC card types on page 345. |
| Upgrade and downgrade call service impact | | Applicable to all solutions.<br><br>See Upgrade and downgrade call service impact on page 347. |
| PVG trunk GWC upgrades and downgrades | | Applicable to IP and AAL2 solutions.<br><br>See PVG trunk GWC upgrades and downgrades on page 348. |
| Ensure compliant characters in RMGC application domain name | | Applicable to IP solutions (Integrated Access Wireline, Cable, IP).<br><br>See Ensuring compliant characters in RMGC application domain name on page 349. |
| Allocate time for a GWC upgrade | | Applicable to all solutions.<br><br>See Allocating time for a GWC upgrade on page 350. |
| Impact of an upgrade on GWC configuration | | Applicable to all solutions.<br><br>See Impact of an upgrade on GWC configuration on page 350. |

## Upgrade order for all GWC card types

All GWC cards of the same type must be upgraded before moving on to the next group. For example, all audio controller GWC cards must be upgraded before upgrading the next GWC card-type present in your system.

The order presented includes all GWC card types, even though some of the card types indicated cannot co-exist in the same installation. For the GWC card type order specific to your solution, refer to the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

Upgrade GWC card pairs from SN05, SN06, SN06.2, or SN07 to SN07 in the following order of card type:

***Note:*** For definitions of the terminology in the list, refer to the Glossary of terms in the Gateway Controller Basics NTP, NN10189-111.

**GWC card type upgrade order**

| Order | GWC card type |
|---|---|
| 1 | AC |
| 2 | BICC - UA-AAL1 solutions only |
| 3 | VRDN |
| 4 | Session Server - SN07 to SN07 upgrades only; see Note 1 |
| 5 | SIP-T/APG/RA - see Note 2 |
| 6 | APG/RA - see Note 2 |
| 7 | SIP-T/APG |
| 8 | APG |
| 9 | SIP-T |
| 10 | Trunk |
| 11 | H.323 - controls Real time protocol Media proxy (RTP MP) |
| 12 | V5.2 trunk |
| 13 | Lines - includes CICM |

***Note 1:*** The Session Server (SS) is a new component in SN07. It can replace the Virtual Routing Destination Node (VRDN) GWC as a SIP-T interface. The following office configurations are supported in SN07: SS only, VRDN SIP-T only, or VRDN SIP-T and SS co-existing in the same office. For the upgrade order specific to your solution, refer to the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

***Note 2:*** Offices can only have one GWC with an RA. Therefore, an office will either have a SIP-T/APG/RA GWC or an APG/RA GWC but not both. In addition, some non-AAL1 solutions will support provisioning a combination of DPT and APG endpoints on the same GWC. This allows endpoints of different GWC types to coexist on the same GWC card. Referred to as a “combo profile”, the GWC is limited to 1008 APG ports, while the APG standalone is limited to 3024 APG ports. The RA server can be included or excluded on the same GWC under both APG capacity variants.

***Note 3:*** Parallel upgrades are not supported. While it is possible to save time by loading all GWC card pairs of a given GWC type and performing all the SwActs at the same time, this is not recommended or supported for a live office upgrade as this would cause an out of service condition for all GWC nodes.

***Note 4:*** Starting in SN06, the Redirecting media gateway controller (RMGC) application migrates from the CS 2000 Management Tools server to the GWC platform. RMGC service cannot be provided between upgrading the CS 2000 Management Tools server and commissioning the GWC-based RMGC service. Refer to the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP) for a complete migration strategy for this feature.

It is assumed that an existing Audio Controller GWC will be used to host the RMGC application. If commissioning a new GWC for RMGC in SN07, refer to appropriate procedures in the Gateway Controller Configuration Management NTP, NN10205-511.

## Upgrade and downgrade call service impact

The following matrix shows expected service impact for the GWC card types over the supported GWC load change scenarios.

***Note:*** Contact Nortel customer support for information on call service impact regarding any upgrade involving SN06.1.

### Upgrade and downgrade call service impact

| GWC type | SN05/06/6.2 -> SN07 Upgrade | SN07 -> SN07 Maintenance (Patching) | SN07 -> SN06.2/06 Downgrade | SN07 -> SN05 Downgrade |
|---|---|---|---|---|
| AUDCNTL | Stable announcement and conference calls survive. | Stable announcement and conference calls survive. | Stable announcement and conference calls survive. | Stable announcement and conference calls not using SN07 features survive. |
| VRDN | All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive. | ALL calls survive. | ALL calls survive. | Calls not using SN07 features survive. |
| SIP-T | All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive. | ALL calls survive. | NO calls survive. | NO calls survive. |
| PVG Trunk | All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive. | ALL calls survive. | NO calls survive. | NO calls survive. |
| APG | All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive. | ALL calls survive. | SIP-T calls using an APG do not survive. | SIP-T calls using an APG do not survive. |
| Line or H.323 | Stable 2-party calls survive. Possible limited functionality after the swact.<br>For unstable dialing, ringing, clearing or multi-party calls the behavior is unpredictable. | Stable 2-party calls survive. Possible limited functionality after the swact.<br>For unstable dialing, ringing, clearing or multi-party calls the behavior is unpredictable. | SOME calls may survive.<br>Billing records might not be produced when calls go on-hook.<br>H.323 gateway-based calls will not survive. | SOME calls may survive.<br>Billing records might not be produced when calls go on-hook.<br>H.323 gateway-based calls will not survive. |

## PVG trunk GWC upgrades and downgrades

SN05 to SN07 upgrades and SN07 to SN05 downgrades to PVG TDM trunk GWCs are impacted by changes in the IP IW SPM and the CS 2000 software loads. This item applies to IP and AAL2 solutions. These changes involve how echo cancellation (ECAN) is managed to accommodate the IP IW SPM. In an SN05 to SN07 upgrade, the GWC is upgraded before the CS 2000. Once the PVG GWC is upgraded to software release GC07/GT07, it will manage ECAN control for PVGs differently. This change also has an impact on upgrade rollbacks. The details of this change are as follows.

Prior to SN06, if a trunk GWC-based ISUP or PRI trunk group was datafilled in table TRKSGRP with field ECSTAT set to EXTERNAL, the GWC would send a command to activate the echo canceller integrated in the TDM gateway for that trunk group. This would occur unless ISUP or PRI messaging indicated that echo cancellation was already being performed between the echo cancellation and the source of the echo. If the ECSTAT field was not set to EXTERNAL for an ISUP or PRI trunk (that is, it was set to NONE), the echo canceller in the gateway would not be activated by the GWC under any circumstances.

In SN06 and any subsequent releases, this behavior is essentially reversed such that the echo canceller in the gateway will be activated automatically if the ECSTAT field is set to INTERNAL on GWC-based ISUP or PRI trunk types. If the ECSTAT field is set to EXTERNAL, it is assumed that an external echo canceller exists on the TDM trunk connected to the TDM gateway and that the external echo canceller has cancelled the echo. Therefore, if the TRKSGRP ECSTAT field is set to EXTERNAL, the echo canceller in the gateway will not be activated.

The new interpretation of the ECSTAT field will take effect upon activation of the GC07/GT07 GWC software load, after the upgraded trunk GWC card is rebooted. The only valid values for TRKSGRP field ECSTAT for GWC PRI and ISUP trunks in SN07 will be EXTERNAL or INTERNAL.

On upgrade from SN05 to SN07, GWC ISUP trunks datafilled as EXTERNAL will be reformatted to INTERNAL. GWC PRI trunks will be reformatted to INTERNAL. GWC ISUP and PRI trunks will always indicate to upstream or downstream switches that echo cancellation has been applied on the TDM interface (either externally or internally). During a GWC upgrade from SN05 to SN07, the following occurs:

- When the inactive side of the GWC is loaded with the GC07/GT07 load or later, the trunk sub group data in the GWC will change

ECSTAT from NONE to EXTERNAL and from EXTERNAL to INTERNAL.

- When the Core is upgraded to SN07, the same table changes will occur for GWC based trunk groups only.

If a GWC is rolled back (downgraded) from SN07 to SN05, then all the trunks on that GWC have to be BSY/RTS so that they receive the right ECSTAT datafill. However, the rollback must occur before the Core is upgraded for the BSY/RTS of the GWC to have the correct effect. If the Core is already upgraded and rolled back, the TRKSGRP data is not reverted and a subsequent rollback of the GWC to SN05 will result in incorrect ECAN behavior on all GWC based ISUP and PRI trunk groups.

## Ensuring compliant characters in RMGC application domain name

If you are upgrading to SN07 and intend to use the Redirecting Media Gateway Controller (RMGC) application, you need to be aware that using invalid or non-RFC 1034 compliant characters (such as the underscore character) for the GWC domain name in the GWC database could render the RMGC application unusable. Check the cmshortCLLIname, which is datafilled in table OFCENG as office parameter OFFICE_CLLI_NAME in the XA-Core, before the upgrade begins to determine if it uses any characters that are not compliant with RFC 1034. Correct this value before the upgrades are started on the XA-Core. Refer to your applicable Office Parameter Reference Manual, NTP 297-8001-855 or NTP 297-9051-855, to perform this task.

Consult your site system administrator for assistance in determining the domain name for your site. If you are commissioning a new GWC for RMGC in SN07, refer to procedures in the GWC Configuration Management NTP, NN10205-511.

## Allocating time for a GWC upgrade

The time required for an average upgrade is 24 minutes for each GWC node (card pair) for the GWC software. Under a moderately loaded 10BaseT network, the load takes about 2 minutes to transfer. Transfer time can increase over a heavily loaded network.

The following time factors apply to tasks in the GWC upgrade activity.

- Total upgrade time for each GWC pair is 24 minutes (12 minutes for each card)
- Time needed to apply GWC fileset to CS 2000 Core Manager or CBM is 5 minutes
- Time to perform a GWC node warm SWACT is 1 minute
- Time to post upgrade call processing check for each GWC node is 2 minutes

## Impact of an upgrade on GWC configuration

Once the CS 2000 Core Manager or CBM is upgraded, you cannot provision Gateway Controllers until the CS 2000 Management software package is upgraded and configured on the CS 2000 Management Tools server.

## CS 2000 call agent identifier required in SN07

When upgrading to an SN07 you need to set the call agent identifier (ID) for each CS 2000 in your network using the CS 2000 GWC Manager.

Setting the call agent ID for a CS 2000 distinguishes it from other CS 2000 devices in your network. It also permits the automatic assignment of a unique middebox ID for each network address translator (NAT) provisioned in your network. When provisioning a NAT, the system generates a middlebox ID. Starting in SN07, the Call Agent ID is incorporated in this automatically generated number. This ensures the uniqueness of all NAT middlebox IDs across more than one CS 2000.

***Note:*** It is the user's responsibility to ensure that the call agent ID assigned to each CS 2000 in the network is unique.

The presence of unique IDs for each CS 2000 and for each NAT middlebox in the network allows inter-CS 2000 trunks to be configured as intra-domain SIP-T trunks. Therefore, NAT VPN information for both ends of the call can be communicated and compared. This enables the flow of information between gateways hosted on different CS 2000s through the insertion of media proxies, as required. NAT information can be compared even if the gateways reside in different VPNs.

In addition to NATs, middlebox IDs for policy enforcement point (PEP) servers and limited bandwidth links (LBLs) are also automatically generated using the CS 2000 call agent ID.

## Upgrading GWCs containing NATs or PEP servers

During an upgrade to SN07, the need to upgrade the middlebox IDs of existing NATs means that a temporary increase the use of media proxies may occur. GWCs with different versions of software may have different middlebox IDs for the same NAT. This temporary increase may depend on the network configuration and the order in which the GWC nodes are upgraded. It may be advantageous to limit the period of time during which there are GWC cards at different software versions.

If you have NATs or PEP servers in your network, and you need to

upgrade your GWC cards to SN07, it is recommended that you perform one of the following procedures:

- Upgrade without soak test
- Upgrade with soak test on page 353



**CAUTION**

If a temporary increase in the use of media proxies is likely to have a negative impact on your network, take the following precautions:

- Perform any steps to upgrade GWC cards during a low traffic period.
- Try to limit the time it takes to perform any steps to upgrade GWC cards.

If necessary, contact Nortel customer support for advice on how to proceed.

## Upgrade without soak test

Perform an upgrade without a soak test using the following steps:

1. Set a unique call agent identifier (ID) for the CS 2000. Refer to procedure Set the call agent identifier on page 33.

   The CS 2000 Management Tools software generates new middlebox IDs for the following items that have already been provisioned:

   - network address translators (NATs)
   - policy enforcement point (PEP) servers

2. Upgrade all GWC cards that will support internet transparency media endpoints in SN07.

   To upgrade a GWC card, refer to Upgrading the Gateway Controller on page 834.

   As part of this upgrade, the new middlebox IDs for already provisioned NATs are downloaded to each GWC. Therefore, additional media proxy usage may occur, depending on the network configuration and the order in which the GWC nodes are upgraded.

   ***Note:*** If a temporary increase in the use of media proxies is likely to have a negative impact on your network, then perform

this step during a low traffic period. Also, try to limit the time it takes to perform this step.

3. If there are Centrex IP Client Manager (CICM) gateways in the network, the middlebox IDs on the CICM Element Manager must also be upgraded to reflect the new middlebox IDs.

   This must be done before the CICM is upgraded to SN07.

   For information on working with the CICM, refer to your CICM documentation.

4. Repeat steps 1 to 2 for each CS 2000 in your network.

   Intra-domain SIP-T trunks may now be configured. You can configure intra-domain SIP-T trunks by modifying the XA-Core TRKOPT table at the maintenance and administration position (MAP). Refer to procedure “Provisioning dynamic packet trunks” in the CS 2000 Configuration Management NTP applicable to your solution.

## Upgrade with soak test

Perform an upgrade with a soak test using the following steps

1. Upgrade a small number of GWC nodes supporting internet transparency media endpoints to SN07.

   To upgrade a GWC card, refer to Upgrading the Gateway Controller on page 834.

2. Perform a soak test on the GWC cards upgraded in step 1.
3. Set a unique call agent identifier (ID) for the CS 2000. Refer to procedure Set the call agent identifier on page 33.

   The CS 2000 Management Tools software generates new middlebox IDs for the following items that have already been provisioned.

   - network address translators (NATs)
   - policy enforcement point (PEP) servers

4. Perform the following steps for each GWC node that has been upgraded and soak tested. Refer to the GWC Security and Administration NTP, NN10213-611, for procedures to perform each of the steps:

   a. Busy the standby unit.
   b. Lock the standby unit.
   c. Unlock the standby unit.
   d. SwAct the GWC units in the node.

e. Busy the new standby unit.

f. Lock the new standby unit.

g. Unlock the new standby unit.

This causes the new middlebox IDs generated in step 3 to be downloaded to each GWC card in a node.

5. Upgrade all remaining GWC cards that will support internet transparency media endpoints in SN07.

   To upgrade a GWC card, refer to Upgrading the Gateway Controller on page 834.

   As part of this upgrade, the new middlebox IDs for already provisioned NATs are downloaded to each GWC. Therefore, additional media proxy usage may take place, depending on the network configuration and the order in which the GWC nodes are upgraded.

   ***Note:*** If a temporary increase in the use of media proxies is likely to have a negative impact on your network, then perform this step during a low traffic period. Also, try to limit the time it takes to perform this step.

6. If there are Centrex IP Client Manager (CICM) gateways in the network, the middlebox IDs on the CICM Element Manager must also be upgraded to reflect the new middlebox IDs.

   This must be done before the CICM is upgraded to SN07.

   For information on working with the CICM, refer to your CICM customer documentation.

7. Repeat step 1 through step 5 for each CS 2000 in your network.

   Intra-domain SIP-T trunks may now be configured. You can configure intra-domain SIP-T trunks by modifying the XA-Core TRKOPT table at the maintenance and administration position (MAP). Refer to procedure “Provisioning dynamic packet trunks” in the CS 2000 Configuration Management NTP applicable to your solution.

# Set the call agent identifier

## Purpose of this procedure

This procedure allows you to set a unique call agent identifier (ID) for each Communication Server 2000 (CS 2000) in the network.

Setting the call agent ID for a CS 2000 distinguishes it from other CS 2000 devices in your network. It also permits the automatic assignment of a unique middebox ID for each network address translator (NAT) provisioned in your network. When provisioning a NAT, the system generates a middlebox ID. Starting in SN07, the Call Agent ID is incorporated in this automatically generated number. This ensures the uniqueness of all NAT middlebox IDs across more than one CS 2000.

***Note:*** It is the user's responsibility to ensure that the call agent ID assigned to each CS 2000 in the network is unique.

The presence of unique IDs for each CS 2000 and for each NAT middlebox in the network allows inter-CS 2000 trunks to be configured as intra-domain SIP-T trunks. Therefore, NAT VPN information for both ends of the call can be communicated and compared. This enables the flow of information between gateways hosted on different CS 2000s through the insertion of media proxies, as required. NAT information can be compared even if the gateways reside in different VPNs.

In addition to NATs, middlebox IDs for policy enforcement point (PEP) servers and limited bandwidth links (LBLs) are also automatically generated using the CS 2000 call agent ID.

***Note:*** It is recommended that the call agent ID not be changed after it has been set.

## When to use this procedure

Use this procedure if you are upgrading your GWC nodes to SN07.

***Note:*** For additional information on when and how to set the call agent ID as part of an SN07 upgrade, refer to CS 2000 call agent identifier required in SN07 on page 351.

The call agent ID value must be set before you can provision any of the following:

- NAT devices
- PEP servers
- LBLs

For details, refer to the GWC Configuration Management NTP, NN10205-511.

You may also use this procedure if you need to change the call agent ID for a CS 2000. This should not be required for the normal operation of your network.

***Note:*** It is recommended that the call agent ID not be changed after it has been set.

**CAUTION**

Changing the call agent ID will make it more difficult to rollback (downgrade) your GWC cards to an earlier software load.

## Prerequisites

Ensure that you upgrade the CS 2000 Management Tools software package (CS2M) to SN07. Specifically, the CS 2000 GWC Manager and Nodes Configuration applications must be upgraded.

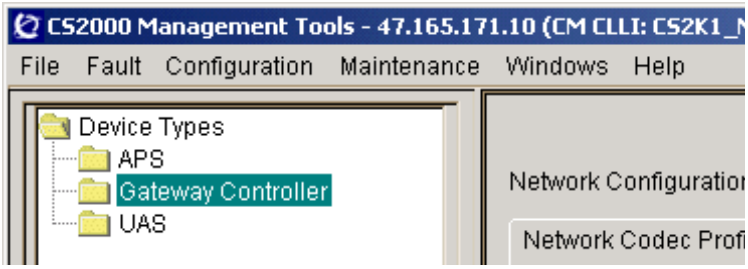
For details, refer to the upgrades NTP for your solution.

***Note:*** For additional information on when and how to set the call agent ID as part of an SN07 upgrade, refer to CS 2000 call agent identifier required in SN07 on page 351.

## Action

### *At the CS 2000 GWC Manager client*

**1** At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types menu.

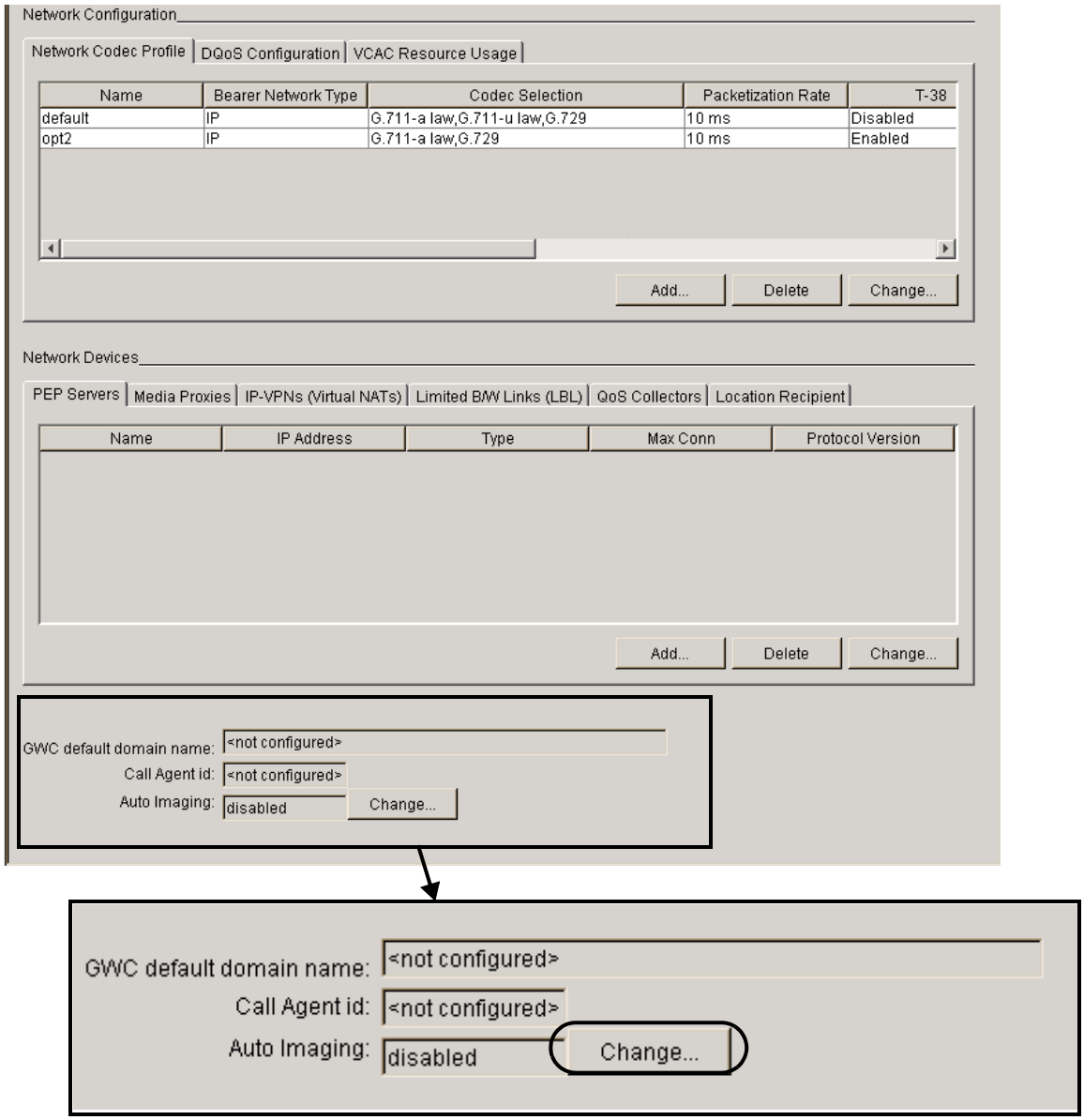


2 Note the current setting for Call Agent id at the bottom of the screen.

Call Agent id will have one of the following values:

- <not configured>
- A unique identifier between 1 and 255 inclusive

Disregard the other settings in this part of the screen for the purpose of this procedure. If you wish to change other settings, refer to the appropriate procedure in this NTP.

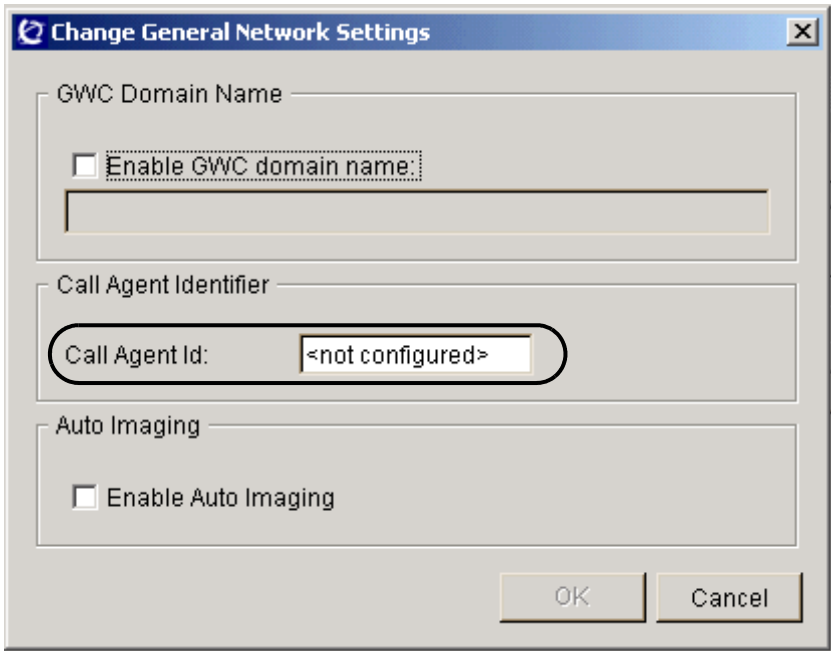


3 Determine your next step using the following table:

| If | Do |
|---|---|
| you wish to set the call agent ID for the first time | step 4 |
| you wish to change a call agent ID that has already been set | step 5 |

4 Perform the following steps to set the call agent ID for the first time:

**a** Click the **Change** button at the bottom of the network screen to display the Change General Network Settings window.




**b** Click in the Call Agent id field and assign a call agent ID value.

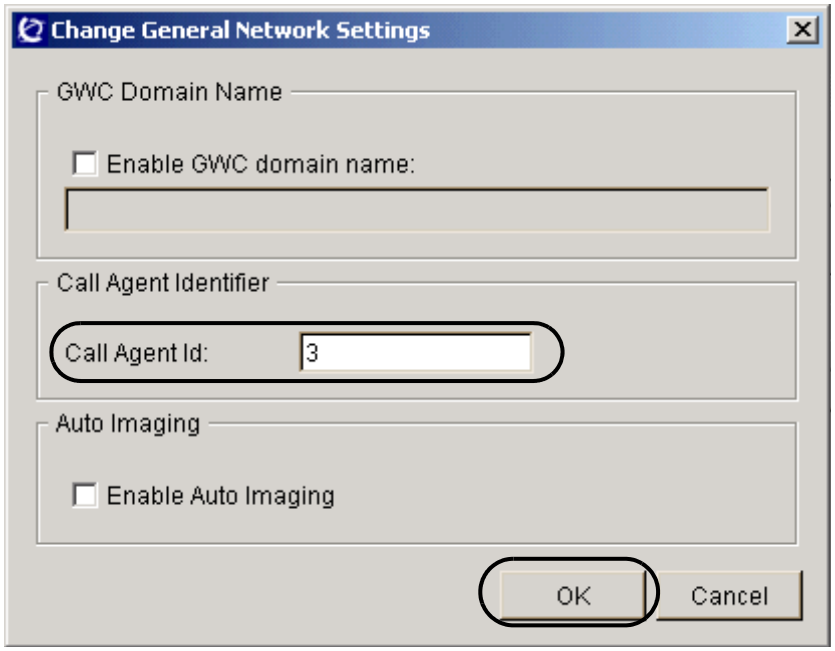
The range of valid values is between 1 and 255 inclusive. Contact your site system administrator to determine the call agent ID you should be using.

***Note 1:*** If the value typed is invalid, the text field is outlined in red and the OK button is disabled. If this happens, simply type a valid value in the field.

***Note 2:*** The system does not check for call agent IDs that are already used in your network. Ensure that the call

agent ID you are assigning is not already used by another CS 2000.

**c** Click the **OK** button.




The first time the Call Agent ID is set, the system automatically updates NAT middleboxes which have already been provisioned to incorporate the newly provisioned call agent ID into the NAT middlebox IDs. GWC units which need to be synchronized to this new data will be identified by having data synchronization alarms raised against them.

**d** Go to step 6.

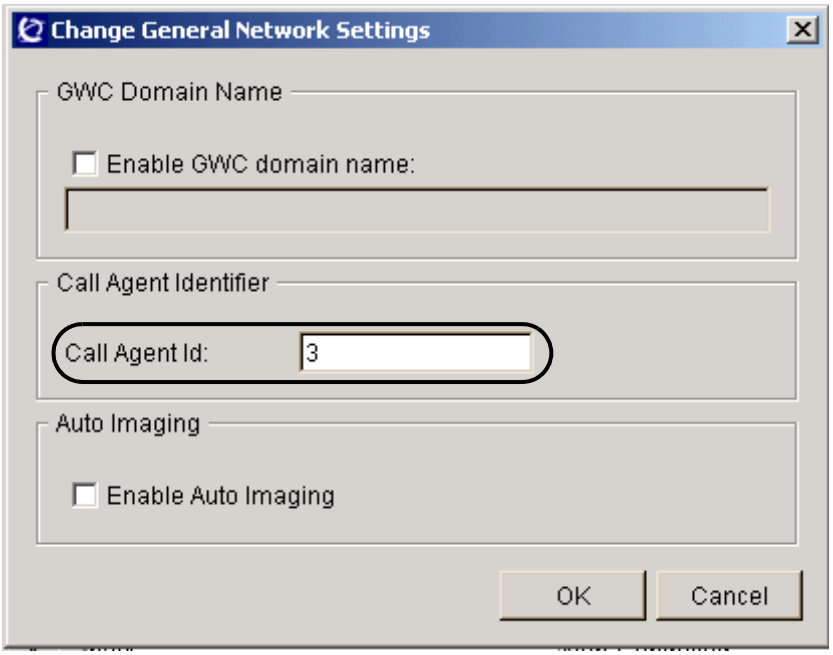
**5**

**CAUTION**

Changing the call agent ID will make it more difficult to rollback (downgrade) your GWC cards to an earlier software load.

Perform the following steps to change the call agent ID:

**a** Click the **Change** button at the bottom of the network screen to display the Change General Network Settings window.




**b** Click in the Call Agent id field and assign a new call agent ID.

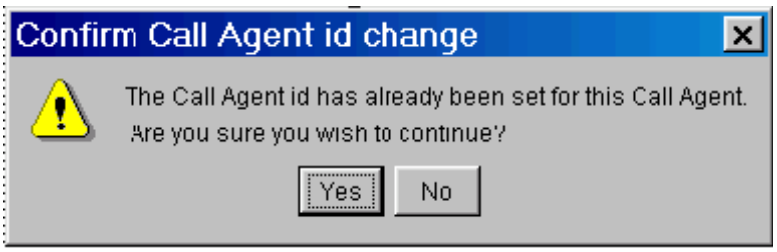
The range of valid values is between 1 and 255 inclusive. Contact your site system administrator to determine the call agent ID you should be using.

***Note 1:*** If the value typed is invalid, the text field is outlined in red and the OK button is disabled. If this happens, simply type a valid value in the field.

***Note 2:*** The system does not check for call agent IDs that are already used in your network. Ensure that the call agent ID you are assigning is not already used by another CS 2000.

**c** Click the **OK** button.

When changing the call agent id for a CS 2000, the system displays the following message:



**d** Click **Yes** to continue with the change.

The new Call Agent ID will only be used in the middlebox ID for NATs provisioned after the change has been made. The middlebox IDs of previously provisioned NATs are not modified. This ensures consistency, in case some NATs have been provisioned into more than one CS 2000.

**6** The procedure is complete.

# Preparing to upgrade the USP

Complete the procedures in this section before you install a new GUI and begin a software upgrade.

## Pre-upgrade check

Before beginning upgrade procedures, complete this check from your alternate boot server to make sure your system is running in a predictable, stable manner. If you are upgrading from USP8.0, perform all the steps in the following procedure. If you are upgrading from USP9.0, begin at step 2.

**Procedure 1 Verifying that your system is running**

***At the OAMP workstation***

1. Record the list of site names and their RTC IP addresses.
   - **a** Open the USP8.0 GUI (double-click the desktop icon).
   - **b** Click **Configure**.
   - **c** Record the list of site names and their RTC IP addresses. This information will be entered into the Java GUI.
2. Log in to the USP.
3. Make sure that all system nodes are in-service or offline, and unlocked. To do this, perform the step below for the version from which you are upgrading.
   - If you are upgrading from USP8.0, click **System Mgmt** on the main menu and click the shelf icon. The Shelf_name window appears. Verify that the LED icons for each in-service system node are green and each offline node are yellow.

     ***Note:*** If your system contains multiple shelves, repeat the above check for each shelf. To return to the Shelf_name window, click on the **Close** button.

   - If you are upgrading from USP9.0, click **Configuration>platform>node**. Click **Graphical View**.
4. Take corrective action to clear all outstanding alarms.
5. Verify that there are not more than 16 paths on any IPS7 card. If your system does have cards with more that 16 paths you must redistribute them among the system nodes. See the section Configuring ASP Paths in the Configuration guide for more information on how to perform this procedure.

6 Take a snapshot of the running configuration. Use your File Manager to copy it to the alternate boot server, and update your alternate boot snapshot. See Create and change the alternate boot data snapshot on USP9.0 or USP10.0 on page 365.

7 Perform test calls and verify the calls complete successfully.

8 Open the inactive RTC system node provisioning and maintenance window. To do this, click System Mgmt on the main menu to open the System Configuration window, click the icon for the control Communications Applications Module (CAM) shelf to open the shelf_name window, and click the icon for the inactive RTC system node.

9 Check the RTC to see if it is locked.

| If: | Do: |
|---|---|
| the RTC system node is locked | proceed to the next step. |
| the RTC system node is unlocked | click **Lock** in the Maintenance portion of the window and proceed to the next step. |

10 Click **Load** to download the RTC system node boot image and re-initialize the RTC system node.

11 When the initialization of the inactive RTC system node is complete, click **unlock** to unlock the RTC.

12 Click **SWACT** to make the inactive RTC system node Active.

13 Repeat steps step 8 to step 12 for the other RTC.

14 Make sure that the RTC system node in slot 12 (RTC12) is the active RTC system node. If not, click **SWACT** to make RTC12 the active system node.

## Create and change the alternate boot data snapshot on USP8.0

For USP 8.0, change the alternate boot data snapshot for your system when you have made significant system configuration changes.

After the changes have been made, you should create a new data snapshot, copy the data snapshot to your OAMP workstation, and change the alternate boot data snapshot for your site.

To change the alternate boot data snapshot on a USP 8.0 system, perform the following steps:

### Procedure 2 Creating and changing the snapshot for USP8.0

***At the OAMP 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 size and activity. The Snapshot Successful dialog box appears when the backup is complete, click ok to close. The Backup Status box indicates that 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.

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

6 Open the File Manager window. To do this, return to the Administration window and click File Manager. To access the file manager function, you must be working from the OAMP workstation configured as the alternate boot server.

7 The left side of the screen displays the files present on the Alternate Boot Server (ABS). The right side of the screen displays files present on the selected rtc displayed in the drop box. For example, to view files on rtc-15, select rtc-15 from the drop-box on the top of the right screen.

8 Select the active RTC system node from the drop-box.

9 Open the snapshot folder.

10 Open the folder corresponding to the version of the USP software that you are running.

11 Select the snapshot file you want to copy. When you select a file, its description is displayed in the Description box.

12 Copy the snapshot to the ABS by clicking **<-**. An hourglass appears while the data snapshot is copied. The folders in ABS portion of the window are 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, depending on system activity, to copy from an RTC system node to your alternate boot server.

13 Select **Administration>ABS Settings**.

14 Select the data snapshot from the Alt. Boot Data Snapshot list. Once the snapshot is selected, the window displays the Description.

15 Click **OK** or **Apply** to save the change. If you click OK, the window closes.

## Create and change the alternate boot data snapshot on USP9.0 or USP10.0

For USP9.0 or 10.0, change the alternate boot data snapshot for your system when you have made significant system configuration changes.

After the changes have been made, you should create a new data snapshot, copy the data snapshot to your OAMP workstation, and change the alternate boot data snapshot for your site.

To change the alternate boot data snapshot on a USP9.0 or 10.0 system, perform the following steps:

**Procedure 3 Creating and changing the data snapshot for USP9.0 or USP10.0**

***At the OAMP workstation***

1 Click **Administration>backup**.

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

3 Click the corresponding checkboxes to activate the following options, as appropriate:

- transfer snapshot to alternate boot server

  ***Note:*** Nortel Networks recommends that you enable this option. If you don't select this option, a warning dialog box will appear; select yes to continue.

- set as active snapshot on alternate boot server

  ***Note:*** Nortel Networks recommends that you enable this option. If you don't select this option, a warning dialog box will appear; select yes to continue.

- delete oldest snapshot on alternate boot server if maximum reached (16)
- delete oldest snapshot on rtc if maximum reached (5)

4 Click **Create** to create the data snapshot.

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

6 If you selected transfer snapshot to alt boot server, go to step 12.

7 Click **Administration>File Manager**.

8 Select the active RTC system node from the **Destination** list in the right window pane.

9 Select the new data snapshot from the **Snapshot** box in the **Destination** portion of the window. Make note of the timestamp of the data snapshot.

10 Copy the snapshot to your alternate boot server by clicking **<-**. An hourglass appears while the snapshot is copied. The boxes in the Source portion of the window will be updated with the information for the copied snapshot when the copy operation is complete.

***Note:*** These files are large and can take several minutes to copy.

11 When the file is transferred, click **Close.**

12 Update the Alternate Boot Data Snapshot using the ABS Settings window:

- Open the Alternate Boot Server (ABS) Configuration Manager window by Clicking **Administration> alternate-boot-server**.
- Select an alternate snapshot by clicking the arrow button.
- Click **Modify** to save your changes and close the window.

13 Your backup is complete.

# Preparing to upgrade CS 2000 Compact

Perform the following procedures when the upgrade software media is delivered, approximately 35 days before the ONP, to verify office stability and prepare the office for an upgrade.

Review Site preparation overview before performing the procedures in this section. Be sure to understand SITE preparation responsibilities before the ONP and that a current office image must be taken within 24 hours of the ONP.

### Site preparation phase

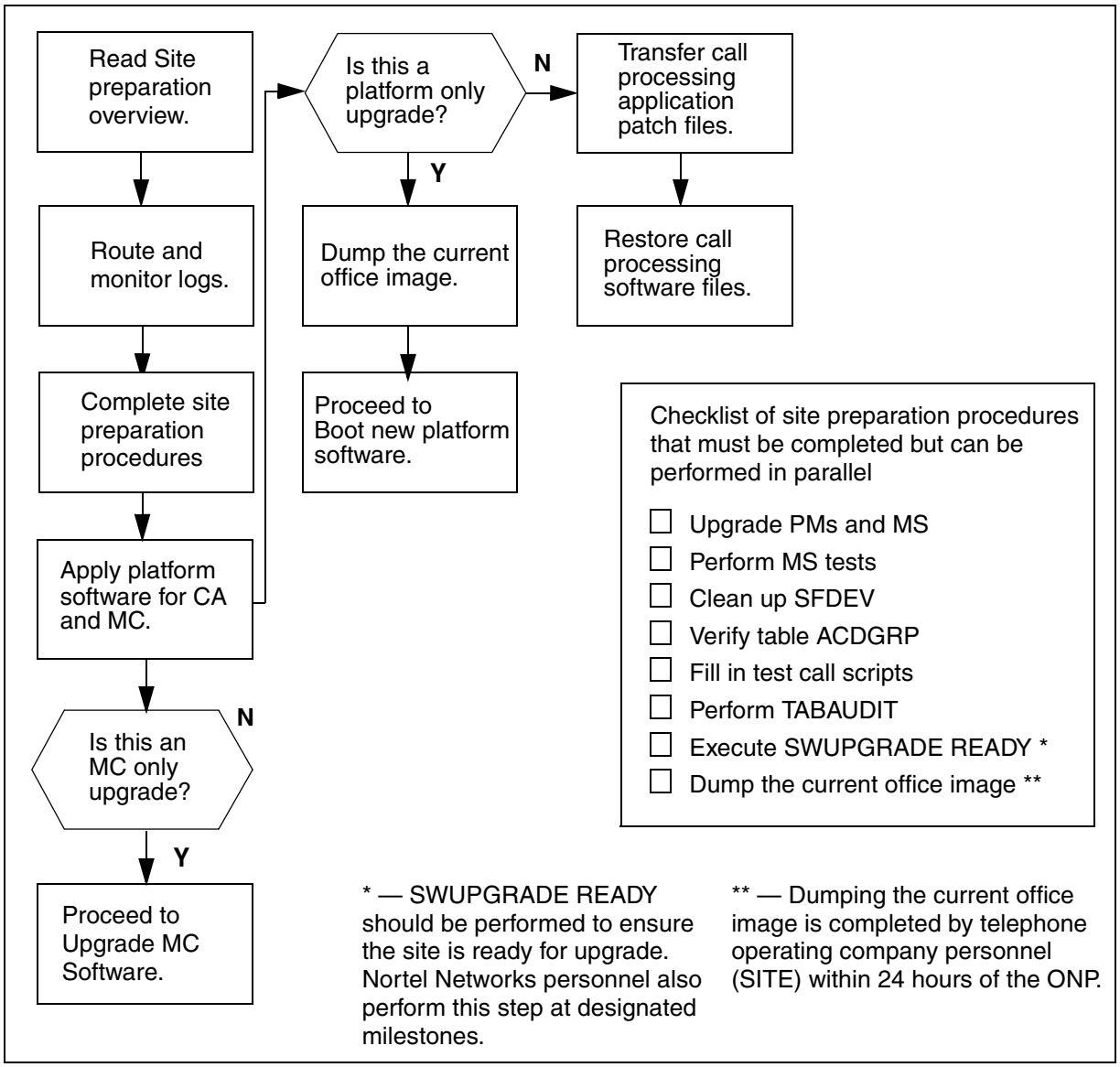


Table , Process timeline indicates the timing of events that need to be completed by telephone operating company personnel for an ONP. This timeline does not apply to platform only MR upgrades or Message Controller only upgrades.

**Process timeline**

| Days before the upgrade | Site preparation activity |
|---|---|
| 45 days | Site delivery checklist and acceptance of schedule arrives at site |
| 35 days | • first software media and documentation shipment arrives at site<br>• site begins checking logs daily, refer to Route and monitor logs on page 372<br>• begin upgrading and verifying PMs and other network components with the latest software loads, refer to Upgrade Peripheral Modules and Message Switch on page 373 |
| 30 days | Begin data consistency checks, refer to Perform TABAUDIT on page 408 |
| 15 days | Ensure that scheduled RExTsts complete successfully |
| 7-4 days | • ensure SFDEV is clear, refer to Clean up SFDEV on page 402<br>• continue to monitor logs<br>• if office is equipped with PMs, ensure that the latest PM loads and XPM patch files are restored to the proper disk volumes<br>• site receives final shipment of software media and documentation |
| 6 days | • verify all network nodes are loaded, patched, and working<br>• verify dial in connectivity, refer to Remote site access on page 1136<br>• ensure all software media are on site<br>• verify that site personnel are familiar with the upgrade process |

**Process timeline**

| Days before the upgrade | Site preparation activity |
|---|---|
| 5 days | The final site readiness check is performed by Nortel Networks personnel. Nortel Networks Software Delivery Engineer dials in an runs Execute SWUPGRADE READY on page 412. |
| 3-2 days | • verify site personnel has prepared test calls plan<br>• obtain name of site personnel representative with the authority to decide in case of an abort with the CANCEL command<br>• verify patches for the new software load are downloaded to the site<br>• ensure all site preparation checklist items are complete |
| Day of upgrade | Refer to Site responsibilities the day of the software delivery on page 1131. |
| Night of upgrade | Refer to SWUPGRADE on page 1140. |

# Site preparation overview

## Planning activities



**CAUTION**
**Possible service interruption**
Application of the following patch types within 30 days of the ONP must be considered a gating issue to the ONP:

Active (ACT) patch applied and activated

Limited (LTD) status patch

Verification (VO) status patch

If any of the above patches are applied to the office within 30 days of the ONP, immediately contact your Nortel Networks regional customer representative or call the Global Software Delivery Hotline for your market.

A successful software delivery application will require certain activities to be performed before the ONP. Some of these activities will depend on factors such as office type and the PCL software being delivered. This section provides a brief overview of the site preparation activities that must take place before the ONP. Other required activities not listed in this section must be approved by and coordinated through the appropriate Nortel Networks customer representatives. The following information: administrative, warnings, and software delivery data services should be reviewed by office personnel as soon as this document is received.

## Pre-application activities

Pre-application activities include upgrading all peripherals (including remotes) to PM loads compatible with the new PCL software load. In addition, Network (ENET) and Message Switch (MS) software upgrades must be completed before the ONP.

Pre-application activities can include (but are not restricted to) the following:

- First shipment of ONP CD-ROMs and documentation to the site
- Site polling by Nortel Networks to obtain specific switch information
- Site preparation procedures

- TABAUDIT procedure
- Final shipment of ONP CDROMs and documentation to site
- Pre-loading the message switch
- Site ready checks
- Site responsibilities the day of the software delivery application

Some of the above activities will be completed by Nortel Networks personnel and some will be completed by the operating company. Site personnel responsible for completing pre-application activities should become familiar with all sections of this document.

## Route and monitor logs

### *SITE — At the ACTIVECM window*

1 Determine if log reports are suppressed.

```
> LOGUTIL; LISTREPS SPECIAL
```

2 If CA or MM log reports are suppressed, remove the suppression.

```
> RESUME log_type
```

**log_type**
is CA, MM, MS, SYSLOG, or ISYSLOG

3 If CA or MM log reports have a threshold set, remove the threshold.

```
> THRESHOLD 0 log_type
```

4 Route the logs to a printer device.

```
> LISTROUTE DEVICE printer
> ADDREP printer log_type
```

**printer**
is a terminal type device like TELNSVR00003

5 Start the printer device.

```
> STOPDEV printer
> STARTDEV printer
> LEAVE
```

### *SDE — At the ACTIVECM window*

6 Enter the BCS update level.

```
> BCSUPDATE
```

7 Check the logs.

```
> LOGCHECK
```

8

**ATTENTION**
Do not proceed until all log activity is explained.

This procedure is complete.

# Upgrade Peripheral Modules and Message Switch

**ATTENTION**
Only perform this procedure if the office is configured with an MS and legacy Peripheral Modules (PM).

**ATTENTION**
This is the first shipment of software and arrives approximately 35 days before the ONP.

Do not perform the following procedure if this is a platform only upgrade (MNCL).

The examples provided in this procedure show how to get the MS and the call processing application images, but this procedure also applies to PM loads and cutover tools necessary to upgrade a TDM to Hybrid solution.

If this procedure is not needed, go to Apply platform software for Call Agent and Message Controller on page 377.

Upgrade of the call processing application on the Call Agent requires an upgrade of all network elements in the Succession network and all element managers before an upgrade of the Call Agent. Refer to *Solutions Upgrades*, NN10261-450 or NN10344-450 for changes in this policy and the upgrade order.

Do not proceed with the Call Agent upgrade unless all other network elements and element managers have been upgraded or *Solutions Upgrades*, NN10261-450 or NN10344-450 indicates which network elements and element managers can be upgraded after the Call Agent.

If the CS 2000 - Compact is equipped with Message Controller cards, the Message Switch, Enhanced Network, and any Peripheral Modules must be upgraded before the Call Agent. Refer to the *Peripheral Module Release Document*, 297-9051-599 (EMEA) or 297-2663-599 (NA). Upgrade of the Message Controllers is completed during step SWUPGRADE in this document.

Because the CS 2000 - Compact does not have a tape drive, software loads delivered for TDM peripherals are shipped on CDROM.

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

**1** Insert the DVD or CDROM in the CDROM tray.

***SITE — At the CORE0 or CORE1 window***

**2** Exit the Call Agent Manager:

```
> 0 all
```

*The operating system prompt is returned.*

```
[mtc@hostname mtc]$
```

**3** Change directory to the destination directory for the peripheral module (PM) loads:

```
> cd /3PC/<sd0x>/<pm_loads_location>
```

**Example**
**> cd /3PC/sd00/pmloads**

**4** Open an FTP session to the CS 2000 Management Tools server and log in:

```
> ftp <cs_2000_mgmt_tools_ip>
```

***Note:*** Log in to the CS 2000 Management Tools server as a user with privilege to change directory and transfer files with FTP.

**Example**

```
[mtc@10.40.44.67 image0]$ ftp <cs_2000_mgmt_tools_ip>
Connected to <cs_2000_mgmt_tools_ip>.
220 ProFTPD 1.2.8 Server (Authorized Use Only) [hostname]
Name (hostname:mtc): maint
331 Password required for maint.
Password:
230 User maint logged in.
ftp>
```

**5** Change directory, list the file size, change the mode to binary, and get the file:

```
ftp> cd /cdrom/cdrom0
ftp> ls
ftp> bin
ftp> prompt
ftp> mget *
```

***Note:*** Do not transfer a file with a name longer than 32 characters.

**Example FTP session of getting PMLOADS**

```
ftp> cd /cdrom/cdrom0
250 CWD command successful.
ftp> ls
ERS20CE.img1020
ENX20CE.img1020
...
LRS20CE.img1020
MPF20CE.bin128
QLI20BT.img1020
ftp> bin
200 Type set to I.
ftp> prompt
Interactive mode off.
ftp> mget *
local:
200 PORT command successful.
150 Opening data connection for ERS20CE.img1020 (binary mode)(5107140 bytes)
226 Transfer complete.
150 Opening data connection for ENX20CE.img1020 (binary mode)(3913740 bytes)
226 Transfer complete.
...
```

6 End the FTP session by typing bye:

```
ftp> bye
```

***At the ACTIVECM window***

7 Enter the DISKUT level and import the upgrade PM loads:

```
> DISKUT
> IMPORT SD00PMLOADS
```

**Example IMPORT of PM loads**

```
DISKUT:
>IMPORT SD00PMLOADS

Attempting to import 24 files selected on SD00PMLOADS.

Imported ERS20CE.img1020 as ERS20CE  IMAGE 1020.
Imported ENX20CE.img1020 as ENX20CE  IMAGE 1020.
...
Imported MPF20CE.bin128 as MPF20CE  BIN 128.
Imported QLI20BT.img1020 as QLI20BT  IMAGE 1020.

Imported 24 files successfully of 24 attempts on SD00PMLOADS.
```

*The PM load files are imported from the native file system into the call processing application file system. If the disk does not have enough space, a prompt to increase the volume size is presented.*

**8** This procedure is complete.

***SITE — At a CS 2000 Management Tools terminal***

**9** Issue the eject command to open the CDROM tray:

```
# eject
```

*Software on the CS 2000 Management Tools server unmounts the DVD and opens the CDROM tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session is ended and no users have changed directory into /cdrom/... directory. Re-enter the eject command.*

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

**10** Remove the DVD from the CDROM tray.

**11** This procedure is complete.

# Apply platform software for Call Agent and Message Controller

Complete this procedure at least two days before the ONP.

This procedure installs the Call Agent platform software, `ncgl_cca_image_5.x.y.z`, and the Message Controller software, `ncgl_mc_image_5.x.y.z` onto the CS 2000 Core Manager or the Core and Billing Manager (CBM). The Message Controller software is installed even if the office is not configured with Message Controller cards. If the office is not configured with a CS 2000 Core Manager or a CBM, this procedure installs the software on `/data/swd/3pc` of the CS 2000 Management Tools server.

For offices without a CS 2000 Core Manager or a CBM, manual action is required. Refer to Offices without a CS 2000 Core Manager or CBM on page 386.

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

**1** Insert the CDROM in the CDROM tray.

***SITE — At a CS 2000 Management Tools terminal***

**2** Log in and then use the su command to gain root privilege.

```
Trying <hostname>...
Connected to <hostname>.
Escape character is '^]'.

Authorized use only, activities logged.
login: username
Password: <password>
Last login: Fri Jan 30 12:48:10 from <otherhost>
prompt:>
prompt:> su - root
Password: <root_password>
#
```

**3** Execute the platform_load_install.sh script.

```
# /opt/nortel/sspfs/Scripts/platform_load_install.sh
```

*The screen clears and a menu is displayed.*

```
      Welcome to the Platform Installation Tool Version 3.2
   ==================================================================
      RPM INSTALLATION/REMOVAL
     ============================
     1) Install RPM from CDROM       2) Install RPM from Disk
     3) Uninstall RPM                4) Query all RPMs

      OTHER
     =========
    C) Change Rotation Parameters          P) View Rotation Parameters
     V) SAM21 Platform Version Installed     X) Exit

      Please choose one of the following: 1
```

**4** Enter **1** and press the Return key to install the software.

*The screen clears and the contents of the .rpm package are displayed.*

```
                Verifying CDROM is mounted
/cdrom/cdrom on /vol/dev/dsk/c0t0d0/cdrom read only/nosuid/mapl-
case/noglobal/rr/traildot/dev=16c0001 on Sat Mar 27 16:34:13 2004
                CDROM is mounted.
                Listing file names in the rpm on the cd.

/swd/3pc/ncgl_cca_5.32.1.0
/swd/3pc/ncgl_mc_5.32.1.0

                Do you want to continue (y/n)? Y
```

***Note:*** *If the message* `There is no cd in the CDROM drive, please check drive` *is displayed, ensure that the CDROM is inserted in the tray for this unit.*

**5** Enter **Y** to proceed with the software installation.

*The software is extracted from the .rpm package. The .rpm package is transferred to the CS 2000 Core Manager or CBM.*

```
              Extracting files from the rpm archive on the cd.

Installing RPM package ncgl_cca_mc_image-5.32-1.0.noarch.rpm
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
ncgl_cca_mc_image-5.32-1.0.noarch.rpm       100%   11MB 750.4KB/s   00:14
root@47.135.214.127's password: <enter root password>
```

6 Enter the root password for the CS 2000 Core Manager or CBM.

*The software is installed on the CS 2000 Core Manager or CBM. If a CBM is used, the .rpm package is then copied to the inactive CBM unit and another prompt for the root password appears. If this happens, enter the root password and press Return. After the load file is installed on the CS 2000 Core Manager or CBM, the transferred .rpm package is deleted from the CS 2000 Core Manager or CBM.*

```
              Extracting files from the rpm archive on the cd.

Installing RPM package ncgl_cca_mc_image-5.32-1.0
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
ncgl_cca_mc_image-5.32-1.0.noarch.rpm      100%   11MB 750.4KB/s   00:14
root@47.135.214.127's password: <enter root password>
Mate IP is 47.135.214.129
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
root@47.135.214.129's password: <enter root password>

      ******* Please hit ENTER key to continue ***********
```

7 A script is run to verify connectivity to the ACTIVEIRM IP address (the call processing application) and to verify hostname aliases. The output depends on whether the office is configured with a CS 2000 Core Manager or a CBM. Refer to Additional information on page 380 for examples.

8 Issue the eject command to open the CDROM tray:

```
# eject
```

*Software on the CS 2000 Management Tools server unmounts the CDROM and opens the CDROM tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session is ended and no users have changed directory into /cdrom/... directory. Reenter the eject command.*

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

9 Remove the CDROM from the CDROM tray.

**10** This procedure is complete.

| If | Do |
|---|---|
| this is a platform only upgrade | Dump call processing application image on page 419 |
| otherwise | Transfer call processing application patch files on page 393 |

## Additional information

After applying the platform software, the installation process invokes the `/swd/3pc/bin/user_config.sh` script to verify or set:

- the configuration of the PassThru feature on the CS 2000 Core Manager or CBM
- hostname aliases core, core0, and core1
- NFS sharing of the Call Agent platform software load

The installation process asks if the ncgl_cca_image software is for CA (Call Agent) or HMEM (Home Location Registry Memory).

The CS 2000 Core Manager or CBM software provides a prompt to determine if the fileset is for a CA or HMEM application.

Enter **CA** and press the Enter key.

```
Is this a CA or HMEM application? [CA/HMEM] CA: CA
```

A check is made to determine if aliases core, core0, and core1, as well as PassThru accounts cmusr, core0usr, and core1usr exist. The response is determined by the current configuration.

## New installation on Core Business Manager

The software prompts for the ACTIVEIRM IP address, adds the host aliases to the `/etc/hosts` file, and creates the PassThru users on both CBM units.

### New installation on CBM

```
Is this a CA or HMEM application ? [CA/HMEM] CA : CA
Checking for existing core alias...
----------------------------------
hostmtc: Hostname or IP address is not in the hosts database: 'core'.


No existing alias from core found

Cleaning up any alias for core0 core1 and any related passthru accounts,
 if found.

Enter the ACTIVEIRM IP ADDRESS (e.g. 172.16.16.72 ) or q : 10.40.64.72

Adding aliases...
-----------------
10.40.64.72~core~~
10.40.64.67~core0~~
10.40.64.70~core1~~

Configuring Passthru Users ...
------------------------------

Creating Passthru accounts...
Creating passthru user cmusr
Creating passthru user core0usr
Creating passthru user core1usr


Sharing NFS mount For CCA Access of /swd/3pc ...
----------------------------------------
NFS mount /swd/3pc successfully shared.
```

### Upgrade on CBM

In an upgrade on the CBM, the software always prompts to confirm the ACTIVEIRM IP address, always removes the core, core0, and core1 aliases, and always adds them back to the `/etc/hosts` file.

**Upgrade on CBM**

```
Is this a CA or HMEM application ? [CA/HMEM] CA : CA
Checking for existing core alias...
-----------------------------------
10.40.64.72~core~~
Please confirm ACTIVE IRM IP address is [10.40.64.72] (yes/no):YES

Temporarily removing alias from /etc/hosts for core core0 core1
and related passthru accounts, while performing network engineering
validation.

Adding aliases...
-----------------
10.40.64.72~core~~
10.40.64.67~core0~~
10.40.64.70~core1~~

Configuring Passthru Users ...
------------------------------

Creating Passthru accounts...
Creating passthru user cmusr
Creating passthru user core0usr
Creating passthru user core1usr

Sharing NFS mount For CCA Access of /swd/3pc ...
-----------------------------------------
NFS mount /swd/3pc successfully shared.
```

### New installation on CS 2000 Core Manager

For a new installation, the software prompts for the ACTIVEIRM IP address. This information is available from the Nortel Networks

Installation Services engineer, or documentation provided by Nortel Networks Installation Services

### New installation on CS 2000 Core Manager

```
Checking for existing aliases...
--------------------------------
hostmtc:Hostname or IP address is not in the hosts database:‘core’.
hostmtc:Hostname or IP address is not in the hosts database:’core0’.
hostmtc:Hostname or IP address is not in the hosts database:’core1’.

Checking for existing passthru accounts...
------------------------------------------
passthru:Undefined passthru user cmuser.
passthru:Undefined passthru user core0usr.
passthru:Undefined passthru user core1usr.

Enter the ACTIVEIRM IP ADDRESS (e.g. 172.16.16.72) or q: 10.40.24.80
Do you wish to proceed? [y/n] y: Y

Checking for existing IP in hosts database.
-------------------------------------------
hostmtc:Hostname or IP address is not in the hosts database:’10.40.24.80’
hostmtc:Hostname or IP address is not in the hosts database:’10.40.24.75’
hostmtc:Hostname or IP address is not in the hosts database:’10.40.24.78’

Adding aliases...
-----------------
10.40.24.80:core::
10.40.24.75:core0::
10.40.24.78:core1::

Adding passthru accounts...
---------------------------
cmuser::221:202,passthru:CA SOS Image:/sdmtools/bin/cm_screener:
  /home/cmuser::telnet:core
core0usr::222:202,passthru:CA Unit 0:/sdmtools/bin/cm_screener:
  /home/core0usr::telnet:core0
core1usr::223:202,passthru:CA Unit 1:/sdmtools/bin/cm_screener:
  /home/core1usr::telnet:core1

exporting NFS mount /swd/3pc...
-------------------------------
Mount already exported to core*.
```

The aliases and PassThru accounts are created. The status information about installation in the figure above does not remain on the screen very long since the installation software clears the screen once the configuration is complete. Please read Important password information.

### Upgrade with correct configuration on CS 2000 Core Manager

In SN05, the cmusr, core0usr, and core1usr accounts were not true PassThru accounts on the CS 2000 Core Manager. These accounts were maint accounts with a profile that launched a telnet session to the destination host. If the configuration information (hostname aliases and user accounts) is available on the CS 2000 Core Manager, then that information is deleted from the CS 2000 Core Manager and reconfigured as true PassThru accounts. Please read Important password information.

**Upgrade with correct configuration on CS 2000 Core Manager**

```
Checking for existing aliases...
--------------------------------
10.40.24.80:core:cm CLLI:Core's IPNETWRK IP Address
10.40.24.75:core0::
10.40.24.78:core1::

Checking for existing passthru accounts...
------------------------------------------
passthru:Undefined passthru user cmuser.
passthru:Undefined passthru user core0usr.
passthru:Undefined passthru user core1usr.

Adding passthru accounts...
---------------------------
cmuser::221:202,passthru:CA SOS Image:/sdmtools/bin/cm_screener:
  /home/cmuser::telnet:core
core0usr::222:202,passthru:CA Unit 0:/sdmtools/bin/cm_screener:
  /home/core0usr::telnet:core0
core1usr::223:202,passthru:CA Unit 1:/sdmtools/bin/cm_screener:
  /home/core1usr::telnet:core1

exporting NFS mount /swd/3pc...
-------------------------------
Mount already exported to core*.
```

***Note:*** Long lines in the display were wrapped.

### Upgrade with incorrect configuration on CS 2000 Core Manager

The SN05 accounts were not true PassThru accounts. If all the necessary information (hostname aliases and user accounts) is not complete on the CS 2000 Core Manager, the fileset application software does not perform any configuration or deletion of data.

Instruction for deleting the existing configuration and reconfiguring the fileset is provided. Once the information is deleted and the reconfiguration is started, the display is similar to New installation on

CS 2000 Core Manager. Please also read Important password information.

**Upgrade when old configuration was incorrect on CS 2000 Core Manager**

```
Checking for existing aliases...
--------------------------------
10.40.24.80:core:cm CLLI:Core's IPNETWRK IP Address
10.40.24.75:core0::
hostmtc:Hostname or IP address is not in the hosts database:'core1'.

Checking for existing passthru accounts...
------------------------------------------
cmusr::221:202,passthru:CA SOS Image:/sdmtools/bin/cm_screener:
  /home/cmuser::telnet:core
core0usr::222:202,passthru:CA Unit 0:/sdmtools/bin/cm_screener:
  /home/core0usr::telnet:core0
core1usr::223:202,passthru:CA Unit 1:/sdmtools/bin/cm_screener:
  /home/core1usr::telnet:core1

There is a partial list of aliases and/or passthru accounts.
THE 3PC APPLICATION WILL NOT BE CONFIGURED.
To configure the 3PC application, please carry out the following steps.

1. From the sdmmtc;nodes level, delete the entries core, core0, core1.
2. Delete the entries cmusr, core0usr, core1usr from either the
   sdmmtc;passthru level or the sdmmtc;user level. These entries could
   exist in either of these levels.
3. From the sdmmtc;config level run config <fileset name>.
```

***Note:*** Long lines in the display were wrapped.

### Important password information

For new installations, PassThru accounts are created. For upgrades from SN05 with correct configuration the old style cmuser, core0user, and core1usr accounts are deleted and then reconfigured as true PassThru accounts. For upgrades without correct configuration data, no changes are made to the existing setup; manual deletion of accounts and reconfiguration of the fileset is required to create the PassThru accounts.

These new PassThru accounts are created without passwords. In this configuration, users log in to the CS 2000 Core Manager or CBM with a username of cmusr, core0usr, or core1usr, and are immediately forwarded to a destination host. The destination host provides a login with password authentication. If password authentication is preferred on the CS 2000 Core Manager or CBM, in addition to the destination host, then reconfigure the accounts at the passthru level of sdmmtc or cbmmtc.

### Offices without a CS 2000 Core Manager or CBM

Offices without a CS 2000 Core Manager or a CBM require manual action to ensure that load delivery is complete. Failure to perform these actions may result in a “no boot” situation. Two tests are available to determine this situation:

- The CS 2000 Management Tools server boots the cards in the SAM21 shelf. This is indicated at the CS 2000 SAM21 Manager client if the SAM21 EM Server IP value at the Reprovisioning window is also the value for Server IP on the same window.
- If the command **echo $SDM_IP** returns a blank line from a command prompt at the CS 2000 Management Tools server.

#### Required actions for offices without a CS 2000 Core Manager or CBM

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

**1** Become the superuser with the **su - root** command and enter the root password when prompted.

**2** View the /etc/hosts file:

```
# cat /etc/hosts
```

**3** If values for `core`, `core0`, and `core1` are not listed, enter them in the file.

- `core` is the same IP address as the ACTIVEIRM IP address. For example, 172.16.16.72.
- `core0` is the same as the `core` value, but the last octet is 5 less than the last octet of the `core` value. For example, 172.16.16.67.
- `core1` is the same as the `core` value, but the last octet is 2 less than the last octet of the `core` value. For example, 172.16.16.70.

Make a backup copy of the /etc/hosts file:

```
# cp /etc/hosts /etc/hosts.bak
```

Enter the values with the vi editor, the dtpad graphical editor, or appending the lines to the end of the file:

```
# echo “172.16.16.72 core” >> /etc/hosts
# echo “172.16.16.67 core0” >> /etc/hosts
# echo “172.16.16.70 core1” >> /etc/hosts
```

4 Edit the /etc/dfs/dfstab file to allow the /data/swd/3pc directory to be shared on the network:

```
# echo "#Begin CCA NFS Configuration" >>
/etc/dfs/dfstab

#  echo "share -F nfs -o rw=core0:core1
/data/swd/3pc" >> /etc/dfs/dfstab

# echo "#End CCA NFS Configuration" >>
/etc/dfs/dfstab
```

5 View the file to ensure the changes are correct:

```
# cat /etc/dfs/dfstab
```

*Ensure that the end of the file resembles the following output.*

```
...
#Begin CCA NFS Configuration
share -F nfs -o rw=core0:core1 /data/swd/3pc
#End CCA NFS Configuration
```

6 Enable the sharing:

```
# /usr/sbin/shareall
```

7 This procedure is complete.

# Electronic Software Delivery (ESD) for Call Agent

Both the PCL and NCL software loads for the Call Agent are available for electronic transfer from Nortel Networks to a customer dropbox. An example of the PCL is CSNN07BG, and an example of the NCL is ncgl_cca_image_5.33.1.0.

**ATTENTION**
This procedure applies only to the following loads: CM Core, CCA LINUX, and MC.

## Audience

This procedure is intended for telephone operating company personnel who have an ESD agreement with Nortel Networks. When the agreement was established, the operating company furnished Nortel Networks with the location of an electronic dropbox and a username and password pair for delivering software loads. When Nortel Networks delivers a software load to the dropbox, an electronic mail notification is sent to the E-mail address specified by the telephone operating company when the ESD agreement was established.

## When to use this procedure

Use this procedure after receiving electronic notification for the following software loads:

- PCL
  - SNC0000n.n.R.PCL.PPC3.vault.nn.D.tar.gz for North America
  - SWC0000n.n.R.PCL.PPC.vault.nn.D.tar.gz for International
  - SEC0000n.n.R.PCL.PPC3.vault.nn.D.tar.gz for SL-100
  - SDC0000n.n.R.PCL.PPC3.vault.nn.D.tar.gz also for SL-100
- NCL
  - 3PC000n0.n.R.NCL.NAP.vault.nn.D.tar.gz for Standard release
  - 3PC0M0n0.n.R.NCL.NAP.vault.nn.D.tar.gz for Maintenance releases

**n**
is an integer value such as 7 and is part of the product order code

**vault**
is a string that identifies the Nortel Networks software vault that holds the software

**nn**
is an integer value that indicates the repository version of the software

## Action

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

**1** Make a temporary directory to store the ESD software:

```
$ mkdir /data/iso_esd
```

**2** Change directory to the newly created location:

```
$ cd /data/iso_esd
```

**3** Ensure that enough disk space is available for the ESD software. For one PCL and one NCL, 500 MB is recommended.

```
$ 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.*

```
$ df -k /data
Filesystem             kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d20       3082223  144121 2876454     5%    /data
```

2876454 / 1000 = 2876 MB free

**4** Transfer the ESD software files from the dropbox on the repository server. The repository server is the machine owned by the telephone operating company that was selected to be the destination for the ESD software files:

```
$ ftp <repository_server>
```

Log in and change directory to the dropbox location on the repository server.

**5** Change the transfer mode to binary.

```
ftp> bin
```

6 Retrieve the ESD software load:

```
ftp> get <esd_filename>.tar.gz
```

**Example**
**ftp> get 3PC0M070.7.R.NCL.NAP.SDC.1.D.tar.gz**

***Note:*** Determine the actual ESD filename from the Nortel Networks notification, or listing the contents of the dropbox with the **ls** command.

7 Repeat step 6 for all ESD software loads recorded in the notification from Nortel Networks and then end the FTP session:

```
ftp> bye
```

8 Extract the ESD software load from the tape archive format:

```
$ gtar xvzf <esd_filename>.tar.gz
```

**Example**
**$ gtar xvzf 3PC0M070.7.R.NCL.NAP.SDC.1.D.tar.gz**

*The ESD software load is uncompressed, and a new directory named after the ESD software filename is created. The directory name is the name of the ESD filename without the .tar.gz suffix. The contents of the ESD software load are placed in this new directory.*

9 Change directory to the newly created directory:

```
$ cd <esd_filename>
```

**Example**
**$ cd 3PC0M070.7.R.NCL.NAP.SDC.1.D**

10 The remainder of this procedure depends on the ESD file:

| If the ESD file is a | Do |
|---|---|
| PCL | step 11 |
| NCL | step 12 |

11 This step applies to PCL ESD software loads only.

**a** Rename the PCL file from a .bin1020 suffix to a .img1020 suffix:

```
$ mv SNC0007_CM.bin1020 SNC0007_CM.img1020
```

**b** Record the location of the call processing application files, /data/iso_esd/<esd_filename>, such as /data/iso_esd/SNC00007.7.R.PCL.PPC3.SDC.2.D.

c Go to procedure Restore call processing application files on page 395 and specify this location for the call processing application files instead of /cdrom/cdrom0 in step 5. This procedure is complete.

**12** This step and the remainder of the procedure applies to NCL ESD software loads only.

Become the root user:

```
$ su - root
```

*A prompt for the root password is presented. Enter the root password.*

**13** The ESD software is formatted as an ISO 9660 image. Use the mount_iso.ksh script to mount the ISO 9660 image:

```
# /opt/nortel/sspfs/Scripts/mount_iso.ksh mount
/data/iso_esd/<esd_directory>/<iso_image>.img.
tape
```

**Example**
**# mount_iso.ksh mount**
**/data/iso_esd/3PC0M070.7.R.NCL.NAP.SDC.1.D/iso_ncgl_cca-5.33-1.0.img.tape**

***Note:*** A space is required after the word mount and before the word /data.

*A response is printed to the terminal. Use the response to determine if the command was successful:*

**mount_iso.ksh command responses**

| Response | Meaning |
|---|---|
| Is is very important for the user of this command to know that if you mount an iso image. It is a MUST that you unmount an image before removing the image file. If the file is deleted while the OS has it mounted, it can be harmful to the runtime applications on this unit | This response indicates success. |
| Provided full path to ISO image does not exist | Verify the location and name of the ISO 9660 image, such /data/iso_esd/3PC0M070.../...img.tape, and retry. |

**mount_iso.ksh command responses**

| Response | Meaning |
|---|---|
| ISO Image Already Mounted | Enter **mount_iso.ksh umount** to unmount whatever ISO 9660 image is currently mounted, and retry. |
| Error creating the image device location | This response indicates an operating system error with the loopback file driver. Retry the command, and if it fails a second time, contact Nortel Networks support personnel. |
| ERROR MOUNTING <ESD_filename> | This response indicates that either the ISO 9660 file is corrupt, or the `/tmpmnt` directory has been deleted. |

*The contents of the ESD software file are available in directory `/tmpmnt/noarch`.*

**14** To install the software now, list the contents of the `/tmpmnt/noarch` directory (**ls /tmpmnt/noarch**) and record the name of the .rpm file.

Enter the **platform_load_install.sh** command.

Select **2**, Install RPM from Disk.

Enter the .rpm filename when prompted.

Enter /tmpmnt/noarch when prompted for the location of the .rpm file.

**15** To install the software later, copy the contents to a location on the CS 2000 Management Tools server. When installing the software at the later date, proceed as in step 14 except specify the location of the software instead of /tmpmnt.

**16** Unmount the ESD file:

```
# mount_iso.ksh umount
```

**17** This procedure is complete.

# Transfer call processing application patch files

Complete this procedure at least two days before the ONP.

**ATTENTION**
Do not perform this procedure for a platform only upgrade.

Call processing application patch files are delivered electronically through Regional Patch Selector (RPS). Contact Nortel Networks support personnel for information about RPS and call processing application patch files.

***SITE — At a terminal window***

**1** Log in to the CS 2000 Core Manager or CBM as the root user if not already logged in:

```
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

**2** Change directory to the location of the call processing application patch files:

```
# cd <path_to_files>
```

**3** Open an FTP session to the call processing application:

```
# ftp cm
```

**4** Login with a valid username and password.

***Note:*** The user must have FTP privilege and permission to write to SFDEV.

**5** Change directory to the store file device (SFDEV):

```
ftp> cd /SFDEV
```

**6** Set the transfer options:

```
ftp> bin; site lrecl 128
```

**7** Use the put command to transfer the call processing application patch files:

```
ftp> put <patch_file_name>
```

***Note:*** Optionally use the MPUT and PROMPT commands to transfer multiple files. The MPUT command transfers multiple files. The MPUT command accepts wildcard pattern matching characters. The PROMPT command prevents prompting for each file.

**8** This procedure is complete.

# Restore call processing application files

Complete this procedure when the final shipment of software arrives.

**ATTENTION**
Do not perform this procedure for a platform only upgrade.

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

**1** Insert the DVD in the CDROM tray.

***SITE — At the CORE0 or CORE1 window***

**2** Exit the Call Agent Manager:

```
> 0 all
```

*The operating system prompt is returned.*

```
[mtc@hostname mtc]$
```

**3** Change directory to the destination directory for the upgrade call processing application image:

```
> cd /3PC/<sd0x>/<image_file_location>
```

**Example**
**> cd /3PC/sd00/image**

**4** Open an FTP session to the CS 2000 Management Tools server and log in:

```
> ftp <cs_2000_mgmt_tools_ip>
```

***Note:*** Log in to the CS 2000 Management Tools server as a user with privilege to change directory and transfer files with FTP.

**Example**

```
[mtc@10.40.44.67 image0]$ ftp <cs_2000_mgmt_tools_ip>
Connected to <cs_2000_mgmt_tools_ip>.
220 ProFTPD 1.2.8 Server (Authorized Use Only) [hostname]
Name (hostname:mtc): maint
331 Password required for maint.
Password:
230 User maint logged in.
ftp>
```

5 Change directory, list the file size, change the mode to binary, and get the file:

```
ftp> cd /cdrom/cdrom0
ftp> ls
ftp> bin
ftp> prompt
ftp> mget *
```

***Note:*** Do not transfer a file with a name longer than 32 characters.

**Example**

```
ftp> cd /cdrom/cdrom0
250 CWD command successful.
ftp> ls
MUC00020810335_MS.img1020
SNC00007810335_CM.img1020
ftp> bin
200 Type set to I.
ftp> prompt
Interactive mode off.
ftp> mget *
local: SNC00007810335_CM.img1020 remote: SNC00007810335_CM.img1020
200 PORT command successful.
150 Opening data connection for SNC00007810335_CM.img1020 (binary mode)
226 Transfer complete.
150 Opening data connection for MUC00020810335_MS.bin1020 (binary mode)
226 Transfer complete.
```

6 End the FTP session by typing bye:

```
ftp> bye
```

***At the ACTIVECM window***

7 Enter the DISKUT level and import the upgrade call processing application and Message Switch images:

```
> DISKUT
> IMPORT <volume_name>
```

**Example of IMPORTing image files**

```
DISKUT:
>IMPORT SD00IMAGE1

Attempting to import 2 files selected on SD00IMAGE1.

Imported MUC00020810335_MS.img1020 as MUC00020810335_MS  IMAGE 1020.
Imported SNC00007810335_CM.img1020 as SNC00007810335_CM  IMAGE 1020.

Imported 2 files successfully of 2 attempts on SD00IMAGE1.
```

*The call processing application and Message Switch images are imported from the native file system into the call processing application file system. If the disk does not have enough space, a prompt to increase the volume size is presented.*

**8** Use the set boot file command to enter the image in to the ITOC and make it bootable:

```
> ITOCCI
> SBF CM <filename_cm> 15
```

**Example**
**> SBF CM SNC00007547159_CM 15**

*The complete ITOC is printed to the terminal. If an MS image was loaded too, use the SBF MS <image_name> <position> command for the MS image too. If there is no free space in the ITOC use the clear boot file command to remove the oldest entry: CBF CM <image_name>.*

***SITE — At a CS 2000 Management Tools terminal***

**9** Issue the eject command to open the CDROM tray:

```
# eject
```

*Software on the CS 2000 Management Tools server unmounts the DVD and opens the CDROM tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session is ended and no users have changed directory into /cdrom/... directory. Reenter the eject command.*

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

**10** Remove the DVD from the CDROM tray.

**11** This procedure is complete.

# Transfer application image to storage

Complete this procedure at least two days before the ONP.

For an upgrade from SN04, the upgrade call processing application image is transferred to the running call processing application image using FTP.

For an upgrade from SN05, the upgrade call processing application image is transferred to platform storage and then imported to the running call processing application.

## Upgrade from SN05 and newer

Use this procedure if this is an upgrade from SN05 or newer. Do not use this procedure to upgrade to SN05.

***At the CORE0 or CORE1 window***

1 Exit the Call Agent Manager.

```
> 0 all
```

2 Change directory to the destination directory for the upgrade call processing application image.

```
> cd /3PC/<sd0x>/<image_file_location>
```

**Example**
**> cd /3PC/sd00/image**

3 Open an FTP session to the CS 2000 Core Manager and log in.

```
> ftp sdm
```

***Note:*** Log in to the CS 2000 Core Manager as a user with privilege to change directory and transfer files with FTP.

**Example**

```
[mtc@10.40.44.67 image0]$ ftp sdm
Connected to sdm.
220 hostname SFTPD Server (Version 18.10.0.0 Mar  8 2002) ready.
Name (sdm:mtc): maint
331 Password required for maint.
Password:
230 User maint logged in.
ftp>
```

4 Change directory, list the file size, change the mode to binary, and get the file.

```
ftp> cd /swd/3pc
ftp> ls
ftp> bin
ftp> get <image_file_name>
```

***Note:*** Do not transfer a file with a name longer than 32 characters.

**Example**

```
ftp> cd /swd/3pc
250 CWD command successful.
ftp> ls
-rw-r--r--   1 maint    maint       1527 Jul 19 15:43 0001AF07C436
-rw-rw-rw-   1 maint    maint  232583460 Jul 17 09:39 CSNN06BK
ftp> bin
200 Type set to I.
ftp> get CSNN06BK
local: CSNN06BK remote: CSNN06BK
200 PORT command successful.
150 Opening data connection for CSNN06BK (binary mode) (232583460 bytes).
226 Transfer complete.
```

5 End the FTP session by typing bye and then list the files to verify that the file size is the same as it was on the CS 2000 Core Manager.

```
ftp> bye
>ls -l
```

### *At the MAPCI window*

6 Enter the DISKUT level and import the upgrade call processing application image. Determine the right syntax:

```
>DISKUT
>IMPORT <disk_vol> <image_file_name> 1020 IMAGE
```

**Example**
**> DISKUT; IMPORT SD00IMAGE CSNN06BK 1020 IMAGE**

**IMPORT command syntax determined by release**

| Upgrade from | IMPORT syntax |
|---|---|
| SN05 | IMPORT <disk_vol> <image_file_name> 1020 IMAGE |
| SN06 and newer | IMPORT <disk_vol> |

*The call processing application image is imported from the native file system into the call processing application file system. If the disk does not have enough space, a prompt to increase the volume size is presented.*

**7** This procedure is complete.

## Upgrade from SN04

Only perform this section if upgrading from SN04 to SN06.

***SITE — At the SDM window***

**1** Enter the /swd/3pc directory.

```
# cd /swd/3pc
```

**2** Transfer the file to the Call Agent with FTP. The transfer can require five to six hours.

**Example**

```
# ftp cm
Connected to core.
220 Welcome to Northern Telecom Supernode FTP BCS 52
Name (cm:root): <username>
331 Password required.
Password:<password>
230 User logged in, proceed
ftp> bin
200 Type set to I.
ftp> quote site lrecl 1020
200 Command okay.
ftp> cd /SD00IMAGE
200 Command okay.
ftp> put CSSNC06BG
```

Replace SD00IMAGE with the preferred location for the image.

Replace CSSNC06BG with the name of the image file.

***Note:*** To provide an indication of transfer progress, optionally enter **hash** after the **cd** command.

**3** After the transfer completes, end the FTP session.

```
ftp> quit
```

***SDE — At the ACTIVECM window***

**4** Enter the disk utilities level.

```
> DISKUT
```

**5** List the files in the volume that contains the transferred image.

```
> LF <vol_name>
```

**vol_name**
is SD00IMAGE or SD01IMAGE

6 Change the file attributes of the transferred image.

```
> FA <image_name> SET ATTR CURRENT IMAGE
```

**image_name**
is the name of the file transferred in step 2

7 This procedure is complete.

# Clean up SFDEV

Use this procedure to remove files from the Store File Device (SFDEV).

If call processing application patch files were downloaded in SFDEV, do not delete these files.

***ACT — At the ACTIVECM window***

**1** Determine the files in SFDEV:

```
> LISTSF ALL
```

**2** Copy files from SFDEV to storage:

```
> SCANF SFDEV COPY <disk_vol> NAME <file_name>
```

**disk_vol**
is the destination storage volume like SD00TEMP

**file_name**
is the name of the file to copy

**3** Erase files that are not essential from SFDEV:

```
> ERASESF <file_name>
```

**4** This procedure is complete.

# Verify table ACDGRP

Perform this procedure to prevent the software from incorrectly renumbering tuples in table ACDGRP during the call processing software upgrade.

### *ACT — At the ACTIVECM window*

**1** Determine if there are non-consecutive keys in table ACDGRP:

```
> OMSHOW ACDGRP ACTIVE
```

**2** Review the output and note if any keys are missing:

```
ACDGRP
CLASS:   ACTIVE
START:2002/06/20 09:30:00 THU; STOP: 2002/06/20 09:54:27 THU
SLOWSAMPLES:         15 ; FASTSAMPLES:         147 ;
       KEY (AUTOMATIC_CALL_DISTRIB_GROUP)
          ACDOFFR     ACDANSR    ACDDFLCT    ACDABNDN
            ACDNS    ACDPRMPT    ACDBLOCK    ACDTMOFL
         ACDTMINF    ACDTMANS      ACDCIF     ACDXFER
           ACDCPK    ACDUSAGE    ACDUSAG2     ACDICQD
          ACDREQD     ACDDMCT    ACDRQABN    ACDRQRTE

  0 NACDP
                0           0           0           0
                0           0           0           0
                0           0           0           0
                0           0           0           0
                0           0           0           0

  2 NACD2P
                0           0           0           0
                0           0           0           0
                0           0           0           0
                0           0           0           0
                0           0           0           0
```

Index key 1 is missing.

**3** If any index keys are missing, have translation personnel provision dummy tuples in the key indexes. Also provide datafill in table DNROUTE for each tuple added to table ACDGRP.

**4** This procedure is complete.

## Fill in test call scripts

Test calls should be made and verified to work as expected prior to the software upgrade, preferably on the day of the ONP. Identify calling irregularities ahead of time. This will avoid unnecessary investigation of a pre-existing condition after SWACT.

**ATTENTION**
Nortel Networks recommends that SITE personnel complete their Test Call Scripts before continuing with the software release upgrade process. Identifying calling irregularities now avoids unnecessary troubleshooting after SWACT.

This section presents generic guidelines for creating a test call plan to be used both before and after the switch of activity (SWACT) to a new load.

The purpose of test calls is to verify the performance of newly installed software for telephone switching systems. Test calls can ensure the smooth operation of thousands of calling situations with different combinations of telephone sets, service features, and traffic conditions on the network. Such testing helps ensure the availability and reliability of features and services for telephone users.

“Test call scripts” refers to the verification calls as predefined by the Telephone/Carrier Operating Company. These are test calls to be performed after activating the new software load in order to confirm acceptability of the new load. In the ONP procedure the test call scripts are put to use as follows:

- As a part of site preparation, this procedure instructs the operating company to fill in and test the test call scripts before beginning the upgrade. This is to provide a thorough test plan exercise for validating the new software load.
- Then, after activating the new software load, the operating company performs the test call scripts again to verify the software load.

The test call scripts provided below are only examples of call types that could be included in the Test Call Scripts. These samples include only basic call processing tests and provide some, but not all, critical test calls. These are provided only as a guideline. Each telephone/carrier

office should determine the best mix of test calls to use based on the office's unique configuration.

**ATTENTION**

The test calls listed in the following procedures will not apply to every office.

The telephone office will have to customize the list according to its own particular configuration.

Nortel Networks recommends including the following items in your POSTSWACT testing routine.

Add any other items that are determined to be important.

POSTSWACT call checklist

__ Verify date, time and DIALTONE

__ Perform Critical Call Tests (for example, 0- and 0+7/10). See the following procedure.

__ Perform IDDD (International Direct Distance Dialing) calls

__ Check Equal Access origination and termination

__ Perform CCIS (Common Channel Inter-office Signaling) calls

__ Verify ACTS (Automatic Coin Toll Service)

__ Verify DRAMS (announcements and SIT tones)

__ Check WATS (Wide Area Telephone Service), INWATS, OUTWATS, 2-way

__ Verify Pay Station Coin Control (Coin Collect and Coin Return)

__ Verify miscellaneous services such as 311, 411, 611, and repair services

__ Check EAS (Extended Area Service) calls

__ Perform TOPS (Traffic Operator Position System) calls

__ Perform MCCS (Mechanized Calling Card Service) calls

__ Perform DISA (Direct Inward System Access) calls

__ Verify Custom Calling Features

***SITE — At the office***

**1** Perform the critical test calls and record the results.

| Test description | From: line type or CLLI | To: call type and digits dialed | Test result |
|---|---|---|---|
| Check for DIALTONE on all line modules | | | |
| Verify ‘0’ minus route | | | |
| Verify ‘0’ plus route | | | |
| Verify ONI 1-7, 1-10 digits | | | |
| Verify EAS incoming and outgoing routes | | | |
| Verify CAMA routes | | | |
| Verify local Tandem routes | | | |
| Verify DDO routes | | | |
| Verify Directory Assistance | | | |
| Verify critical service routes (911, police, file, hospitals, and radio stations) | | | |
| Verify TOLL COMP (DTS) route | | | |
| Verify 1FR intra-office call | | | |
| Verify Remotes:<br>• EAS outgoing (one route)<br>• ‘0’ plus ‘0’ minus<br>• CAMA ANI<br>• 1FR intra-Remote | | | |
| Verify Operator Intercept route | | | |
| Verify all (idle) customer/network trunks | | | |

**2** Perform additional test calls sample.

**a** Verify regular POTS calls:

line (1FR) -> line (1FR)

(969-xxxx -> 969-xxxx)

line (PPHONE) -> trunk -> line (1FR)

(969-xxxx -> 9-1-514-970-xxxx)

**b** Verify use of different PM types:

line (LM) -> line (RLM)

(969-xxxx -> 969-xxxx)

line (LCM) -> line (RLCM)

(969-xxxx -> 969-xxxx)

**c** Verify use of different trunk types:

line (1FR) -> PTS trunk -> line (1FR)

(968-xxxx -> 969-xxxx)

line (1FR) -> ISUP trunk (all variants supported by office) -> line (KSET-Disp M5209T)

(968-xxxx -> 6-456-xxxx)

**d** Verify ISDN calls:

line (KSET-Disp M5317T) -> trunk -> line (KSET-Disp M5209T)

(968-xxxx -> 6-456-xxxx)

line (PPHONE-Disp M5317T) -> trunk -> line (1FR-Disp Maestro)

(968-xxxx -> 9-969-xxxx)

line (KSET-Disp M5317T) -> trunk -> line (PPHONE-Meridan Bus.)

(968-xxxx -> 9-1-819-456-xxxx)

line (KSET-Disp M5317T) -> line (KSET-PSET)

(968-xxxx -> 968-xxxx)

line (BRAMFT set) -> line (BRAFS set)

(968-xxxx -> 968-xxxx)

line (1FR) -> line (BRAKS set)

(968-xxxx -> 968-xxxx)

**3** Proceed after test call scripts are verified.

# Perform TABAUDIT

Begin this procedure 30 calendar days before the software delivery application date and complete the TABAUDIT with no errors at least 10 days before the ONP. Nortel Networks Global Software Delivery recommends scheduling automatic TABAUDITs (AUTOTABAUDIT), rather than manual TABAUDITs. TABAUDIT must complete successfully before the ONP.

Restrictions on AUTOTABAUDIT:

- Only one user at a time is allowed to enter the AUTOTABAUDIT level.
- Before executing AUTOTABAUDIT, a list of session parameters must be defined from within the AUTOTABAUDIT level.
- Only one AUTOTABAUDIT session can execute at a time. However, multiple AUTOTABAUDIT sessions can be scheduled.
- The parameters for the active AUTOTABAUDIT session cannot be changed without terminating the session first.
- AUTOTABAUDIT cannot be executed at the same time as TABXFR or an image dump.
- For wireless applications on HLR offices, AUTOTABAUDIT should be scheduled to execute during off hours to avoid delays with subscriber provisioning.

***SITE — At the ACTIVECM window***

**1**



**CAUTION**
**Possible service interruption**
Review software delivery bulletins and current warning bulletins about TABAUDIT.

Enter the automated table audit level:

```
> TABAUDIT; AUTO
```

**2** Clear the list of tables to be included in the check:

```
> CLEAR INCLUDED
```

3 Clear the scheduled list of time frames:

```
> CLEAR SCHEDULE ALL
```

***Note:*** This command clears all scheduled TABAUDIT sessions identified in table AUTOTAB.

4 Set all tables for verification:

```
> INCLUDE ALL
```

5 Define the scheduled AUTOTABAUDIT session:

```
> TIMEFRAME SINGLE <start_time> [<start_date>]
<stop_time> [<stop_date>]
```

**start_time**
is the hour and minute to begin the TABAUDIT and is specified as HH:MM, such as 23:30

**start_date**
is an optional parameter and is specified as YYYY:MM:DD, such as 2002:06:21

**stop_time**
identifies the latest time by which that the TABAUDIT must complete

***Note:*** The timeframe must be 30 minutes or more.

6 Verify the parameters:

```
> STATUS
```

```
AUTOTABAUDIT is scheduled to execute during the start
and stop period between the start and stop dates.
-------------------------------------------------------------------------
|                                                                       |
|                        AUTOTABAUDIT STATUS                            |
|                                                                       |
-------------------------------------------------------------------------
| Active Timeframe    | Executing Timeframe  |                          |
-------------------------------------------------------------------------
| Start        Stop   |   Start      Stop    | Scheduling  |  REGULAR   |
| Date         Date   |   Time       Time    | Option      | or SUBSET  |
-------------------------------------------------------------------------
|                                                                       |
|2002/06/24 2002/06/24    18:30      20:00   | SINGLE      |  REGULAR   |
|                                                                       |
-------------------------------------------------------------------------
Current time      : 2002/06/24 07:16:07
AUTOTABAUDIT      : Inactive
The following events were logged while verifying tables:
 1 TABAUDIT aborted. All included tables not verified. Out of time.
The following tables are included for the REGULAR AUTOTABAUDIT:
  From table VERSIONS (0)                  to table INWATNPA (1408).
No tables have been excluded for the REGULAR AUTOTABAUDIT.
No tables have been included for the SUBSET AUTOTABAUDIT.
The following tables are excluded for the SUBSET AUTOTABAUDIT:
  From table VERSIONS (0)                  to table INWATNPA (1408).
```

**7** Begin the table audit;

**> EXECUTE**

**8** Confirm the table audit:

**> Y**

**9** The audit can require 30 minutes to complete.

**10** Verify the table audit results:

**> REPORT ERRORS**

| If | Do |
|---|---|
| no errors are reported | step 12 |
| errors are reported | Correct the errors using the table editor and repeat from step 4. Refer to the Additional information. |

**11** If any tables failed, perform the following steps for each table.

**a** Quit to the TABAUDIT level:

```
> QUIT
```

**b** Include the failed table:

```
> INCLUDE <table_name>
```

**c** Execute the TABAUDIT:

```
> EXECUTE
```

**d** View the results:

```
> REPORT <table_name>
```

**e** Repeat from step b for each failed table.

**12** Quit to the CI level:

```
> QUIT ALL
```

**13** This procedure is complete.

## Additional information

Use the following procedure to assist in repairing tables.

***SITE — At the ACTIVECM window***

**1** Enter the table that has an error:

```
> TABLE <table_name>
```

**tab_name**
is a table name like TRKMEM

**2** Position on the failed tuple:

```
> POS <tuple>
```

**tuple**
is the failed tuple such as “AL7ITICS7 2”

**3** Check the tuple:

```
> CHECK
```

**4** Note the error message and make corrections.

**5** Repeat this procedure for all failed tables.

# Execute SWUPGRADE READY

Nortel Networks Global Software Delivery personnel complete this procedure at scheduled milestones before the ONP.

At any time during this procedure, to determine the status, use the **DISP STEPS** command. Help for steps is available with the **HELP** command. A step can be re-run with the **RUNSTEP <step_name>** command. Ensure that all steps complete successfully, but a step can be overridden with the **OVERRIDE** command. To cancel the procedure, use the **CANCEL** command.

The steps are determined by the CS 2000 - Compact configuration. If the CS 2000 - Compact is configured with Message Controller cards, more steps are provided.

**SWUPGRADE READY steps**

| without Message Controllers | with Message Controllers |
|---|---|
| SETUP_ENV_VARS | SETUP_ENV_VARS |
| | VERIFY_SN_PECS_INFO |
| VERIFY_LOGS_INFO | VERIFY_LOGS_INFO |
| DEVICE_CHECK | DEVICE_CHECK |
| TABAUDIT_VERIFY_TABLES | TABAUDIT_VERIFY_TABLES |
| | DISPLAY_PERIPHERAL_LOAD_NAMES |
| | DISPLAY_SPM_LOADNAMES |
| | DISPLAY_PRL_LOADS |
| | CHECK_ISN_PMS |
| | DISPLAY_MS_FW_LOADS |
| | VERIFY_PM_LOAD_NAMES |
| | LIUINV_CHECK |
| | C7LINK_CHECK |
| | CHECK_LTCINV |

**SWUPGRADE READY steps**

| without Message Controllers | with Message Controllers |
|---|---|
| DISPLAY_NOP_USERS | DISPLAY_NOP_USERS |
| DISPLAY_DPP_VERSION | DISPLAY_DPP_VERSION |
| | CHECK_LCMINV |
| SBA_CHECK | SBA_CHECK |
| SBA_VOLSIZE_CHECK | SBA_VOLSIZE_CHECK |
| READY_STATUS | READY_STATUS |
| READY_COMPLETE | READY_COMPLETE |

***SDE — At the ACTIVECM window***

**1** Enter the SWUPGRADE level:

```
> SWUPGRADE READY
```

**2** Begin the process:

```
> START
```

*Step SETUP_ENV_VARS begins. This step sets the environment variables that will be used during the READY session. Default values appear in square brackets and variables without brackets have no default. To accept the default value press the Return key without entering a value.*

*Values consisting of more than one word must not be enclosed in quotes. If they are, the quotes will be considered as part of the word and the variable will be either set to an incorrect value or not set at all.*

**a** Set the TRACE_USER variable.

**TRACE_USER (no default)**
Holds the USER name on whose console output messages are printed. Changing the value of this variable, also changes the value of the TRACE_DEVICE variable, and causes the output to be redirected to the new USER device.

Value: <user name> or ME - a user name, such as ADMIN, or ME which indicates the current user

***Note:*** For clarity purposes, it is recommended to set this variable to a user other than the current user.

The USER must be LOGGED IN when this variable is set.
The current setting is: <none>

```
> ME
```

**b** Do not change the TRACE_DEVICE variable, press the Enter key.

**TRACE_DEVICE**
Holds the device name on which output messages are printed. Changing the value of this variable causes the output to be redirected to the new device.

Value: <trace device name> - a string, such as MAP

***Note:*** For clarity purposes, it is recommended to set this variable to a device other than the terminal currently logged onto.

The current setting is: <none>

```
>
```

**c** Set LOGS variable.

**LOGS**
Holds the names of the logs that are checked by the LOGS step. More than one log can be specified by entering log names separated by a blank.

**Example**
CM — Check CM logs and display a message if CM logs are recorded.

**Example**
'SWERR TRAP' — Check traps and swerrs. Display a message if traps or swerrs are recorded.

The current setting is: TRAP SWERR

```
> TRAP SWERR
```

**d** Set TO_CSP_CM_LOAD variable. Enter the value of the CSP load number.

**TO_CSP_LOAD**
The TO_CSP_LOAD variable allows the user to set the CSP load to which the site plans to upgrade. This variable is then used to check the PMs for a software load which equals this value.

The current setting is: 0

```
> 19
```

***Note:*** CSP 19 is equivalent to the SN06 release.

**e** Do not set the PM_VERIFY_FILE variable, press the Enter key.

**PM_VERIFY_FILE**
The PM_VERIFY_FILE variable allows the user to set which verification file will be used to validate if the queried peripheral module loads are valid.

The current setting is: NONE

**>**

**f** Do not change the PRINTER variable, press the Enter key.

**PRINTER**
The PRINTER variable holds the name of the printer on which output messages are recorded. The printer echoes all output sent to the trace device. Changing the value of this variable causes the recording to be directed to the new device.

Value: <printer name> or SINK

where <printer name> is a device datafilled in table TERMDEV. SINK indicates not to record to a printer device.

The current setting is: SINK

**>**

**g** Do not change the PAUSE_ENABLED variable, press the Enter key.

**PAUSE_ENABLED**
PAUSE_ENABLED is used to determine if the READY steps will run continuously or be paused out after executing. A NO setting allows the READY platform to run until completion of all the steps. A YES setting prompts the process to pause after each step is run. This pause allows time for the user to review the results and set a step COMPLETED/NEEDED before proceeding.

***Note:*** Type HELP STEP_STATUS for more information on setting the step status.

The current setting is: YES

**>**

```
SWUPGRADE variables for target READY:

Variable Name                                        Value
------------------------------------------------------------
TRACE_USER                          =    ME
TRACE_DEVICE                        =    TELNSVR00033
LOGS                                =    TRAP SWERR
TO_CSP_LOAD                         =    19
PM_VERIFY_FILE                      =    NONE
PRINTER                             =    SINK
PAUSE_ENABLED                       =    YES

Setup completed.
Enter GO to begin execution of steps.
```

**h** Commit the variable changes:

**> GO**

*Step SETUP_ENV_VARS completes.*

*If the CS 2000 - Compact is configured with Message Controller cards, step VERIFY_SN_PECS_INFO runs. This step checks and prints the Message Switch software load and all the hardware in the Message Switch.*

*Step VERIFY_LOGS_INFO runs and completes. This step displays any log reports provided in environment variable LOGS. These logs should be checked periodically for front-end stability. Include or exclude any log(s) the user would like displayed.*

*Step DEVICE_CHECK runs. This step verifies that all devices on the active CPU are in an OK, OFFLINE, or UNEQUIPPED status. These are acceptable states for SWACT. Any devices found in any other state are displayed.*

*Step TABAUDIT_VERIFY_TABLES runs. This step verifies that TABAUDIT has been executed and tables to be dumped and restored have been audited in the last thirty days.*

*If the CS 2000 - Compact is configured with Message Controller cards, steps DISPLAY_PERIPHERAL_LOAD_NAMES, DISPLAY_SPM_LOADNAMES, DISPLAY_PRL_LOADNAMES, CHECK_ISN_PMS, and DISPLAY_MS_FW_LOADS run. These steps print all the PM names, locations, and software load names for the PMs in the office, as well as the firmware loads in the Message Switch.*

**3** If the CS 2000 - Compact is configured with Message Controller cards, step VERIFY_PM_LOAD_NAMES runs. This step queries all the PMs with downloadable software and verifies that each PM is loaded with the load specified in PM_VERIFY_FILE. PM_VERIFY_FILE was set during step SETUP_ENV_VARS. This file is a PM to PM load cross reference. If the file is not available, or a PM is running a different load, the process stops. Correct the problem, type GO and press the Enter key.

*Step VERIFY_PM_LOAD_NAMES completes.*

*If the CS 2000 - Compact is configured with Message Controller cards, steps LIUINV_CHECK, C7LINK_CHECK, CHECK_LTCINV, and CHECK_LCMINV run. These steps ensure that no LIU name has a LIUNO greater than 512, that all MSB7 and LIU7 PMs have field LINKNAME datafilled, that all DTCs datafilled in table LTCINV for CCS7 are datafilled correctly, and that LCMs have the amount of memory datafilled in table LCMINV and that the LCMs are in service.*

**4** Step DISPLAY_NOP_USERS runs and completes.

*This step displays all NOP/MPC users and their status.*

**5** Step DISPLAY_DPP_VERSION runs and completes.

*This steps displays DPP hardware and software information and DPP status.*

**6** Steps SBA_CHECK runs and completes.

*This step verifies that on an XA-Core machine if an upgrade is being performed to CSP16 and beyond, then all the backup volumes are configured only on IOP disks. No older disk types are supported as backup for the SBA streams on an XA-Core platform from CSP16 onwards.*

**7** Step SBA_VOLSIZE_CHECK runs and completes.

*This step verifies that the size of the volumes that are configured as backup for SBA satisfy the minimal size requirements. This check will print out those stream-volume pairs whose backup volume sizes are below the minimal criterion that have been set.*

**8** Step READY_STATUS runs and completes.

*This step displays step state and status.*

**9** Step READY_COMPLETE runs and completes. Ensure that step READY_STATUS indicates all steps are complete.

```
> QUIT
```

*This step reminds the user to quit the SWUPGRADE increment and QUIT from the switch after the READY program is completed.*

**10** This procedure is complete.

# Dump call processing application image

Complete this procedure the day of the ONP.

***SITE — At the ACTIVECM window***

**1** Enter the disk utilities level:

```
> DISKUT
```

**2** Verify that there are at least 500 000 free blocks for an office image:

```
> LV SD00IMAGE; LV SD01IMAGE
```

```
> LV SD00IMAGE; LV SD01IMAGE
Volumes found matching the prefix SD00IMAGE:
-----------------------------------------------
NAME        TYPE      TOTAL       FREE TOTAL  OPEN  ITOC  LARGEST
                     BLOCKS     BLOCKS FILES FILES FILES  FREE SEGMENT
-------------------------------------------------------------------------
SD00IMAGE   STD    1638400     822665     0     0     0     822665
Total number of volumes matching prefix SD00IMAGE : 1.
Volumes found matching the prefix SD01IMAGE:
-----------------------------------------------
NAME        TYPE      TOTAL       FREE TOTAL  OPEN  ITOC    LARGEST
                     BLOCKS     BLOCKS FILES FILES FILES  FREE SEGMENT
-------------------------------------------------------------------------
SD01IMAGE   STD    1638400     814430     3     0     1     814430
Total number of volumes matching prefix SD01IMAGE : 1.
>
```

***Note:*** If there is not enough space, determine if old images can be deleted. Use the **DDF** command to delete files. Refer to DDF Example for more information.

**3** Dump the image to a disk volume:

```
> AUTODUMP MANUAL
```

if AUTODUMP is active for the office.

*or*

```
 > DUMP <image_name> <disk_vol> ACTIVE UPDATE
VERBOSE NODE CM
```

**image_name**
is the name of the file to create

**disk_vol**
is sd00image or sd01image

if AUTODUMP is not active for the office

*The dump can require two hours to complete.*

4 Record the name of the image on a sheet of paper. If this upgrade is an ONP, it is important to have a current image as a backup in the event that the ONP fails. If this is a platform only MR upgrade, it is necessary to know the name of the image so it can be loaded during procedure “LDMATE (Load inactive)” in *Upgrading the Call Agent,* NN10065-461.

5 Nortel Networks recommends backing up the image. The backup procedure is documented in *Call Agent Fault Management*, NN10087-911 and is reproduced here for convenience under heading Backup image.

6 This procedure is complete.

If this is a platform only upgrade, proceed to “Boot new platform software” in *Upgrading the Call Agent,* NN10065-461. Otherwise, the next phase of the upgrade takes place on the day of the upgrade is begins on Site responsibilities the day of the software delivery on page 1131.

## DDF Example

The following figure shows an example of using the DDF command.

```
>diskut
Disk utility now active.
DISKUT:
>lf sd00image0

File information for volume SD00IMAGE0:
{NOTE:  1 BLOCK = 512 BYTES }


-------------------------------------------------------------------------
FILE NAME                       O R I O O V FILE   MAX    NUM OF    FILE
                                R E T P L L CODE   REC   RECORDS    SIZE
                                G C O E D D        LEN        IN      IN
                                    C N                     FILE  BLOCKS
-------------------------------------------------------------------------
CSNW06BA                        I F            0  1020    208457  415286
.ITOC                           O F            0  1024         1       2
SCS06BA_WC_0131_CM              I F Y          0  1020    213073  424482
SCS05BK_WC_0131_CM              I F            0  1020    196563  391591
SCS05BK_WC_0128_CM              I F            0  1020    196563  391591

>ddf CSNW06BA
Delete CSNW06BA from volume SD00IMAGE0?
Please confirm ("YES","Y","NO","N"):
>y
File CSNW06BA has been deleted from volume SD00IMAGE0.
```

## Backup image

Use the following procedure to back up a call processing application image.

***At the active Call Agent Manager window (CORE0 or CORE1)***

1 Quit the Call Agent Manager interface:

```
> QUIT ALL
```

2 Change directory to the location of the image. If the image was dumped to disk SD01, substitute sd01 for sd00 in the following figure.

```
[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 Use the mount command to determine the IP addresses of the STORM units.

**[mtc@ip_address mtc]$ mount**

*Determine which STORM unit provides sd00 and which provides sd01. This information is needed in step 7.*

```
[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 frame*

4 Insert a DVD-RW (write once DVD) in the CDROM tray. A rewritable DVD (DVD+RW) will not work. If the CS 2000 Management Tools server uses two Sun Microsystems Netra 240 machines, insert the DVD-RW into the active unit. The active unit is identified by a lit USER LED.

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

5 Log in as a maintenance level user such as the maint user. Root permissions are needed 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 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 "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 3.

**/path_to_file**
is the absolute path to the files on the STORM unit to copy such as
`/nfsserv/3pc/cs/sd00/image0/IMG_TO_BACKUP`

**Example**
Copy an office image named S040210135002_CM from SD00ADUMP0:

**$ scp "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.*

**8** Rename the image file to end in ".img1020:"

```
$ cd /data/tmp
$ mv <IMG_TO_BACKUP> <IMG_TO_BACKUP>.img1020
```

**9** Change directory to `/data` and make an ISO9660 image named dvdimage.iso with Rock Ridge extensions from the image:

```
$ cd /data
$ mkisofs -R -o /data/dvdimage.iso
/data/tmp/<IMG_TO_BACKUP>.img1020
```

***Note:*** There is a space after /data/dvdimage.iso and before /data/tmp/<IMG_TO_BACKUP>.img1020

*Status is printed to the terminal:*

**Create dvdimage.iso with mkisofs command**

```
$ mkisofs -R -o /data/dvdimage.iso /data/tmp/<IMG_TO_BACKUP>.img1020
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)
$
```

**10** Become the root user:

**$ su - root**

Provide the root password at the prompt.

**11** 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. Re-enter 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
```

**12** 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.*

**13** 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.***

**14** 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****.*

**15** Check that ISO 9660 image recorded correctly:

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

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

**16** 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.*

17 Use the **rm** command to erase the image so the volume does not fill up:

```
$ rm /data/tmp/<IMG_TO_BACKUP>.img1020
$ rm /data/dvdimage.iso
```

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

18 Remove the DVD-RW from the tray and close the tray. Label the DVD-RW.

19 Store the DVD-RW per office procedure.

20 This procedure is complete.

# Preparing to upgrade the Multiservice Switch 15000/Media Gateway 15000/20000 in Succession IP Solutions

**ATTENTION**
Direct upgrade from SN05 to SN07 is not supported for Nortel Networks Multiservice Switch/Media Gateway 7480/15000/20000 nodes. Upgrade to SN06.2 first and then upgrade from SN06.2 to SN07. Refer to NTP 241-5701-272 *Passport 7400, 15000, 20000 Software Upgrade* in the SN06.2 Helmsman collection for the upgrade to SN06.2 and then return to this document to complete the upgrade to SN07.

The following topics are discussed in this section:


- Who should read this document and why on page 428
- What you need to know on page 429
- How this document is organized on page 429
- What's new in this document on page 430


## Who should read this document and why

This document is intended for users who are using hitless software migration to upgrade Nortel Networks Multiservice Switch 15000/Media Gateway 15000/20000 nodes from:

- an SN06 or SN06.2 software version, or from one SN07 software version to another software version within the context of a PacketTrunking - IP (PT-IP), PacketTrunking - AAL2 (PT-AAL2), Integrated Access Cable (IAC), or Integrated Access Wireline (IAW) solutions.

This document is also intended for users who are using hitless software migration to upgrade Nortel Networks Multiservice Switch 15000/Media Gateway 15000 nodes from:

- one SN07 software version to another software version within the context of an Universal Access - Internet Protocol (UA-IP) solution upgrade. This document does not describe hitless software

migration for Multiservice Switch 20000 and Media Gateway 20000 nodes within the UA-IP solution.

The MultiService Switch provides IP routing functionality over both Ethernet and ATM while the Media Gateway 15000 provides standard trunk gateway functionality.

Note the following:

- For a non-hitless software migration on Multiservice Switch 15000/Media Gateway 15000/20000 or Media Gateway 7480 elements in UA-IP, PT-IP, PT-AAL2, IAC, and IAW solutions from SN06, or SN06.2 to SN07, refer to the NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software* guide.

  ***Note:*** After you have performed the non-hitless software migration using the NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software* guide, refer to Feature activation on page 1296 in this document to activate the features.

- The upgrade of other components within the UA-IP solution is not within the scope of this document. For more information about the solution level upgrades, see NN10320-100 *ATM Solutions Basics*, NN10004-100 *UAA Product and Technology Fundamentals*, and NN10300-100 *IP Solutions Basics*.
- The examples shown in this document represent an SN07 to SN07 upgrade of Multiservice Switch 15000/Media Gateway 15000 in a UA-IP solution.

## What you need to know

To perform the procedures discussed in this document, you must have an extensive knowledge of Unix, Nortel Networks Preside Multiservice Data Manager servers, and Multiservice Switch/Media Gateway software.

## How this document is organized

This document presents a detailed flow chart of the specific tasks required to upgrade a Nortel Networks Multiservice Switch 15000/Media Gateway 15000/20000 node via Hitless software migration using Nortel Networks Preside Multiservice Data Manager (MDM) Command Console.

It also contains a detailed description of what happens on the node during a hitless software migration (HSM). Finally, it contains

troubleshooting information and procedures to abort the upgrade if required.

The guide has three parts that reflect the basic phases of the upgrade:

- preparation phase
- migration phase
- new feature activation, troubleshooting and rollback phase

The preparation phase is the phase during which information is gathered and software is downloaded. This phase is described in the sections:

- Information collection on page 438
- Downloading and backing up node software on page 446

The migration phase is the phase during which pre-HSM checks are made, the migration occurs, and post migration check are made. This phase is described in the sections:

- HSM (Command Console) pre-work on page 1236
- HSM (Command Console) activation on page 1261

The new feature activation, troubleshooting and rollback phases are phases where the new features are activated (if applicable), problems are fixed, or the migration is rolled back (if required). These phases are described in the sections:

- Feature activation on page 1296
- “Rollback” in Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP), NN10419-461
- “Troubleshooting a software upgrade” in Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP), NN10419-461

## What’s new in this document

This document is new in PCR 6.1 and SN07.

### Branding changes

The terms Passport 15000 and PVG have been rebranded in conjunction with the new Nortel Networks' brand simplified naming format:

- The Passport 15000 is now referred to as the Nortel Networks Multiservice Switch 15000.
- The PVG is now referred to as the Media Gateway 15000.

The Multiservice Switch 15000 and Media Gateway 15000 network elements continue to share common hardware and software aspects. Hybrid systems can combine these network elements' capabilities, despite the fact that no specific brand exists for such hybrids.

For more information on the product rebranding, refer to NN10600-000 *Nortel Networks Multiservice Switch 7400/15000/20000 What's New in PCR6.1*.

# Software migration

Upgrading a Nortel Networks Multiservice Switch 15000/Media Gateway 15000/20000 node in a carrier grade configuration is also known as a hitless software migration (HSM). HSM is not supported on Multiservice Switch/Media Gateway 7480 elements. During an upgrade of a Succession solution's components, the node must be upgraded so that you can access new, enhanced, or corrected software applications.

***Note:*** If you are performing a software upgrade on Multiservice Switch/Media Gateway 7480 elements or, a non-hitless software upgrade on Multiservice Switch/Media Gateway 15000/20000 elements, or an upgrade on out-of-service (OOS) Multiservice Switch/Media Gateway 15000/20000 nodes, refer to the NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software* guide.

This section describes the prerequisites that must be in place before an HSM can proceed. For overview information on performing HSM using Preside Multiservice Data Manager (MDM), see What happens to the node during a hitless software migration on page 1231.


- Prerequisites to performing a software upgrade on page 432
- Upgrade task flow on page 436


## Prerequisites to performing a software upgrade



**CAUTION**
**Calls in process of being set up are dropped**
This strategy removes standby control and function processors from service. As a result, redundancy of the active shelf components is not available and some calls in the process of being set up (known as transient calls) are dropped. Stable calls are unaffected by the migration.

- Preside MDM software is backwards compatible and can manage the current and previous Nortel Networks Multiservice Switch/Media Gateway releases. However, Preside MDM software is not necessarily forward compatible. As a result, upgrade Preside MDM servers before upgrading the nodes they manage. To upgrade

servers, see NN10185-461 *Upgrading Preside MDM in Succession Networks*.

- If you have DS-1 IMA interfaces using the Edgelink100 MUX, ensure that you use Edgelink100 MUX software (R3.3) during the SN07 upgrade. Contact Telco Systems to get the Edgelink100 MUX software and upgrade procedures: *http://www.telco.com/products/Transport/M13Multiplexers/EdgeLink100/*
- Ensure that all configuration changes from the Global Bulletin System (GBS) and any associated Method of Procedure (MOP) are reflected on the node before performing the upgrade.
- Before performing the upgrade, ensure that all journal files are either used or purged by issuing the *display ProvisioningSystem restorePossible* command. If the response is “yes”, see the table “Impact of an error condition on an HSM” in *Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP)*, NN10419-461.
- Determine the order in which the nodes are upgraded. For in-band OAM topologies, you must upgrade all Multiservice Switch 15000/Media Gateway 15000 nodes in the following sequence:
  - all remote nodes first
  - Gateway nodes next (non-preferred first and preferred, second). For more information about preferred and non-preferred gateways, see NN10028-111 *Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP* and In-band OAM quick reference on page 1312.
  - For all out-of-band OAM configurations, upgrade all the Multiservice Switch 15000/Media Gateway 15000 nodes:
    - not physically co-located with the CS2K first
    - physically co-located with the CS2K next
- You need extensive knowledge of Unix, Multiservice Switch/Media Gateway software, and the Succession portfolio architecture.
- You need a:
  - user ID for Nortel Networks web support. See Download release notes on page 440
  - user ID for Preside MDM software download
  - user ID for general access to Preside MDM

— Multiservice Switch user ID configured for local access, and access to FTP, FMIP, Telnet and Preside MDM server

— Multiservice Switch user ID with a minimum command scope of *device* and a command impact of *configuration*.

To determine your command scope and impact, type **me**. Information about your user ID is displayed.

- Nortel Networks recommends that you perform the tasks involving commands issued from the command line using Preside MDM Command Console tool rather than a Telnet session. For more information on using the Command Console, see 241-6001-804 *Preside MDM Workstation Utilities User Guide*.
- Ensure that all components supporting the service intended to be hitless are enabled. A check of all components should be performed prior to activating the migration provisioning to minimize any impacts to associated services.
- Nodes must be connected to Preside MDM servers. The nodes must also be in service and capable of supporting traffic and network management functions. In addition, the nodes must not have any major or critical alarms raised on them.
- Review *Nortel Networks Multiservice Switch Release Notes PCR6.1* to determine the following:

  — how the data model has changed for this release and how you must adjust your configuration to compensate for these changes

  — which features and services are required by this release and by each of the processor cards, and which software files and applications you need to download to support these features and services

  — if the software you are installing is compatible with the other software already on the node

- Ensure that you have an alternate way to access the node in case you lose IP connectivity during the migration.

  For example, you can connect an operator terminal as described in the section “Connecting an operator terminal” in the NN10600-130 *Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*. You could also use a modem or some other mode of out-of-band connectivity that should have been in place during the initial installation of the node.

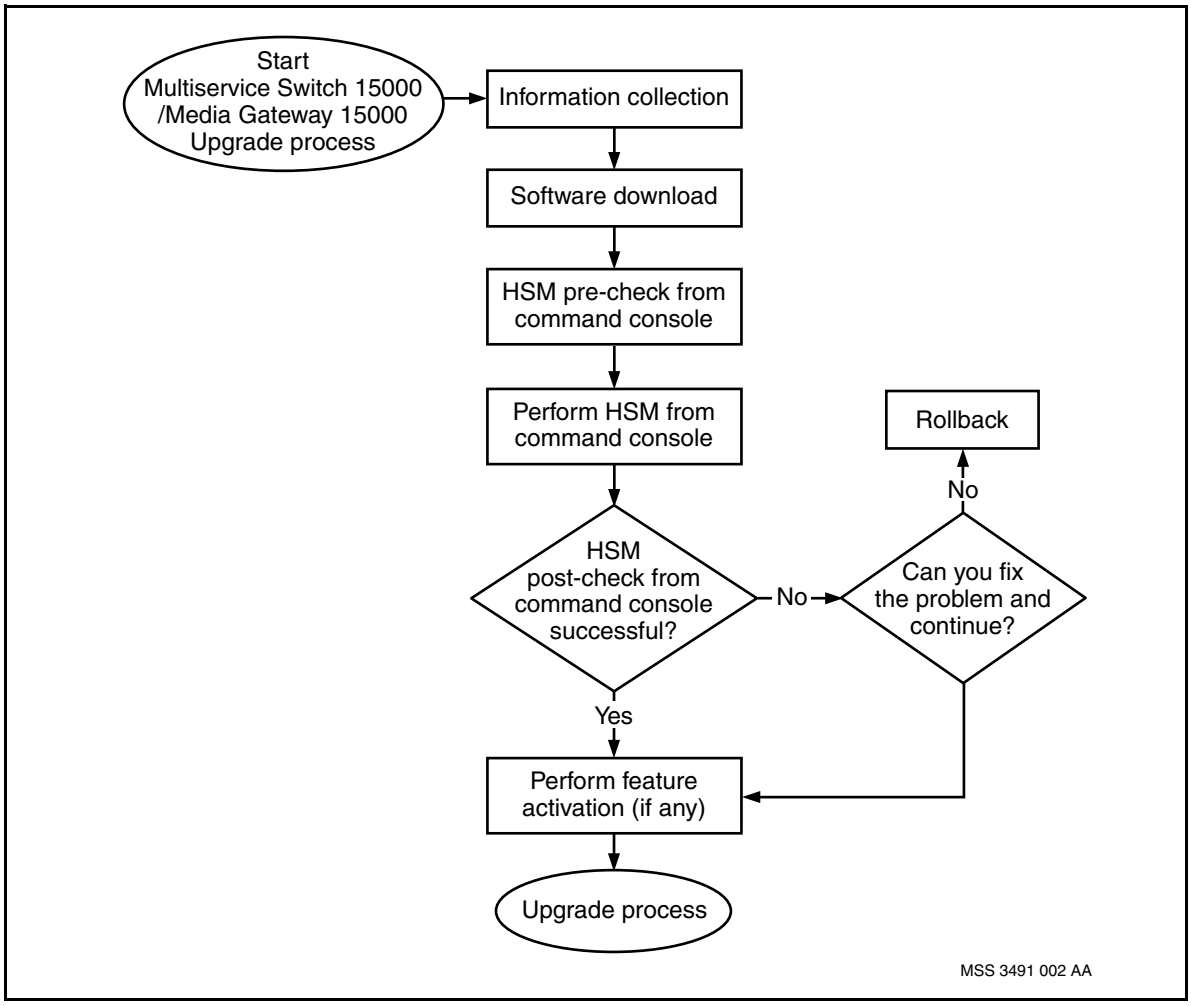
- You must complete the tasks described in the section Upgrade task flow on page 436 before installing additional hardware and configuring additional capabilities.
- Because of the amount of time required to remove old software releases, you may want to do this several days before beginning the upgrade. In particular, running the *tidy Software* command can take several hours to complete. As a result, you may want to run it overnight.

# Upgrade task flow

The figure Upgrade task flow on page 436 shows the sequence of procedures you must perform to upgrade Multiservice Switch 15000 nodes deployed as a Media Gateway 15000. To link to any procedure, go to the list that follows the task flow charts.

***Note:*** For information on performing upgrades on out-of-service (OSS) nodes, refer to the NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software* guide.

### Upgrade task flow



## Work flow navigation

- Information collection on page 438
- Downloading and backing up node software on page 446
- HSM (Command Console) pre-work on page 1236 for migrations performed from the Command Console
- HSM (Command Console) activation on page 1261
- Feature activation on page 1296
- “Rollback” in *Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP)*, NN10419-461

# Information collection

Collect information to identify and avoid any compatibility issues that could prevent a software migration completing successfully.

## Prerequisites to information collection

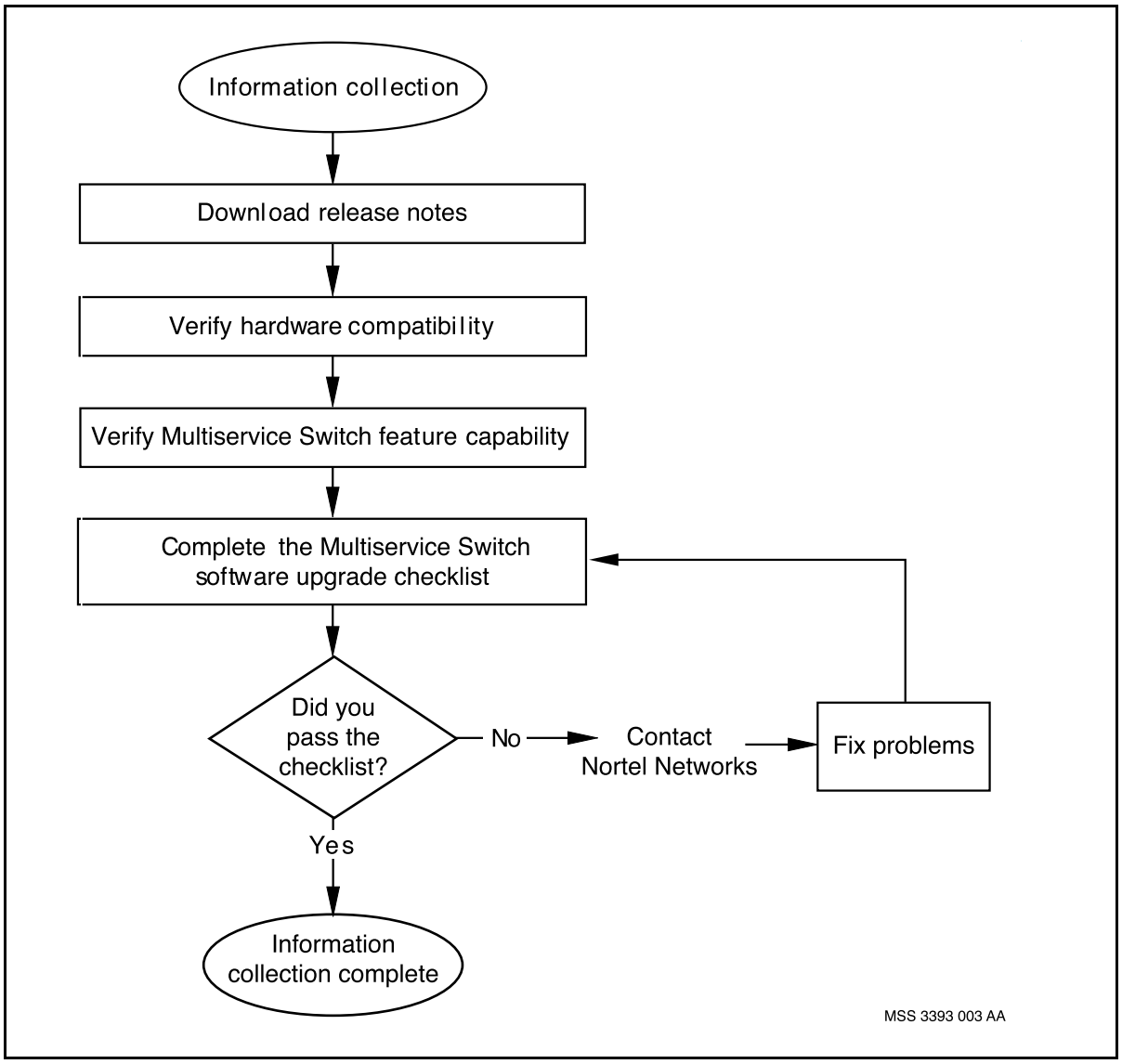
Before you start collecting information, you must:

- determine the order in which the Multiservice Switch 15000/Media Gateway 15000/20000 nodes will be upgraded
- determine if the Nortel Networks Preside Multiservice Data Manager (MDM) servers have been upgraded
- confirm which release of software is active on the node
- determine an upgrade path to identify the release to which you are migrating
- ensure that the node is operating without known errors or failures

## Information collection task flow

The task flow shows you the sequence of procedures you perform to collect information about the upgrade. To link to any procedure, go to Work flow navigation on page 439.

**Information collection task flow**




## Work flow navigation

- Download release notes on page 440
- Verify hardware compatibility on page 441
- Verify node feature compatibility on page 442
- Complete the software upgrade checklist on page 443

## Download release notes

Download the release notes for Multiservice Switch 15000/Media Gateway 15000/20000 in Succession solutions to collect specific information affecting hardware and services for each of the Multiservice Switch/Media Gateway software release (PCR) and Multiservice Switch for Succession software releases involved in the migration.

1. Go to the Nortel Networks public website. *http://www.nortelnetworks.com/*
2. In the section titled Support, click *Technical Documentation*.
3. Click Passport in the list of products.
4. Click *Documentation* under Passport Packet Voice Gateway (PVG).
5. A security screen appears requesting your user ID and password for web support.
6. Enter your user ID and password.
7. Select and download all the documentation you require.

## Verify hardware compatibility

Verify hardware compatibility to confirm that your hardware configuration will support all the software versions that will be used in the migration.

***From the node***

1 Note the product engineering codes (PECs) of all the function processor cards used installed in the node.

**d shelf card/* prc**

2 Review the hardware compatibility section in Nortel Networks Multiservice Switch Release Notes for each release in your migration path to determine if there are any other hardware considerations.

3 Compare your hardware configuration to the minimum supported hardware information in the Nortel Networks Multiservice Switch Release Notes of each release in the migration path.

## Verify node feature compatibility

Verify the compatibility of features on the node to confirm that your configuration of services and features will not be negatively affected by the software migration.

***From the node***

1 Create a list of all the applications loaded on the node:

**d -p sw lpt/* fl, log**

2 Refer to the Nortel Networks Multiservice Switch Release Notes for each PCR in your migration path to confirm there are no known compatibility issues.

3 If you have any doubt about the compatibiliy between your existing features and your migration path, contact your Nortel Networks Service Representative before beginning the migration.

## Complete the software upgrade checklist

Complete the software upgrade checklist to confirm that all potential complications have been considered and eliminated. Use the information gathered from performing the Information collection on page 438.

**Software upgrade checklist**

| Task | Yes | No | Date and Comments |
|---|---|---|---|
| A migration order has been established for all the Multiservice Switch/Media Gateway nodes in the network. | | | |
| Migration plan has been created including acceptance criteria and fall back strategy (backup and restore). | | | |
| Migration plan has been reviewed and verified by migration prime as well as operational and engineering resources. | | | |
| Migration operator has complete knowledge of Multiservice Switch/Media Gateway node applications, features and software. | | | |
| Migration operator has complete knowledge of all software versions in the migration. | | | |
| *Nortel Networks Multiservice Switch Release Notes* for all PCR releases in the migration path have been reviewed for potential impacts to the migration plan. | | | |
| Network health has been analyzed to verify that no known problems exist. | | | |
| Network management platform meets minimum hardware requirements. | | | |
| Network management software is compatible with each release in the migration plan. | | | |
| | | | |

| Task | Yes | No | Date and Comments |
|---|---|---|---|
| Multiservice Switch/Media Gateway hardware is compatible with all releases in the migration plan. | | | |
| Multiservice Switch/Media Gateway software is compatible with all releases in the migration plan. | | | |
| All provisioning files have been saved (backed up). | | | |
| Network configuration changes have been prohibited. | | | |
| The software version you are migrating to has been downloaded and installed on the Preside Multiservice Data Manager server acting as an SDS. | | | |
| The software version patches to be applied have been downloaded and installed on the Preside Multiservice Data Manager server acting as an SDS. | | | |
| All configuration changes, including patches, from the Global Bulletin System (GBS) and the Method of Procedure (MOP) are reflected on the node and server before performing the upgrade. | | | |
| The file system is organized and the migration operator knows which software versions are applicable to the migration plan. | | | |
| For networks using in-band OAM, is this node a gateway node, or a remote node? | | | |
| The software version currently running on the node is: | | | |
| The current patches running on the node are: | | | |
| The intended software after the migration is: | | | |
| | | | |

| Task | Yes | No | Date and Comments |
|---|---|---|---|
| The software patches you are applying during the upgrade are: | | | |
| The PCRs between the intended software release and the current PCR operating on the node: | | | |
| | | | |

# Downloading and backing up node software

Before you begin your upgrade, ensure that the correct version of Nortel Networks Multiservice Switch/Media Gateway software and the correct patches have been downloaded to the Nortel Networks Preside Multiservice Data Manager (MDM) server acting as the software distribution site (SDS). After verifying that you have the correct software and patches, you can download them to the Multiservice Switch 15000/Media Gateway 15000/20000 nodes. The SDS site must be a Preside MDM server for IP.

## Prerequisites to software download and backup

Review the prerequisites:

- Within the UA-IP solution, one of the Preside MDM servers has been configured as a software distribution site (SDS). The server acting as the SDS manages, stores, and provides access to Multiservice Switch/Media Gateway software and patches. To upgrade a node, download the required software from this server to the nodes.
- Downloading software and patches onto the SDS server, and downloading the software and patches from the server to the nodes can be done at any time prior to the hitless software migration (HSM). Unless there are specific operational requirements, perform these tasks before the upgrade period begins.
- The application version list must contain the following applications: base, networking, atmNetworking, ip, wanDte, ethernet, pvg, and aal1Ces. The application version list must not contain any additional applications.

***Note:*** WanDte is not mandatory for all upgrades. It must only be downloaded and activated in SN07 if it is present in the pre-SN07 release.

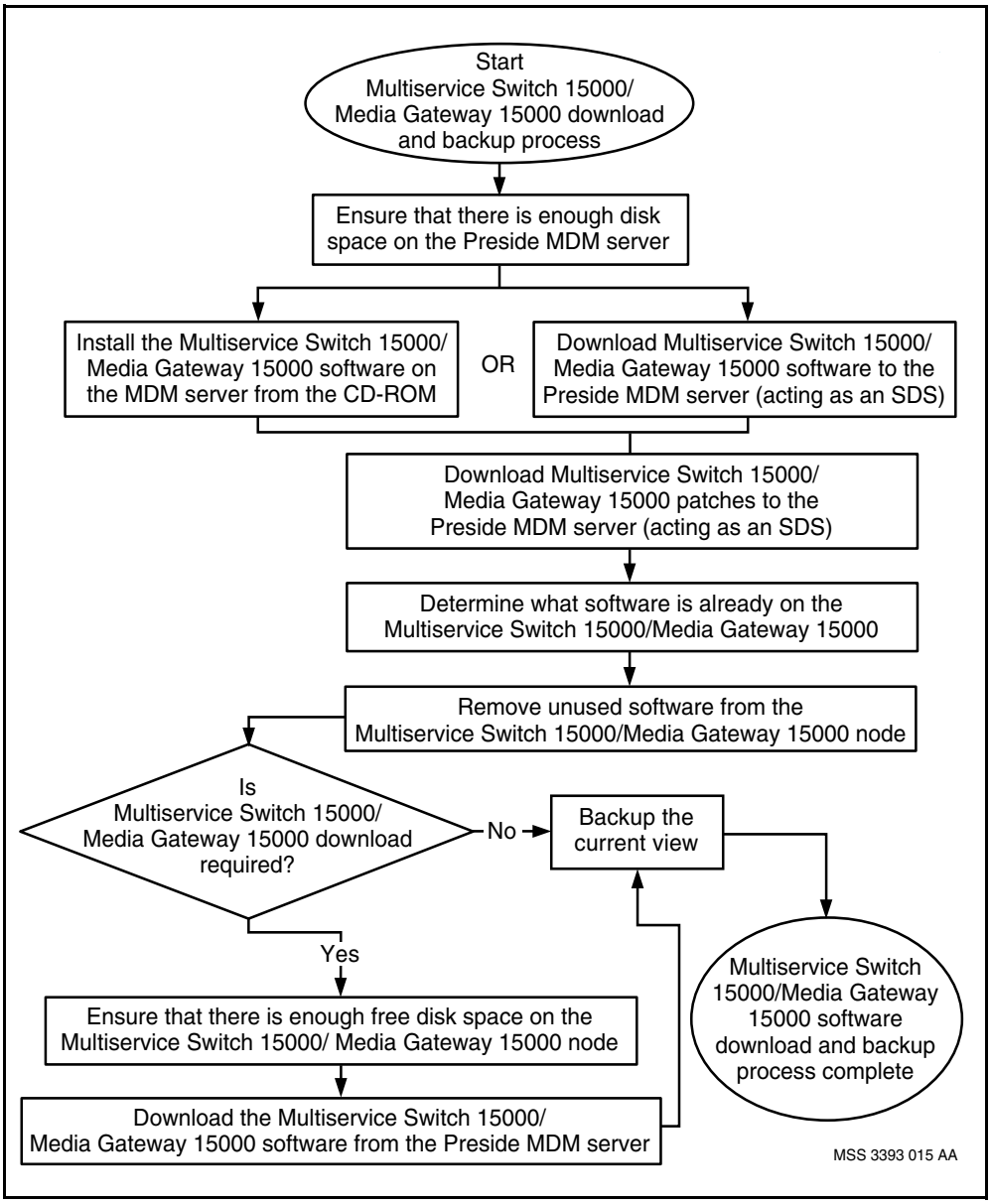
## Software installation and download task flow

The task flow shows the sequence of procedures to perform in order to download software and patches to the server acting as the SDS, and then downloading them to the nodes.

The procedures to configure the server as an SDS, downloading the software and patches to the SDS server, and finally downloading it to the nodes are listed following the Software download and backup task flow on page 447.

These procedures are located in two documents. Four are in this document and the remaining procedures are in the NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation*. To complete this task, perform the procedures in the listed sequence.

### Software download and backup task flow



## Work flow navigation

- Ensuring that there is enough disk space on the server on page 449
- Download the software to the server from Nortel Networks website on page 451
- Download software patches to the server from Nortel Networks website on page 453
- Installing software on the server from CD-ROM on page 455
- “Determining what software is already on the node” in NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation*
- “Removing unused software from the node” in NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation*
- Ensuring that there is enough free space on the node on page 457
- Download software from the Preside MDM server on page 459
- Back up the current view on page 463

# Ensuring that there is enough disk space on the server

Before downloading the required software and patches to the Nortel Networks Preside Multiservice Data Manager (MDM) server acting as the SDS, verify that the server has sufficient disk space.

## Prerequisites

- The software requires approximately 350 Mbytes of space. See *Nortel Networks Multiservice Switch Release Notes PCR6.1* to verify the amount of disk space required by this release.

## Procedure steps

***From the server acting as the SDS***

1 Log in to the Multiservice Switch 15000/Media Gateway 15000/20000 node using the appropriate permissions.

2 Determine how much disk space is available on the partition containing the Nortel Networks Multiservice Switch/Media Gateway software:

**df -k /localdisk/pp15ksw/software**

***Note:*** This directory path assumes that the SDS server user ID configured to access the downloadable has a home directory of /localdisk/pp15ksw. If the user ID has a different home directory, adjust the directory accordingly.

The system indicates (in kilobytes) how much disk space is available in the disk partition.

3 Verify that the space available is more than 350 Mbytes. It is recommended that you have more than the minimum space available.

4 If there is not 350 Mbytes of space, remove files from the SDS server, as required. You can safely remove software from the SDS after all subtending nodes are upgraded to a new release.

Software is located among multiple directories (base, networking, atmNetworking, ip, wanDte, ethernet, pvg, and aal1Ces). Each release subdirectory must be located and

removed. The directory structure on the SDS includes the following directories:

- a user-defined home directory which is the default login directory.

  The home directory must have a subdirectory called software.

- application directories, which contain the software application version directories
- software application version directories, which contain all the control files and object files for a particular version of an application

# Download the software to the server from Nortel Networks website

After verifying that Nortel Networks Preside Multiservice Data Manager (MDM) server acting as the SDS has sufficient disk space, you can begin to download the software from Nortel Networks website. When you download the software from this website, a copy of the software is placed in the directory you specify.

## Prerequisites

- You need a web access account with a user name and password. Contact your Nortel Networks customer representative for more information on accessing the website.
- Refer to the software downloads area of the Nortel Networks website (*www.nortelnetworks.com*) to determine the software load that you must install.
- The software you need to download may be composed of more than one file. Ensure that you download all software files that belong to the release you require.
- After downloading the required software release from the website, you need to download the associated patches.
- Verify which Multiservice Switch software and patches are available on the Preside MDM server.
- Ensure that there is enough disk space on the server.

### *From the server acting as SDS*

1 Login to the server acting as the SDS.

2 On the web, go to *www.nortelnetworks.com*.

3 In the Support section of the window, click *Software Downloads*.

The Software Downloads window opens.

4 Click *Log In*.

5 When prompted, enter your user name and password for the web access login.

6 In the Product Family section of the Software Downloads window, click *Passport*.

The Passport Product Family window opens.

For Multiservice Switch 15000/20000 patches in an UA-IP solution or, to obtain patches for Media Gateway 15000/20000 from SN06 or SN06.2 to SN07 in a PT-IP, PT-AAL2, IAC, or IAW solution network, go to step 7.

7 Under the Passport Packet Voice Gateway (PVG) section, click *Software*.

The software patches you can download are listed.

8 Click the version of the release software you want to download.

***Note:*** The software you want to download may be composed of more than one file. Ensure that you download all software files that belong to the release you require.

The Software Downloads: Software Detail Information window opens.

9 Click the load name listed beside the File Download heading.

A Save As dialog opens.

10 Specify a folder in the user ID home directory of the server to indicate where you want the software placed. This is typically: **/localdisk/pp15ksw/**

11 Click **Save**.

12 On the Preside MDM server, change directories to the directory containing the software (This is the same directory you specified in step 10.):

**cd /localdisk/pp15ksw/**

13 Uncompress the software file:

**uncompress <load_name>.tar.Z**

14 Untar the software file:

**tar -xvf <load_name>.tar**

15 Repeat step 9 through step 14 for every software file you want to download.

16 Remove the tar file.

**Variable values**

| Variable | Value |
|---|---|
| <load_name> | The name of the software load file that you want to download. |

# Download software patches to the server from Nortel Networks website

In addition to the main software release, you may need to download the patches from Nortel Networks website to the Preside Multiservice Data Manager (MDM) server acting as the SDS. When you download the patches from this website, a copy is placed in the specified directory. The SDS site must be a Preside MDM server for IP.

## Prerequisites

- You need an account with a user name and password. Contact your Nortel Networks customer representative for more information on accessing Nortel Networks website.
- Refer to the software downloads area of Nortel Networks website (*www.nortelnetworks.com*) to determine the software patches that you must install. If there are no patches listed for this release, it means that there are no patches currently required for this release.
- Verify which Nortel Networks Multiservice Switch software and patches are available on the Preside MDM server.
- Ensure that there is enough disk space on the server.

### *From the server acting as the SDS*

**1** Log in.

**2** On the web, go to *www.nortelnetworks.com*.

**3** In the Technical Support section of the window, click *Software Downloads*.

The Software Downloads window opens.

**4** Click *Log In*.

**5** When prompted, enter your user name and password for access login.

**6** In the Product Family section of the Software Downloads window, click *Passport*.

The Passport Product Family window opens.

For Multiservice Switch 15000/20000 patches in an UA-IP solution or, to obtain patches for Media Gateway 7480/15000/20000 from SN06 or SN06.2 to SN07 in a PT-IP, PT-AAL2, IAC, or IAW solution network, go to step 7.

**7** Under the Passport Packet Voice Gateway (PVG) section, click *Software*.

The software patches you can download are listed.

8 Click the patch that you want to download.

The Software Downloads: Software Detail Information window opens.

***Note:*** If there are no patches listed for this release, it means that there are no patches currently required for this release. You can move on to the next task in the upgrade process.

9 Click the patch name listed beside the File Download heading.

10 A Save As dialog is displayed.

11 Specify a folder in the home directory of the MDM user to indicate where you want the patch placed. This is typically: */localdisk/pp15ksw/*

12 Click *Save*.

13 On the Preside MDM server, change directories to the directory containing the patch (This is the same directory you specified in step 11.):

**cd /localdisk/pp15ksw/**

14 Uncompress the patch file:

**uncompress <patch_name>.tar.Z**

15 Untar the patch:

**tar -xvf <patch_name>.tar**

16 Repeat step 8 through step 15 for every patch you need.

17 Remove the tar file.

### Variable values

| Variable | Value |
|---|---|
| <patch_name> | The name of the patch that you want to download. |

# Installing software on the server from CD-ROM

An alternative to downloading Nortel Networks Multiservice Switch/Media Gateway software from the server acting as the SDS, is to install it from the CD-ROM using the installation program.

## Prerequisites

- You need a copy of Nortel Networks Multiservice Switch PCR6.1 software CD. Contact your Nortel Networks customer representative for information on how to order a CD.
- You need the IP address of the Nortel Networks Preside Multiservice Data Manager (MDM) server acting as the SDS.
- After installing the required software release from the CD-ROM you need to download the required patches. For more information, see Download software patches to the server from Nortel Networks website on page 453.

## Installing software

### *From the server acting as SDS*

1 Login.

2 Insert the software CD in the server's CD-ROM drive.

3 Create a directory for mounting the CD:

**cd /**

**mkdir /cdrom**

***Note:*** If the mountable CDs have been used for other applications, you may not have to create this directory.

4 Start the installation program:

**/cdrom/cdrom0/install**

5 Follow the installation program's prompts.

6 When the installation program prompts you for a product, select Passport 15000.

7 When the installation program prompts you, select Install software.

8 When the installation program prompts you for a directory in which to place the software, type the following:

**/localdisk/pp15ksw/**

The installation program indicates when the installation is complete. At this time, the software has been installed in the

directory you defined when prompted by the installation program.

9 Once the software has been successfully installed, log back into the server acting as the SDS.

10 Eject the CD from the CD-ROM drive: **eject cdrom**

## Ensuring that there is enough free space on the node

Before downloading software and patches to the node, ensure that the node has sufficient disk space for the software applications that you need.

### Prerequisites

- Ensure that there is sufficient space to download the software files for the following applications: base, networking, atmNetworking, ip, wanDte, ethernet, pvg, and aal1Ces. The amount of space required for the eight applications is approximately 350 Mbyte.

  ***Note:*** WanDte is not mandatory for all upgrades. It must only be downloaded and activated in SN07 if it is present in the pre-SN07 release.

- If you need to upgrade the fabric card firmware with this release, you also need to download the fabric application. Allocate additional space for this application.
- If you need to download patches, allocate additional space for the patches.
- See Nortel Networks Multiservice Switch Release Notes *PCR6.1* and the software downloads area of Nortel Networks website (*www.nortelnetworks.com*) to determine the software load and patches that you must install, and the amount of disk space required for them. See the section on determining which software is already on the node in NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation*.

***From the node***

1 Log in to the Multiservice Switch 15000/Media Gateway 15000/20000 node using the appropriate permissions.

2 Determine the space currently available on the file system:
**display FileSystem freeSpace**

The number of bytes available on the system is displayed.

3 Verify that the space available is more than 350 Mbyte.

***Note:*** If you need to install patches, you need to allocate additional space for the patches.

4 If the file system does not have enough available space, remove any unused software and provisioning files. See the section on

removing unused software in NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation*.

***Note:*** Removing unused software will usually free up sufficient disk space. However, it is possible that a significant amount of disk space is being used by spooling files if they are not being removed often enough by the Management Data Provider (MDP). If this is the case, use MDP to retrieve and delete spooling files. See 241-6001-309 *Preside MDM Management Data Provider User Guide*.

## Download software from the Preside MDM server

Before beginning the hitless software migration (HSM), you need to download the software from the Nortel Networks Preside Multiservice Data Manager (MDM) server acting as the SDS for the nodes.

### Prerequisites

- Download the software to the server from Nortel Networks website on page 451
- Download software patches to the server from Nortel Networks website on page 453
- You have performed the procedure “Ensuring that there is enough free space on the file system” see NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation*
- Download the software files for the following applications: base, networking, atmNetworking, ip, wanDte, ethernet, pvg, and aal1Ces.

  ***Note:*** WanDte is not mandatory for all upgrades. It must only be downloaded and activated in SN07 if it is present in the pre-SN07 release.

- If you need to upgrade the fabric card firmware with this release, you will also need to download the fabric application. For more information, see Upgrade the fabric on page 1279.
- Refer to the software downloads area of Nortel Networks website (*www.nortelnetworks.com*) to determine the software load and patches that you must install. If there are no patches listed for this release, it means that there are no patches currently required for this release.
- You need the IP address of the Preside MDM server acting as the SDS.
- You need the user ID that has read access to the software on the SDS server, and the associated password for that user ID. This is the user ID for the folder specified in step 10 of Download the software to the server from Nortel Networks website on page 451.
- Use the Preside MDM server Command Console tool to perform this upgrade. For more information on opening the Command Console, see 241-6001-804 *Preside MDM Workstation Utilities User Guide*.

***From the node***

1 Login with the appropriate permissions.

***Note:*** You need a user ID with a minimum command scope of *device* and a command impact of *configuration*.

2 Verify that the downloader is inactive:

**display Software Download status**

The value of the *status* attribute must be inactive.

3 Set the processor target type for the application versions:

**set Software Download processorTargets PPC i960**

4 Create the list of software applications that you need to download:

**set Software Download avListToDownload ! <application_versions>**

You must download the software files for the following applications:

- base_CF01xxx
- networking_CF01xxx
- atmNetworking_CF01xxx
- ip_CF01xxx
- wanDte_CF01xxx

***Note:*** WanDte is not mandatory for all upgrades. It must only be downloaded and activated in SN07 if it is present in the pre-SN07 release.

- ethernet_CF01xxx
- pvg_CF01xxx
- aal1Ces_CF01xxx
- fabric_CF01xxx (only if a fabric upgrade is necessary)
- patch_CF01xxx

***Note:*** You can only download patch_CF01xxx if the switch is already at SN07, or if patch baseFT420A_XXXX is

active on the shelf. See step 8 in Perform HSM using Command Console on page 1263.

The node downloads any patches associated with the application versions you specify.

If you are upgrading a Media Gateway 15000/20000 from SN06 or SN06.2 to SN07 in a PT-IP, PT-AAL2, IAC, or IAW solution network, note the following:

— If the Media Gateway 15000/20000 shelf includes 4pGigE Function Processors (4pGe FP), and you are upgrading from SN06.2, ensure that patch baseFT397A_CE02S2D has been activated on the shelf prior to performing the HSM to SN07. Refer to Bulletin 2004005174 for further information about this patch.

— If you do not have any 4pGigE Function Processors (product code NTHW49AA) installed in the Media Gateway15000/20000 shelf, review Upgrading Multiservice Switch 15000/Media Gateway 15000 in Succession Networks (UA-IP) on page 1231 to see a description of HSM on Media Gateway 15000/20000. From the command console enter the list of pre-check commands provided in the procedure Verify the status of the node before the upgrade on page 1237 to ensure that no components are degraded or disabled prior to HSM.

— If your Media Gateway 15000/20000 network includes the 4pGe FP at SN06, please contact your Nortel account representative to request a similar patch for SN06 prior to performing an HSM to SN07.

**5** Verify that the software applications that you want to download are in the list of software that will be downloaded:

**display Software Download avListToDownload**

**6** Start downloading the software:

**start -host(<ipAddress>) -user(<userId>) -password(<password>) Software Download**

The download process begins.

**7** Monitor the progress of the download:

**display Software Download**

When the *status* attribute is *inactive* and the *filesToTransfer* attribute is *0*, the download is complete.

**8** Verify that the software listed in step 4 was downloaded:

**list Software ApplicationVersion/***

9 Verify that the patches listed in the software downloads area of Nortel Networks website (*www.nortelnetworks.com*) were downloaded:

**list Software ApplicationVersion/* Patch/***

**Variable values**

| Variable | Value |
|---|---|
| <application_versions> | A space-separated, case sensitive list of application versions.<br><br>You must download the new version of the base, networking, atmNetworking, ip, wanDte, ethernet, pvg, and aal1Ces applications.<br><br>*Note*: WanDte is not mandatory for all upgrades. It must only be downloaded and activated in SN07 if it is present in the pre-SN07 release.<br><br>If you need to upgrade the fabric card firmware with this release, you will also need to download the fabric application. For more information, see Upgrade the fabric on page 1279. |
| i960 | An attribute indicating that the i960 processor type is being used. This attribute is always required. |
| <ipAddress> | The IP address of the Preside MDM SDS server. |
| <password> | The password for the, <userID> on the Preside MDM SDS server. |
| PPC | An attribute indicating that the PowerPC processor type is being used. This attribute is always required. |
| <userID> | The user ID for server account that contains software to be downloaded. The value is usually pp15ksw. |

## Back up the current view

Save a current view from a node using Nortel Networks Preside Multiservice Data Manager (MDM) Service Data Backup/Restore tool. This tool copies service data and application version information from the node to a reliable data storage site. This view can be used to restore provisioning on a node in case of file corruption.

### Prerequisites

- The view to be saved must be either a committed or portable view.
- You must have write permissions on the node, with a minimum impact of service, a minimum scope of device, and a minimum access of ftp and fmip.
- The backup site can be the Preside MDM server or another Nortel Networks Multiservice Switch node. It can also be a Software Distribution Site (SDS) configured to store backed-up service data from a node.
- Verify that the backup site has enough space to accommodate the backup. For more information, see NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software*.
- The Service Data Backup/ Restore tool uses the */tmp* directory to perform some of its file processing (for example, archive, compress, and uncompress). Your local disk needs to have twice the amount of space as the actual size of the files you are transferring for back up. You need to clean up the local disk if errors are raised (for example, *"No space left on device")*. In this case, you can mount the */tmp* directory from a lower-usage disk on a selected file server.
- The Service Data Backup/ Restore tool backs up only the node's configuration data. It does not back up node software.
- The Backup server, the Restore server, the Nortel Networks Multiservice Switch 15000 Backup provider, and the Nortel Networks Multiservice Switch 15000 restore provider must all be running on the Preside MDM server in order for the Service Data Backup/Restore tool to function properly. Using the Preside MDM Server Administration tool, verify that these four servers are running. If they are not or if you need more information, see 241-6001-807 *Preside MDM Network Backup and Restore*.
- Using the **display -o prov** command, ensure that the committed view, the current view, the edit view, and the last used view are identical. If these views are not the same, see NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation* for information on making them the same.

- The Preside MDM server has been configured to regularly back up the provisioning files from the nodes. By creating a backup of the committed file before beginning the upgrade, you ensure that you have the most current committed file you can have before beginning the migration.
- If a view is not saved prior to an upgrade attempt and you have to revert to a previous software load, then you must re-configure the old software release manually.
- If you need to revert to a saved view of an older software version, when the node restarts it restarts in the operational state it was in when you saved that view.



**CAUTION**

This procedure backs up all views currently stored on each node and should be done during a maintenance window.

***Procedure steps***

**1** Login to a Preside MDM server.

**2** Open a Preside MDM window:

**/opt/MagellanNMS/bin/nmstool &**

The copyright dialog and the Preside MDM window open.

**3** Click **OK** to close the copyright dialog.

**4** From the Preside MDM window, select Configuration > Passport > Administration > Passport Service Data Backup/Restore.

The Passport Service Data Backup/Restore window opens.

**5** Select the **Add ...** button.

**6** Select the device(s) to be backed up by selecting the groups and/or nodes located in the Device Groups panel.

**7** From the popup menu, select the value **full** to ensure that the default for the backup is to do a full backup and not an incremental one.

**8** Enter the appropriate user ID and password to authenticate for the selected device(s).

**9** Click **OK**.

The added devices now appear in the **Device List** of the main Passport Backup and Restore window.

**10** Click **Backup** to start the backup procedure for all the devices listed in the **Device List**.

This will proceed to backup all the views currently stored on each node, and should be done during a maintenance window.

**11** Alternatively, specific views can be backed up as follows. For each device in the Device List:

- change the parameter under the Mode column from **full** to **selective**.
- select the specific view to backup from the Configuration column.
- click **Backup** to start the backup of the selected view for each node in the **Device List**.

# Preparing to upgrade CICM

This document provides the upgrade strategy for the Centrex IP Client Manager (CICM) 7.11, and upgrade procedures for the CICM Element Manager and CICM nodes.

## Introduction

The upgrade strategy for the Centrex IP Client Manager Series 7.11 is summarized as follows:

- The upgrade of CICM Series 6.12 to CICM Series 7.11 software is performed by Nortel Networks installers only. The Telco CICM administrators will not perform this upgrade.
- Before the CICM is upgraded, the CS2M, Core and GWC is upgraded according to CS2K guidelines.
- MR upgrades for the EM and CICM nodes may be performed by Telco CICM administrators. The EM and CICM MR procedures are provided in this document.
- The following 3 upgrades are supported for this 7.11 release:
  - The software-only upgrade from CICM 6.12 to 7.11 on Hardware Revision B.
  - Upgrade from CICM 6.12 / Hardware Revision B to 7.11 / Hardware Revision C
  - Upgrade from CICM 2.5 / Hardware Revision B to 7.11 / Hardware Revision B
- For any upgrades prior to 6.12 (such as Series 2.4 to Series 2.5), refer to the *Upgrades* section of the CICM 2.5 and CICM 2.4 versions of the *NN10044-111 CICM Product and Technology Fundamentals* document.

### Software version

The software applies independently to both the CICM and the Element Manager, although both should have the same version once an upgrade is completed.

The software version has the following format:
**<Release number>.<build number>**

**Example**
7.11.148
The release number is 7.11
The build number is 148

## Product and Maintenance Release upgrades

There are two types of upgrades: product upgrades and Maintenance Release (MR) upgrades.

### Product upgrades

Product upgrades involve upgrading the release number. For this release, the release number is increased from 6.12 to 7.11. The two product upgrade procedures performed by Nortel Networks installers are:

- Perform an EM 6.12 to 7.11 product upgrade
- Perform a CICM 6.12 to 7.11 product upgrade

Since these product upgrades are performed by Nortel Networks installers only, and not Telco CICM administrators, these upgrade procedures are not included in this document.

### Maintenance Release (MR) upgrades

Maintenance Release upgrades involve build number upgrades, within the same release. With this type of upgrade, the build number is increased. For a 7.11 release, the MR changes the software version build number from 7.11.xxx to 7.11.yyy.

For this release, the following MR upgrade procedures are applicable and included in this document:

- Perform an EM 7.11 MR upgrade
- Perform a CICM 7.11 MR upgrade

Although there are no 7.11 MR upgrades released as of this document publication date, MR upgrades will be made available on CDs and on the CICM-EM Web site as they are released.

## In-service MR upgrades

An in-service MR upgrade process with a minimal outage strategy is utilized for CICM Series 7.11 MR upgrades. This minimal outage upgrade strategy involves the following:

- The Terminal Handover feature can be used to transfer active terminals from the node being upgraded to the mate node.
- Terminals connected to the node being upgraded will suffer an outage while they locate the mate node.
- Active calls using resources on the node being upgraded will be lost.
- The call capacity of the CICM being upgraded is reduced by half.
- EM upgrades have no service impact.

### MR upgrade implementation guidelines

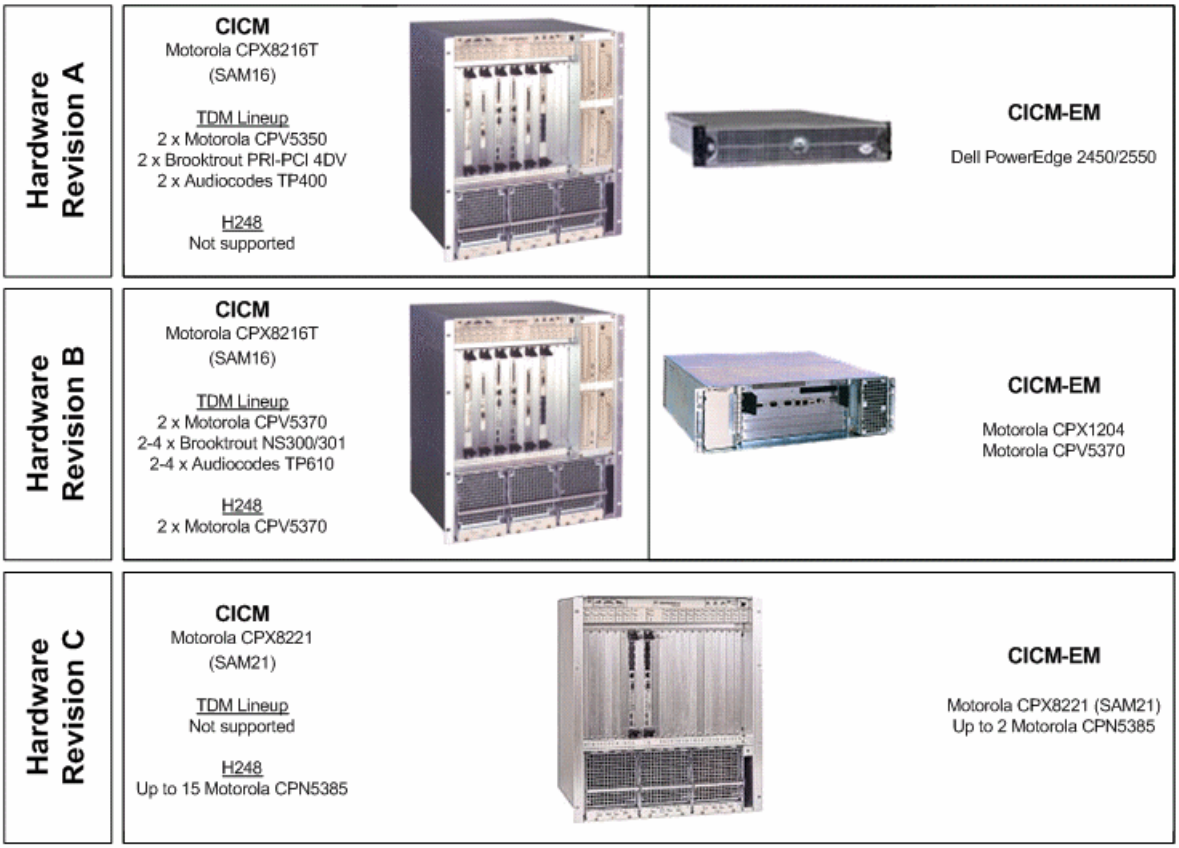
The guidelines for implementing upgrades are:

- Special instructions may be provided in the release notes for Maintenance Release upgrades. It is required to read the release notes prior to upgrade.
- The order of upgrades is: EM, then CICM nodes, then terminals. If a primary and backup EM pair are deployed, both EM(s) must be upgraded prior to the first CICM node upgrade.
  Note: Terminal upgrades are not addressed in this document. Refer to the *NN10027-113 CICM Series 6.12 Etherset Installation Guide and User Manual*, and the *NN10182-113 CICM Series 6.12 m6350 Client Installation Guide.*
- Each node of the CICM is upgraded individually. However, paired nodes should be upgraded to the same software version. Running paired nodes at different versions for extended periods can result in degradation in performance or behavior.
- Configuration changes should not be made during the upgrade.
- The upgrade should be performed during the lowest call traffic period to minimize impact on users.
- The upgrade will take one to two hours to complete.
  Note: Service degradation (call capacity reduction) only occurs for various segments of the upgrade period.
- Resource utilization (i.e. active call count) can be monitored via the Element Manager Web pages. (For MR upgrades only; not applicable to product upgrades.)
- For all procedures provided in this document, it is required to use administrator userids and passwords to login to the Element Manager.

### Hardware review

The following figure shows the hardware revisions available for the TDM and the H.248/Succession versions of the CICM product, for both the CICM Element Manager (CICM-EM) and the CICM gateway itself (CICM). The CICM 7.11 release is supported on a Motorola CPN5385 card mounted on a SAM21 chassis, for new installations (Revision C in Figure 1), and is supported on a Motorola CPV5370 card mounted on a SAM16 chassis, for upgrades (Revision B in Figure 1).

**Figure 1 Hardware revision summary**




## Software review

The following table shows the software versions available for the TDM and the H.248/Succession CICM product, for both the CICM-EM and the CICM itself. The table shows the hardware revisions corresponding to each version of the software, as well as the operating systems each CICM component runs on.

| Version | Supported Hardware Revisions | CICM Operating System | CICM-EM Operating System |
|---|---|---|---|
| 2.0, 2.1, 2.2 (TDM only) | A | Windows NT Embedded | Windows NT Server |
| 2.4, 2.5 (TDM only) | A, B | Windows NT Embedded | Windows NT Server (HW Rev A) Windows 2000 Server (HW Rev B) |

| Version | Supported Hardware Revisions | CICM Operating System | CICM-EM Operating System |
|---|---|---|---|
| 6.12/SN06.2 (H.248 Only) | B | Windows NT Embedded | Windows 2000 Server |
| 7.11/SN07 (H.248 Only) | B, C | Windows XP Embedded | Windows 2000 Server |

***Note 1:*** Although limitations exist, the choice of a particular hardware revision for the CICM does not necessarily limit the choice for the CICM-EM to the same hardware revision, and vice versa.

***Note 2:*** 7.11 CICM-EMs will support 6.12 CICMs.

***Note 3:*** Old hardware revisions are only supported for upgrades; they are no longer part of the current portfolio.

Although in general a given version of the CICM-EM is not backward-compatible with all the older versions of the CICM, a 7.11 CICM-EM can manage a 6.12 CICM. The process of a 6.12 CICM upgrade to 7.11 will be driven by a 7.11 CICM-EM, as the following upgrade sections assume.

Although details are provided for different upgrade paths, the main focus of this upgrade document is the software upgrade of a 6.12 CICM on Hardware Revision B to version 7.11.

## Software ordering process

CICM software is ordered from Nortel Networks via the standard software ordering process. Refer to the CICM Software Release Lineup table below for the Series 7.11 software ordering codes.

**Table 1 CICM Software Release Lineup**

| NCL/MNCL Order Codes | Description |
|---|---|
| CICM0071 | CentrexIP Client Manager Gateway |
| CICMM071<br>CICEM071 | CentrexIP Client Manager Gateway Maintenance Release<br><br>CDROM containing the latest MR release. |

**Table 1 CICM Software Release Lineup**

| NCL/MNCL Order Codes | Description |
|---|---|
| CICE0071 | CentrexIP Client Manager Element Manager Installation Maintenance Release CDROM |
| CICI0071 | CentrexIP M6350 SoftClient Installation Download from <http://www.nortelnetworks.com/centrexip> |
| CIVP0024 | CXIP Backup/Restore Tool (BRT) CDROM |

## CICM 7.11 Overview

The 7.11 CICM release aligns with the SN07 Succession Release. The 7.11 CICM gateway supports only H.248 signalling (i.e. to and from an SN07 gateway controller), which means it does not support the older DMSX/TDM signalling interface.

This CICM 7.11 product release introduces:

- A new hardware line-up (Revision C hardware)
- A new operating system for the CICM gateway (Windows XP Embedded)
- An improved network redundancy model
- Network boot capabilities (for Revision C hardware only)

All new installations of CICM 7.11 use Hardware Revision C, which specifically means:

- Both the CICM software and the CICM-EM run on Motorola CPN5385 CPU cards
- Both cards are mounted on a Motorola CPX8221 (SAM21) chassis.

CICM 7.12 development is ongoing, and will be released as an additional feature pack to provide post-FCS feature content.

### Supported upgrades

The following upgrades are supported for this CICM 7.11 release:

- The software-only upgrade from Succession Release 6.12/CICM 6.12 to 7.11 on Hardware Revision B.
- Upgrade from CICM 6.12 / Hardware Revision B to 7.11 / Hardware Revision C
- The conversion from TDM: The upgrade from CICM 2.5 / Hardware Revision B to 7.11 / Hardware Revision B

The following table summarizes the supported upgrade paths for both software-only and software/hardware upgrades.

**Table 2 Summary of supported upgrades to CICM 7.11**

| From | CICM 7.11 Hardware Revision B | CICM 7.11 Hardware Revision C |
|---|---|---|
| CICM 2.5 Hardware Rev A | Not supported | Not supported |
| CICM 2.5 Hardware Rev B | Supported | Not supported |
| CICM 6.12 Hardware Rev B | Supported | Supported |

***Note:*** The upgrade of a 2.5 CICM to 7.11 is only supported as a software upgrade. In this case, both the original and the target configurations must be on Hardware Revision B. The migration from a 2.5 CICM on Hardware Revision B to 7.11 on Hardware Revision C is therefore considered a new installation.

### Upgrade the CICM network identity

As part of the upgrade from 6.12 to 7.11, the CICM nodes are re-assigned internally a new network identity. The following table gives

an example of how the CICM network identities change during the upgrade, specifying which steps of the process actually impact them.

**Table 3 Internal network identity during upgrade process**

| Upgrade Step | Node A | | Node B | |
|---|---|---|---|---|
| | Network Identity | Admin IP Address | Network Identity | Admin IP Address |
| Start | 6.12 CICM | 47.165.169.110 | 6.12 CICM node B | 47.165.169.115 |
| Re-image node A to 7.11 | N/A | N/A | 6.12 CICM node B | 47.165.169.115 |
| Configure node A as 7.11 CICM node A | 7.11 CICM node A | 47.165.169.120 | 6.12 CICM node B | 47.165.169.115 |
| Re-image node B to 7.11 | 7.11 CICM node A | 47.165.169.120 | N/A | N/A |
| Configure node B as 7.11 node B | 7.11 CICM node A | 47.165.169.120 | 7.11 CICM node B | 47.165.169.125 |

## Upgrade strategy

### Before the CICM is upgraded

The following steps are required before the CICM is upgraded:

- Upgrade the CS2M, Core and GWC according to CS2k guidelines.
- Upgrade the CICM-EM to 7.11
- Create a new GWC profile for the SN07 CICM. Maintain the old profile still as back-up for backward compatibility.
- Check the number of spare TPs/endpoints on the GWC. (Additional GWC may be needed during the upgrade, depending on the capacity.)

  ***Note:*** The number of physical terminations (TPs or “endpoints”) on a given SN07 GWC is limited to 8200. A 6.12 CICM requires 1023 TPs, whereas a 7.11 CICM will need up to 3069. Given that the CICM operates in split mode during an upgrade, this means that up to an additional 3069 TPs must be available on the same GWC for the upgrade itself to be carried out. If this is not the case, an extra GWC is required. However, the actual number of TPs used by a 7.11 CICM can be chosen as a multiple of 1023. This

way the TPs overhead can be kept to a minimum during the upgrade (i.e. 1023); then they can be increased at a later stage, with no impact on the service provided.

- Pre-provision the new CICM LENS on the core and GWC.

### During the upgrade

During the upgrade, the CICM hardware is split. The following strategy is followed during the upgrade:

- The primary node is created with the new CS2k network identity.
- The secondary node continues to run the simplex 6.12 load.
- The new CICM node shares the same network identity towards its terminals, so they do not need to be reprogrammed. However, during the upgrade process, the primary node is temporarily configured with a different identity (Unistim IP address), to prevent terminals on the secondary node from re-connecting, and to allow for preliminary testing.

### After the primary CICM node has been upgraded

After the primary CICM node has been upgraded, the following:

- The LENS are migrated from one CICM to the other (the split CICM has two CS2k identities).
- Call processing stops on the secondary node. The terminals are out of service.
- The network identity towards the terminals is restored on the primary node, and the terminals are handed over from the secondary node.

  ***Note:*** The secondary CICM node will perform the handover to the primary CICM node, even though they are not a mated pair.

- Call processing becomes active on the primary node. The terminals are returned to service.
- The secondary node is taken out of service and upgraded, to become the new mate to the primary (with the new CS2k network identity).

## Upgrade sequence

### CICM-EM Upgrade sequence

Due to the internal changes to the Operating System used by the CICM-EM from 6.12 to 7.11, it is not possible to perform a standard EM upgrade, which normally does not require the nodes to be re-imaged.

However, this has no impact on the service provided, as the CICM-EM is not a Call Processing node.

The basic CICM-EM upgrade sequence for 7.11 is:

- Save the Primary Element Manager (PEM) configuration (Perform online backup). Duration: 1 minute

  ***Note:*** This is the final configuration for the paired Element Managers, once the upgrade is completed.

- Take an image-backup using the CICM Backup & Restore tool (CICM BRT). Duration: 1 5 minutes
- Re-image the PEM node from the 7.11 CD. Duration: 10 minutes
- Restore the PEM configuration (online backup). Duration: 1 minute
- Verify that the PEM is fully operational. If this is not the case, restore the configuration, using the CICM Backup & Restore tool.
- Re-image the BEM node from the 7.11 CD. Duration: 10 minutes
- Perform a background synchronization between PEM and BEM of the configuration data. Duration: 5 minutes

***Note:*** The total CICM-EM upgrade time is approximately 35 minutes.

### Upgrade Sequence 1: Split CICM

This section, and the two following sections, detail the steps required to upgrade a 6.12 CICM node on Hardware Revision B (SAM16 chassis), to a 7.11 version of the software, retaining the same hardware.

***Note 1:*** All of the EM-driven operations are carried out using a 7.11 CICM-EM.

***Note 2:*** Service-affecting steps have the note “Service Affecting,” with a description of the service impact.

The upgrade sequence to split the CICM is:

- Any terminals connected to node A are handed over to Node B. Duration: 10-15 minutes
  Service Affecting: Minor loss of service. The duration of the terminal handover process is user-definable. Typical shutdown timeouts range from 10 minutes to a few hours, depending on the telco needs. The minor loss of service is due to the terminals being

forcibly moved from one node to another at the end of the timeout, which may result in calls being dropped, and in reduced capacity.

- Backup the CICM-100 data (user & terminal configuration) to the CICM-EM (stored in a file on the CICM-EM). Duration: 5 minutes
- If required, perform SWACT from the CICM-EM to ensure node B is the master. Duration: 1 minute
- Take an image backup using the CICM BRT. Duration: 5 minutes

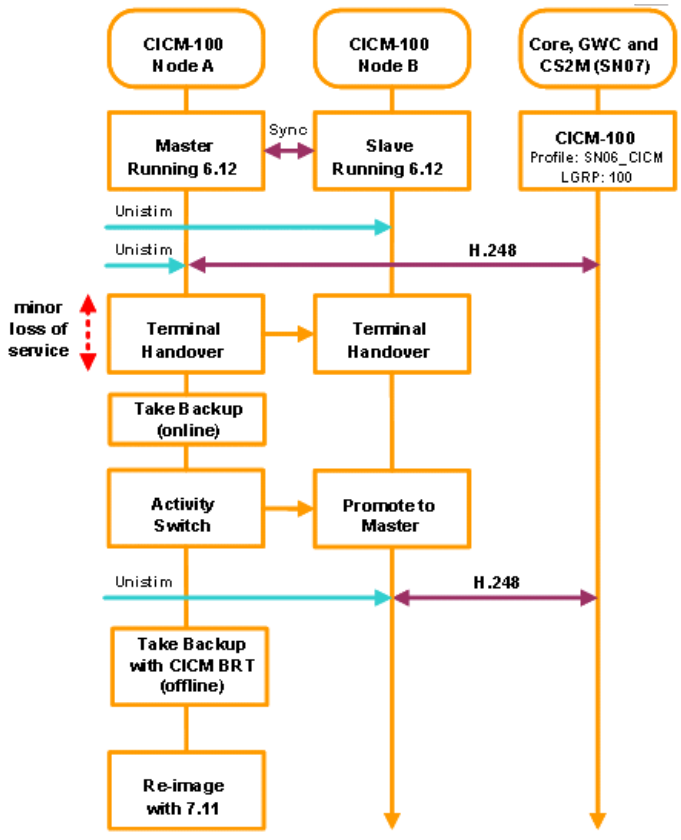
  ***Note:*** This backup can be used to re-image node A back to version 6.12, prior to upgrading node B, if back-out is required.

- Re-image Node A from the CD. Duration: 10 minutes

***Note:*** Any subsequent configuration changes made to node B will be lost.

The upgrade sequence to bring node A to version 7.11 is summarized in the following figure.

**Figure 2 Upgrade sequence to bring node A to version 7.11**



### Upgrade Sequence 2: New CICM RTS

The sequence for returning the CICM to service is:

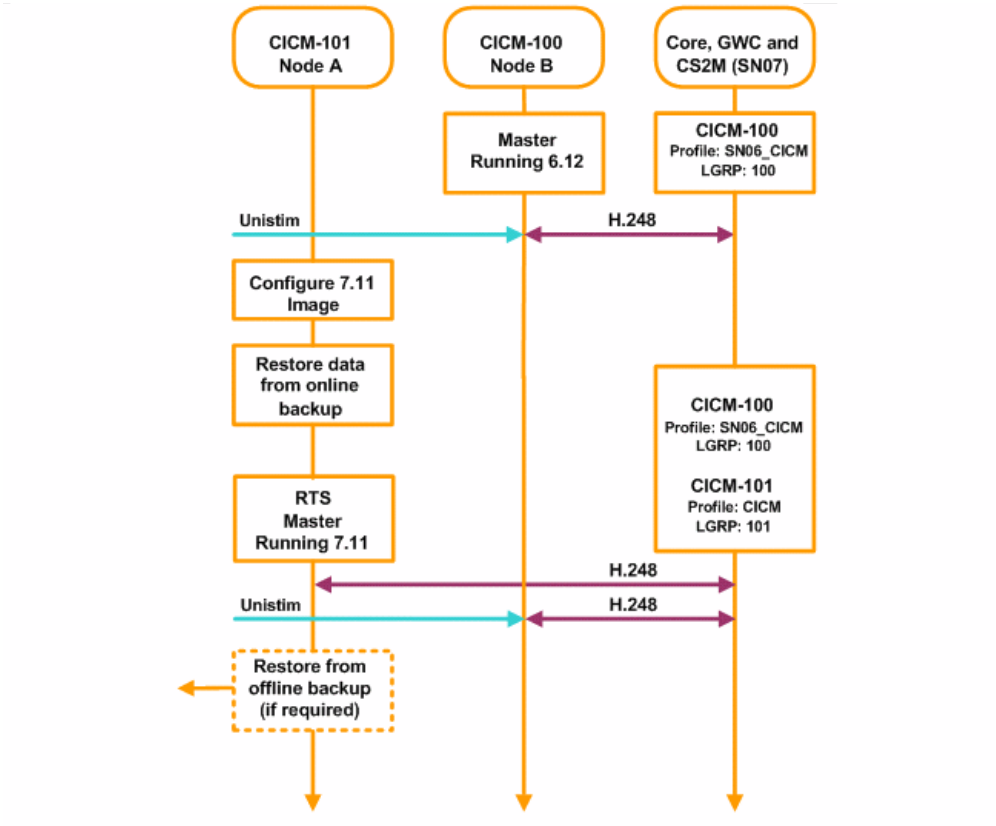
- Configure CICM-101-A as a 7.11 CICM Duration: 10 minutes
- CICM-100-B remains in service (simplex)
- CICM-100-B and CICM-101-A will have different network identities towards the terminals (Unistim IP address), so that the interface can be kept enabled during the upgrade. The new Unistim identity of node A is chosen during the configuration of the 7.11 image, (i.e. prior to restoring the user & terminal data).
- CICM-100-B and CICM-101-A have also different network identities for OAMP and GWC.
- The new LENS is pre-provisioned for CICM-101 on CS2M, Core and GWC.
- User & terminal data is restored from the CICM-EM after configuration of CICM-101-A. Duration: 5 minutes
- CICM-101-A is Returned To Service. Duration: 5 minutes
- Conduct preliminary tests on CICM-101-A9. Duration: variable

  ***Note:*** At this stage, the two halves differ with respect to both network identity and terminal network identity (Unistim IP address).

- If back-out is required, the CICM BRT can be used to restore the image-backup at this time.

The following figure summarizes the upgrade sequence to return node A to service.

**Figure 3 Upgrade sequence to return node A to service**




### Upgrade Sequence 3: Transferring control

The Upgrade sequence 3 for transferring control is as follows:

- Transfer the core line datafill from CICM-100 to CICM-101. Duration: 10 minutes]
- Restore the network interface towards the terminals (Unistim IP address) of CICM-101-A to its original value. Duration: less than 1 minute
- Hand over the terminals from CICM-100-B to CICM-101-A. Duration:10-15 minutes

> ***Note:*** The duration of the terminal handover process is user-definable, and typical shutdown timeouts range from 10-15 minutes to a few hours, depending on the customer needs. This operation causes a minor loss of service, because the terminals are forcibly moved from one node to another at the end of the timeout (which may result in calls being dropped). Capacity may be reduced.

- Terminals are handed over from CICM-100-B to CICM-101-A. Duration: 10-15 minutes

  ***Note:*** The duration of the terminal handover process is user-definable, and typical shutdown timeouts range from 10-15 minutes to a few hours, depending on the customer needs. This operation causes a minor loss of service, because of the terminals being forcibly moved from one node to another at the end of the aforementioned timeout (which may result in calls being dropped), and of course in terms of reduced overall capacity.

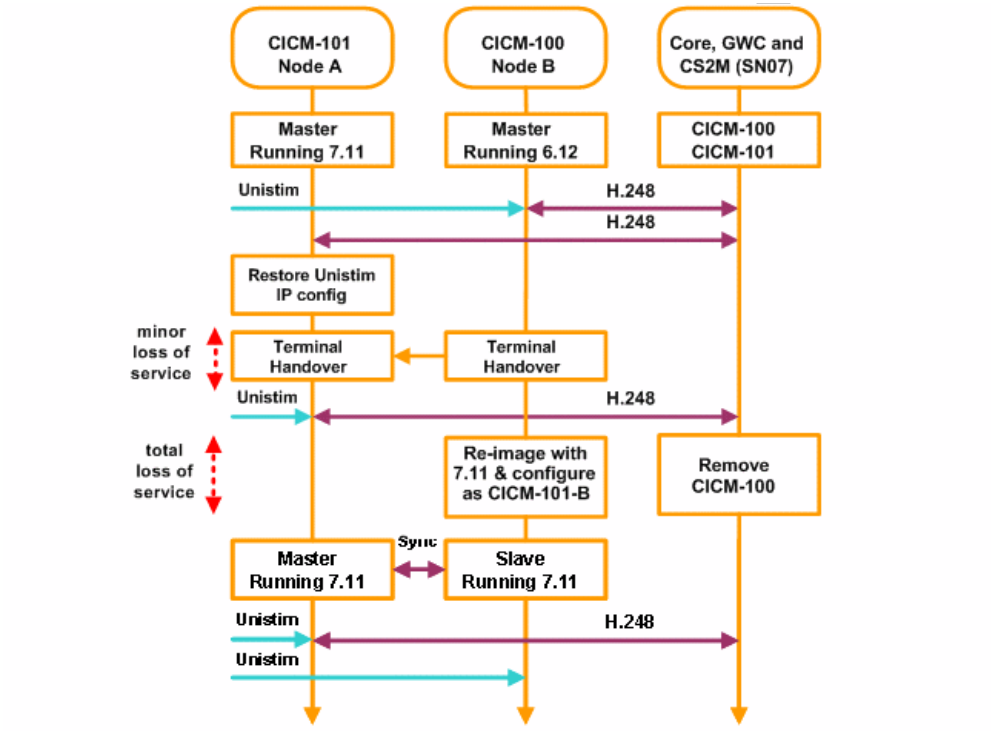
- Upgrade CICM-100-B to 7.11 software load through CD re-image, then configure as CICM-101-B. Duration: 10 + 10 minutes
- Provide CICM-101-B with a new (external) network identity. Duration: 10 minutes

  ***Note:*** Providing the whole CICM with a new network identity at the GWC and CS2M levels causes a total loss of service, in that no calls can complete while the datafill of the core is in progress. However, this step can be carried out simultaneously with the previous one to reduce the overall upgrade time. This step has no impact on the internal network identity, changed during the previous step (which re-defines it as CICM-101-B).

- The CICM-101 is now in service. in duplex mode.

The following figure summarizes the upgrade sequence to bring node B to version 7.11

**Figure 4 Upgrade sequence to bring node B to version 7.11**




## Upgrade sanity

This section details the sanity tests that can be performed during the CICM upgrade process described in the Upgrade Strategy section above, and performed by Nortel Support personnel.

### In-upgrade tests

At the end of the upgrade sequence presented above, CICM-101-A will be fully in service in simplex mode (single 7.11 node). To verify that this is the case, and before proceeding with the upgrade of CICM-100-B, it is advisable to run some preliminary tests, as in the following procedure.

**Procedure 1 Perform in-upgrade test**

***On the core***

1 Create new LENS associated with the CICM-100 identity (profile SN06_CICM).

2 Associate CICM users on CICM-100-B.

3 Verify CallP formally added users.

4 Verify that the new LENs can be moved over the CICM-101 (profile (CICM).

5 Associate CICM users on CICM-101-A.

6 Verify CallP for newly added users.

### Post-upgrade tests

Upon completion of the overall CICM upgrade, CICM-101 should be fully in service in duplex mode (dual 7.11 node). To verify that this is the case, it is advisable to run some tests, as in the following procedure.

**Procedure 2 Perform post-upgrade tests**

***On the Core***

1 Create new LENs associated with the CICM-101 identity (profile CICM).

2 Associate CICM users on CICM-101.

3 Verify CallP for newly added users.

4 Verify locally-hosted calls for CICM-101-A.

5 Verify locally-hosted calls for CICM-101-B.

6 Verify cross-hosted calls for CICM-101.

7 Perform a SWACT and repeat the three tests above.

8 Increase the number of endpoints allocated on the GWC to 3069.

## 7.11 Upgrade issues

This section summarizes the limitations and restrictions of the upgrade process.

### Non-upward compatible software changes

The improved network redundancy model prevents half 6.12 / half 7.11 dual node operation during upgrade. This means that, although the two halves co-exist in the same CICM chassis, they operate as a “split node” (as opposed to being a dual node pair).

The main implications of operating as a split node are:

- The nodes have different network identities: different IP Admin address pairs

  ***Note:*** As part of the upgrade from 6.12 to 7.11, the CICM nodes are re-assigned a new network identity. However, the operator is still allowed to accidentally configure node A to be node B’s mate node, in other words to act as a 7.11 Slave node for a 6.12 Master. As the consequences of such mis-configuration would be far reaching, a minor change is implemented so that, in the event of

CICM versions mismatch, the presence of the mate node will be disregarded.

- Both nodes operate as Master, as they cannot detect each other's presence in the network
- The nodes do not provide any redundancy towards networks or node failures (i.e. no SWACTs or "Hot Takeovers" are possible.)
- Neither the node's MIBs nor their H.248 layers are synchronized.

### Changes to the Succession environment

Changes to the upgrade process in the Succession environment are:

- SESM based line provisioning proxy intercepts the SERVORD commands.
- There is a new CICM profile in the GWC (the old profile is renamed SN06_CICM).
- LENs are pre-provisioned using the new CICM specific line group type "M."
- Pre-provisioning of 3 blocks of 1023 terminations per CICM.

### Service impacts and upgrade times

The following table provides an estimate of the service impacts which result from the upgrade process described above. Total outage time: 10 minutes

**Table 4 Summary of the service-affecting upgrade steps**

| Upgrade Step | Estimated Duration | Loss of Service | Service Impact |
|---|---|---|---|
| Terminal handover from CICM-100-A to CICM-100-B | 10-15 min | minor | • Calls dropping on originating node on expiration of shutdown timeout<br>• Reduced capacity |
| Terminal handover from CICM-100-B to CICM-100-A | 10-15 min | minor | • Calls dropping on originating node on expiration of shutdown timeout<br>• Reduced capacity |
| New network identity for CICM-100-B (datafill GWC/CS2M) | 10 min | major | • Terminal connectivity enabled but no Call Processing available on either node |

The following table provides an estimate of the overall duration for each of the CICM upgrade sequences described above. Total upgrade time (CICM) 105 minutes

**Table 5 Upgrade Times Summary**

| Upgrade Sequence | Estimated Duration |
|---|---|
| Sequence 1: Split CICM | 35 min |
| Sequence 2: New CICM RTS | 20 min |
| Sequence 3: Transferring Control | 55 min |

# Ensuring patch currency

## How to check for the latest patches

Ensure that your baseline software is patch current and then that you have SN07 patches prior to starting the upgrade.

1) Go to http://www.nortelnetworks.com.

2) Click "Software Downloads".

3) Click "Browse product support".

4) Go to major heading "Succession Communication Server 2000".

5) Go to minor heading "Succession Communication Server 2000".

6) Click "Tools".

### To query for (i)SN07 patches

1) Click "Pre Upgrade Patch Calculator".

2) Click "Pre Upgrade Patch Calculator Readme[readme]" for instructions.

Also refer to Succession patching on page 1636.

### To query for patches for your baseline software

1) Click "Patch Audit for Inform Lists".

2) Click "Patch Audit User Guide [readme]" for instructions.

3) Click "Patch Audit Application".

4) Enter path and filename of the inform list from site (or use Browse to find the file).

## Patch order

Refer to Succession patching on page 1636.

## Patching procedures

Refer to Succession patching on page 1636.

# Upgrade backups

For the list of backups to perform as part of advance preparations for end-to-end upgrade, refer to *Global Administration and Security*, NN10402-600.

# Hardware baseline check

For the hardware baseline for your solution, contact customer service for a copy of the *Voice over IP Solution Specification*.



Copyright © 2005, Nortel Networks


# Upgrading IP Solutions

**ATTENTION**
The following sections contain Succession upgrades procedures only. To roll back an upgrade, refer to the component upgrades NTP.

When performing an upgrade, complete the three-tiered process of preparation, upgrade, and post upgrade tasks for each individual component in the order described in the appropriate diagram for your upgrade in the section End-to-end upgrade overview on page 1. After completing the three-tiered process for one component, continue the process for the next component in order.

***Note:*** This Succession Networks upgrade document addresses all IP solutions. Please disregard information about components that do not apply to your solution.

# Upgrading Preside MDM

## Preside MDM software installation

This module contains:

- Prerequisites to installing Preside MDM software on page 489
- Preside MDM software installation task flow on page 490



**CAUTION**
**This upgrade strategy removes network management equipment from service.**
This upgrade strategy removes the servers from service and eliminates server redundancy.

After you shut down the servers and software on this Preside MDM server, communication from this server to the CS2000 Core Manager or IEMS, and the Multiservice Switch network stops. The other Preside MDM server reports alarms as long as the server being upgraded is out of service.

Load balancing between Preside MDM servers is not available and the Preside MDM platform compliance to connectivity standards cannot be met during the upgrade.

The Succession MDM Software Migration window opens displaying the current MDM release.

## Prerequisites to installing Preside MDM software

Before installing new Nortel Networks Preside Multiservice Data Manager (MDM) software and patches, review the following points:

- The upgrade procedure uses the software installation tools and procedures that are packaged with Preside Multiservice Data Manager 15.1 release. Preside MDM software will not support copying the software, configuration, or data from one server to the other. This approach would cause Preside MDM references and process calls to fail.
- You must have extensive knowledge of Unix and Preside MDM tools and software.
- Review the *Preside Multiservice Data Manager Release 15.1 Supplement*. The release supplement describes the features that are new to the software release and includes information on

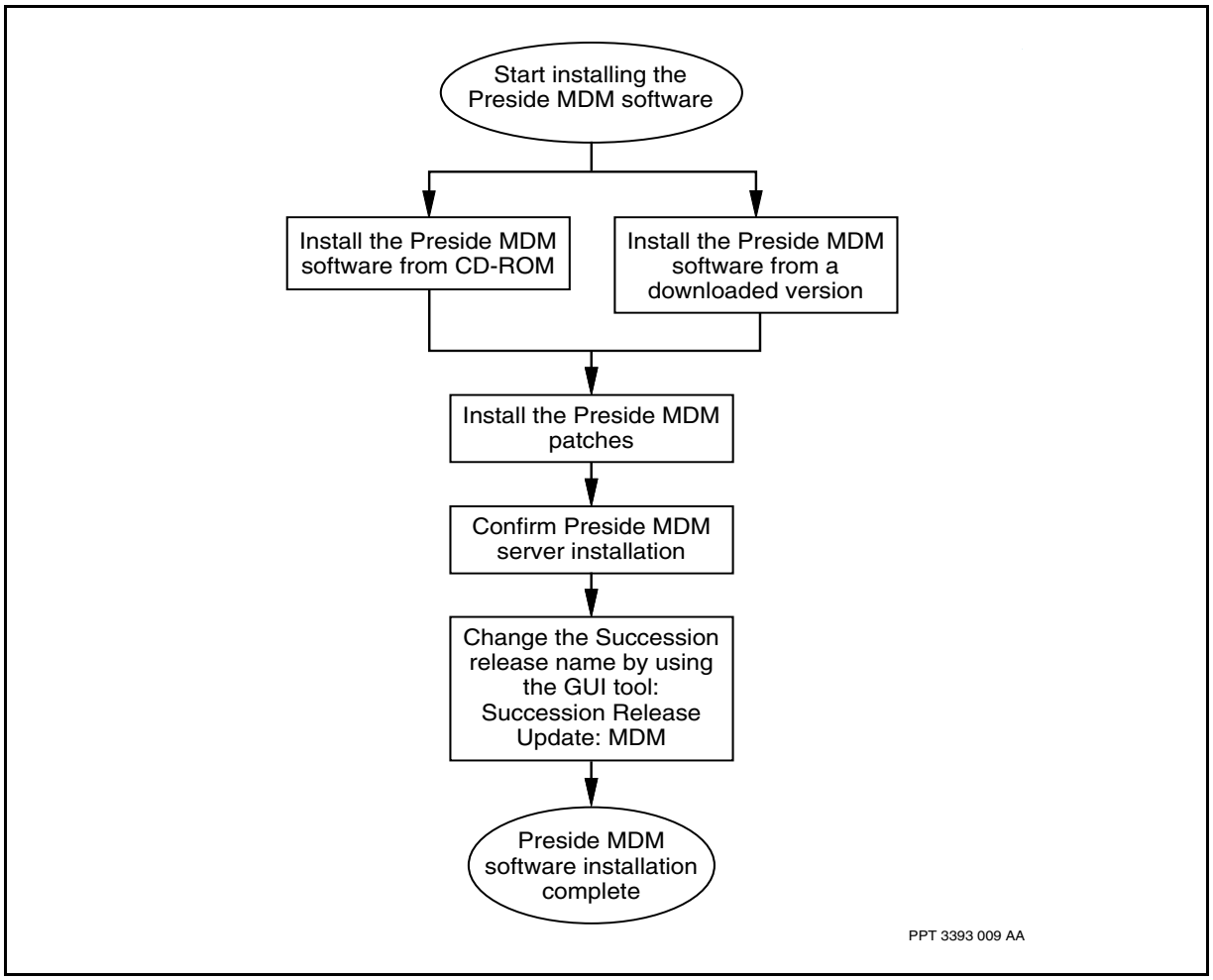
differences in functionality and capability from the old release to the new release. It is essential that you understand the potential impacts before beginning the upgrade.

- You need a Preside Multiservice Data Manager 15.1 software license. If you do not have the license, you will need to order one. Contact your Nortel Networks Sales Representative for additional information.
- Ensure you have performed the procedure: Downloading Preside MDM software from Nortel Networks website on page 155.
- If you are upgrading Preside MDM servers from CD-ROM, you must have an X11 terminal with IP connectivity to the Sun Fire ™ V480 server that you are upgrading. If using a CD to perform the upgrade, you must have access to the CD ROM drive. If upgrading from software that you download from Nortel Networks Electronic Software Distribution (ESD) page, you only need access to the downloaded file. You must also have access to a text editor so that you can edit various files during the upgrade. We recommend using the UNIX VI text editor.

## Preside MDM software installation task flow

The following figure shows you the sequence of procedures you need to perform to install new Nortel Networks Preside Multiservice Data Manager (MDM) software and patches. To link to any procedure, go to the list that follows the task flow chart.

**Figure 1 Preside MDM software installation task flow**




Click on the following links to access the procedure:

- Installing Preside MDM software from a CD-ROM on page 491
- Installing Preside MDM software release from a downloaded software version on page 494
- Installing Preside MDM patches on page 496
- Confirming successful Preside MDM server installation on page 499
- Setting Succession release name identification on page 499

## Installing Preside MDM software from a CD-ROM

Begin installing Nortel Networks Preside Multiservice Data Manager (MDM) software by installing the Preside MDM and MDP software packages using the InstallAnywhere program. The Preside MDM

software installation takes up to 45 minutes depending on the server hardware and packages you are installing. The InstallAnywhere program removes files that need to be removed before loading the new software. The system retains the previous version of Preside MDM software on the server as a back-up while installing the new version.

Preside MDM data configuration is persistent. As a result, you will not lose your configuration data when Preside MDM data packages are deleted.

### Prerequisites

- If you have already downloaded the software as described in Preparing for Preside MDM software migration on page 149, do not perform this procedure. Perform the procedure: Installing Preside MDM software release from a downloaded software version on page 494.

  ***Note:*** For more information, see 241-6001-100 *Preside MDM Installation*.

***From the Preside MDM server***

1 Login - see Logging into Preside MDM servers on page 522.

2 Insert the *Multiservice Data Manager 15.1 Software Disk 1 of 3* CD in the server's CD-ROM drive.

3 Open a Unix window.

4 Create a directory for mounting the CD:

**cd /**

**mkdir /cdrom**

***Note:*** If mountable CDs have been used in the past for other applications, you may not have to create this directory.

5 Stop the MDP servers. If you are running release MDM 14.2, use the command: **mdpadm stop all**

***Note:*** This command must be executed using the mdpadmin user ID.

If you are running release MDM 14.3 or higher then go to step 6. The **nmssvm.server stop** command stops MDM servers and the MDP servers that are defined in the Server Administration tool.

6 Stop the Preside MDM servers:

**/etc/init.d/nmssvm.server stop**

7 Start the installer:

**/cdrom/cdrom0/install_mdm**

The system indicates that it is launching the installer.

8 Enter the environment **DISPLAY** to launch the MDM Installer GUI. If the local IP address is not already populated as the default, enter the local IP address. The command "echo DISPLAY" will show this value. Set the display in the following format: **<IP address>:0.0**

9 Use the following default values required by Succession when prompted. For more information about installation, see 241-6001-100 *Preside MDM Installation*.

| Install panel | Options |
|---|---|
| Installation Option Panel | Select MDM and MDP. |
| Installation Source Path | `/cdrom/cdrom0` |
| Current domain name (refer to Example Old file on page 493) | <domain name required to locate the Preside MDM workstation> |
| MDP User/group info | Provide the user name, password, and UNIX group for MDP.<br>***Note:*** These values are customer dependent. |
| NV Background Pix Maps | No |

***Note 1:*** During the installation, you will be prompted to enter CD 2. Before inserting CD 2, eject CD 1 by issuing the eject command in the terminal window. Before inserting CD 3, eject CD 2 by issuing the eject command in the terminal window.

***Note 2:*** If the Preside MDM workstation does not belong to a domain, you must assign a domain name in the **/etc/hosts** file. Refer to the following example:

**Example**

Old file

**# Internet host table**

**127.0.0.1 localhost**

**10.17.1.2 MDM01 loghost**

Modified file

**# Internet host table**

**127.0.0.1 localhost**

**10.17.1.2 MDM01 MDM01.XYZ.COM loghost**

In the example, **10.17.1.2** represents the local workstation IP address and **XYZ.COM** represents the domain name.

**10** To ensure that all changes have been applied, synchronize the file systems by issuing the sync command three times, pressing Enter after each one.

**sync**

**sync**

**sync**

**11** Return the server to service and apply the changes by rebooting it:

**init 6**

After the reboot, the server should return to service without any problems.

**12** Eject CD 3.

## Installing Preside MDM software release from a downloaded software version

Begin installing Nortel Networks Preside Multiservice Data Manager (MDM) and MDP software packages using the InstallAnywhere program.

The installation of Preside MDM software takes up to 45 minutes depending on the server hardware and the packages you are installing. The InstallAnywhere program removes files that need to be removed before loading the new software.The system retains the previous version of Preside MDM software on the server as a back-up while installing the new version.

Preside MDM configuration data is persistent. As a result, you will not lose your configuration data when Preside MDM packages are deleted. For more information about installing Preside MDM software, see 241-6001-100 *Preside MDM Installation*.

### Prerequisites

- Access the software either by Downloading Preside MDM software from Nortel Networks website on page 155 or, Retrieving Preside MDM software and patches from a drop box on page 154.
- Make a note of the directory name where the software that you downloaded or retrieved was placed.
- Refer to the software downloads area of Nortel Networks website (*www.nortelnetworks.com) to determine the software load and patches that you need. If there are no patches listed for this release, it means that there are no patches currently required for this release.*

***From the Preside MDM server***

1 Login - see Logging into Preside MDM servers on page 522.

2 Open a Unix window or terminal.

3 Change directories to the directory containing the software that you downloaded in Downloading Preside MDM software from Nortel Networks website on page 155.

4 Stop the MDP servers. If you are running release MDM 14.2, use the command: **mdpadm stop all**

***Note:*** This command must be executed using the mdpadmin user ID.

If you are running release MDM 14.3 or higher, use the Server Administration tool to stop the MDP servers.

5 Stop the Preside MDM servers:

**/etc/init.d/nmssvm.server stop**

6 Start the installer: **./install_mdm**

The system indicates that it is launching the installer.

7 Use the following default values required by Succession when prompted. For more information about installation, see 241-6001-100 *Preside MDM Installation*.

| Install Panel | Options |
|---|---|
| Installation Option Panel | Select MDM and MDP. |
| Installation Source Path | /MDM151 |
| | |

| Install Panel | Options |
|---|---|
| Current domain name | <domain name required to locate the Preside MDM workstation> |
| MDP User/group info | Provide the user name, password, and UNIX group for MDP.<br>***Note:*** These values are customer dependent. If MDP is already installed, this information is not required. |
| MDM Operator Client and User Administration | Do not select this option. |
| NV Background Pix Maps | No |

8 Click *Done* to exit the installer window when the install is complete.

9 To ensure that all changes have been applied, synchronize the file systems by issuing the sync after each one:

**sync**

**sync**

**sync**

10 Return the server to service and apply the changes by rebooting it:

**init 6**

After the reboot, the Preside MDM server should return to service without any problems.

## Installing Preside MDM patches

After installing Nortel Networks Preside Multiservice Data Manager (MDM) software, you need to install the patches on the server.

Preside MDM patches are jumbo patches that include all previous patches. As a result, only install the most current versions of each of the patches you need. You cannot install multiple versions of the same patch since you must remove the older version of a patch before you can install a newer version.

The following procedure uses a Preside MDM patch as an example. Repeat the procedure for all the patches that you need installed.

### Prerequisites

- You must have performed the procedure Installing Preside MDM software from a CD-ROM on page 491 or Installing Preside MDM software release from a downloaded software version on page 494.
- Refer to the software downloads area of Nortel Networks website (*www.nortelnetworks.com*) to determine which patches you need to install. If there are no patches listed for this release, it means that there are no patches currently required for this release.
- See Downloading Preside MDM software from Nortel Networks website on page 155 to download the required Preside MDM patches.

***From the Preside MDM server***

1 Login - see Logging into Preside MDM servers on page 522.

2 Display the patches that are currently installed on the system:

**cd /var/sadm/patch**

**ls**

***Note:*** This step and the next two steps are not required if you are performing this procedure immediately after a software migration because there are no previously installed patches.

3 If there are any patches for previous releases listed, uninstall them. Uninstall the patches from the highest (numerically) to the lowest.

**patchrm <patch_name>**

4 When you are prompted to either reboot, re-initialize the NMS servers, or do nothing, choose to do nothing.

***Note:*** Do not reboot the server at this time. You will reboot the server after completely installing the new patches.

5 Change directories to the *patch151* directory:

**cd /patch151**

***Note:*** The *patch151* directory was created in step 3 of Downloading Preside MDM software from Nortel Networks website on page 155. Record the location where you downloaded the patches, if it is not the temporary directory.

6 Display the available patches:

**ls**

7 Using the software downloads area of Nortel Networks website (*www.nortelnetworks.com), determine which patches you need to install. There could be up to three patches to install: MDM, MDP, and DVR.*

8 Uncompress the first patch that you need:

**uncompress <patch_name>.tar.Z**

9 Untar the patch:

**tar xvf <patch_name>.tar**

10 Remove the tar file:

**rm -r <swload_name>.tar**

11 Change directories to the specific patch subdirectory:

**cd /patch151/<patch_name>**

12 In that subdirectory, open the README file associated with the patch and follow the instructions to install the patch.

***Note:*** In the README file, ignore the steps that have you uncompress, tar and reboot.

13 Repeat steps 8 through step 12 for each of the patches you need to install.

14 To ensure that all changes have been applied, synchronize the file systems by issuing the sync command three times, pressing Enter after each one:

**sync**

**sync**

**sync**

15 Return the server to service and apply the changes by rebooting it:

**init 6**

After the reboot, the Preside MDM server should return to service without any problem.

**Table 1 Variable values**

| Variable | Value |
|---|---|
| <patch_name> | The name of the patch that you want to remove or install. The patch names have the MDM, MDP, or DVR release number followed by the patch number. For example, MDM151-01. |

## Confirming successful Preside MDM server installation

After installing Nortel Networks Preside Multiservice Data Manager (MDM) server software and patches, you need to confirm that the installation was successful. Perform the checks found in Post-migration checks on page 1389.

## Setting Succession release name identification

To help identify which Succession release the MDM and Multiservice Switch 15000 are running, and help operators determine if these elements are compatible with other elements in the Succession network, the MDM 15.1 toolset allows you to set the Succession release name on the MDM tool launcher and to modify the *commentText* field of the Multiservice Switch 15000 shelf component. (The *commentText* field contains release and load information).

For Multiservice Switch 15000/Media Gateway 15000 in a VoIP network, the Succession release name can be added through the MDM toolset. However, for Multiservice Switch 15000 in Core ATM networks, migration is done through the Succession ATM Software Migration (SASM) tool. The SASM tool uses Network Activation Tool (NAT) with pre-scripts and post-scripts to validate the health of the Multiservice Switch 15000 before and after the migration. The SASM post script prompts the operator performing the migration to enter the Succession release name.

Perform the procedures:

- Setting the Succession release name on MDM on page 500
- Setting the Succession release name for Multiservice Switch 15000/ Media Gateway 15000 in VoIP on page 502 or,
- Setting the Succession release name for Multiservice Switch 15000 in VoA on page 505

### Prerequisites

- the file /opt/MagellanNMS/cfg/.SuccessionEnabled must exist

### Procedure 1 Setting the Succession release name on MDM

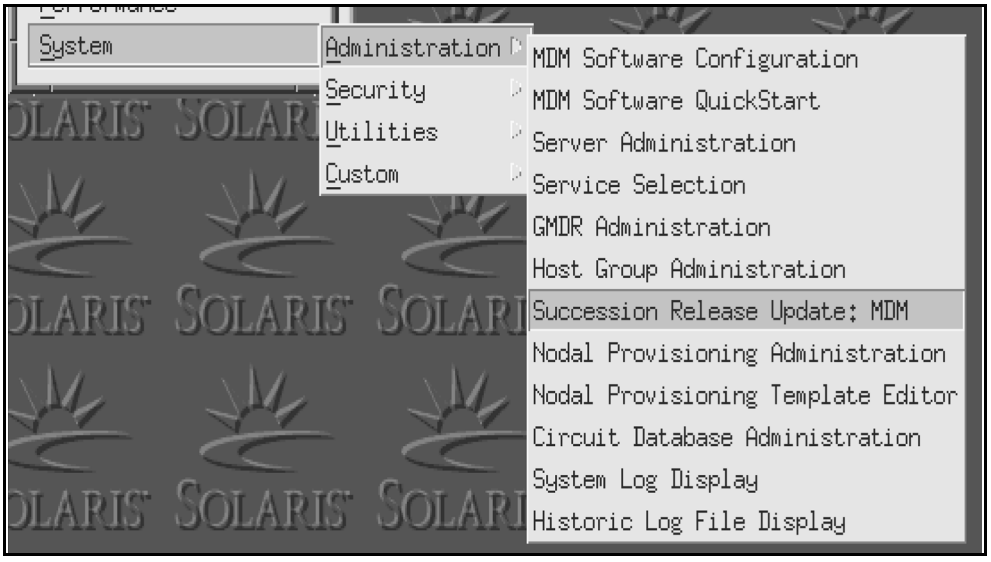
***From the Preside MDM server***

**1** Login - see Logging into Preside MDM servers on page 522.

**2** From the Preside MDM window, choose System > Administration > Succession Release Update: MDM.

The Succession MDM Software Migration window opens and displays the current MDM release.

**Figure 2**



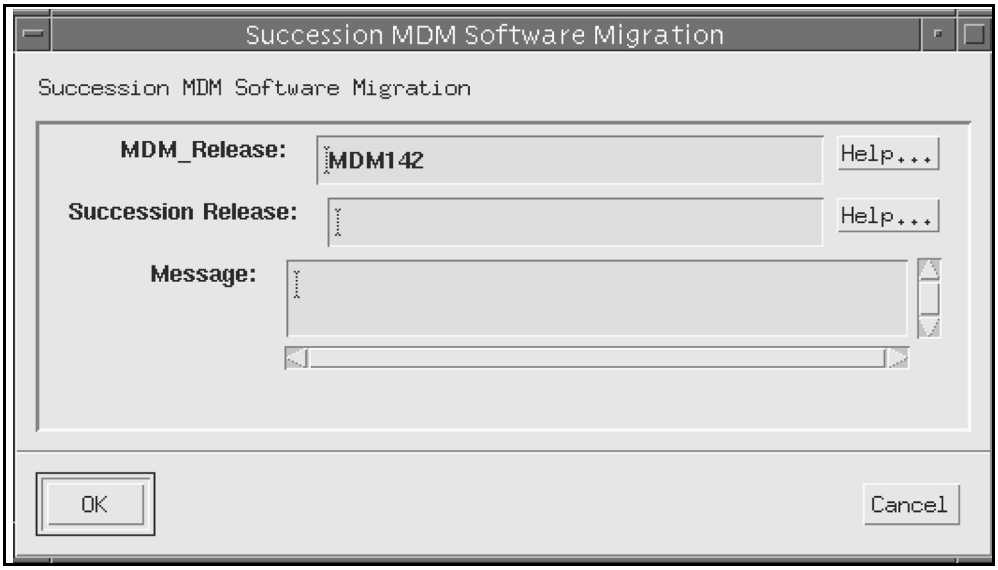

***Note:*** The *file .SuccessionEnabled* is normally created in the */opt/MagellanNMS/cfg/* directory during installation. If the file does not exist, login as root and create it as follows:

**touch /opt/MagellanNMS/cfg/.SuccessionEnabled**

The *.SuccessionEnabled* file does not require any data within it.

**3** Enter the Succession release name using the format: SNxx.y For example: SN06.2 or SN07.

The Succession MDM Software Migration window opens displaying the current MDM release.




**4** Click *OK* and exit and restart the MDM GUI.

The file */opt/MagellanNMS/system/info/release.name* is changed and the MDM toolset icon displays the MDM release name followed by the Succession release name.

If you click *Cancel*, the process is cancelled and the file opt/MagellanNMS/system/info/release.name is unchanged. If nothing is entered into the Succession release field, the information is removed from the MDM toolset.

**Figure 3 MDM toolset menu after modification**



## Setting the Succession release name for Multiservice Switch 15000/Media Gateway 15000 in VoIP

The *commentText* field of the Multiservice Switch 15000/Media Gateway 15000 shelf component contains record release and load information. When upgrading nodes in a Succession network, you can change the node *Shelf CommentText* attribute using the MDM toolset, or run the *Set Shelf CommentText* command to change the attribute information. See NN10070-461 *Upgrading Nortel Networks Multiservice Switch 15000 in Succession Networks PT-AAL1/UA-AAL1* for information about the Set Shelf CommentText command.

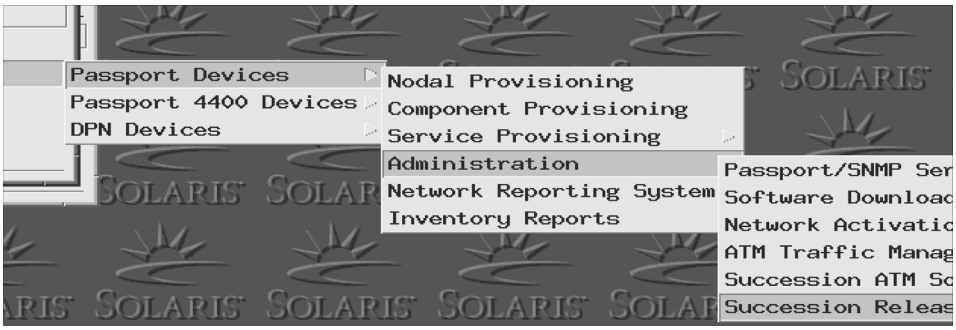
### Procedure 2 Setting the Succession release name for Multiservice Switch 15000/ Media Gateway 15000 in VoIP

***From the Preside MDM server***

1 Login - see Logging into Preside MDM servers on page 522.

2 From the Preside MDM window, choose:

Configuration > Passport > Administration > Succession Release Update: Passport.




Initial screen for setting the Media Gateway 15000/Media Gateway 15000 shelf display.

3 Select the Multiservice Switch 15000//Media Gateway 15000 element name.

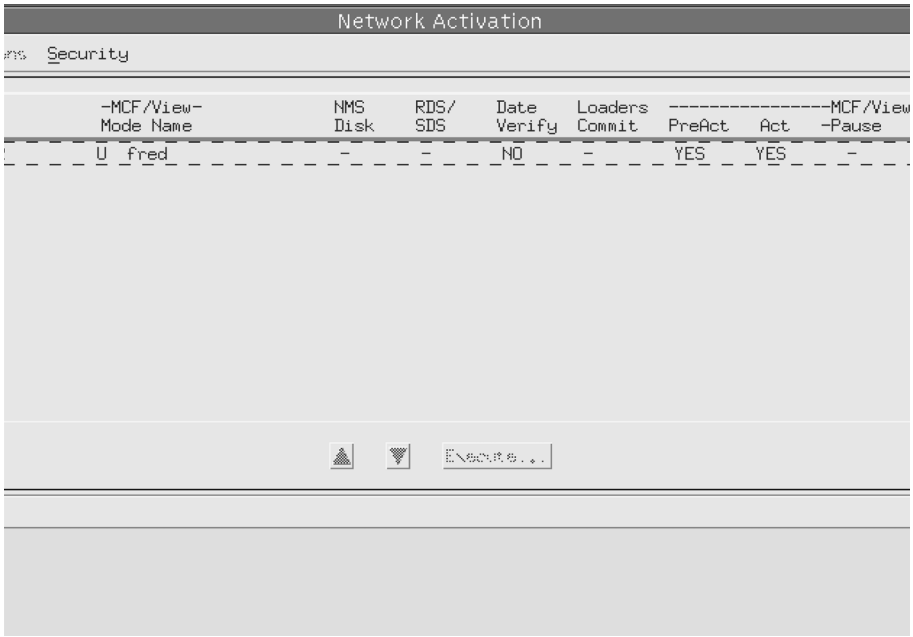



**4** Select the View name.

This is the Multiservice Switch 15000/Media Gateway 15000 element name and View name where the provisioning will be saved.

**5** Click *OK*.

The Network Activation tool (NAT) starts.



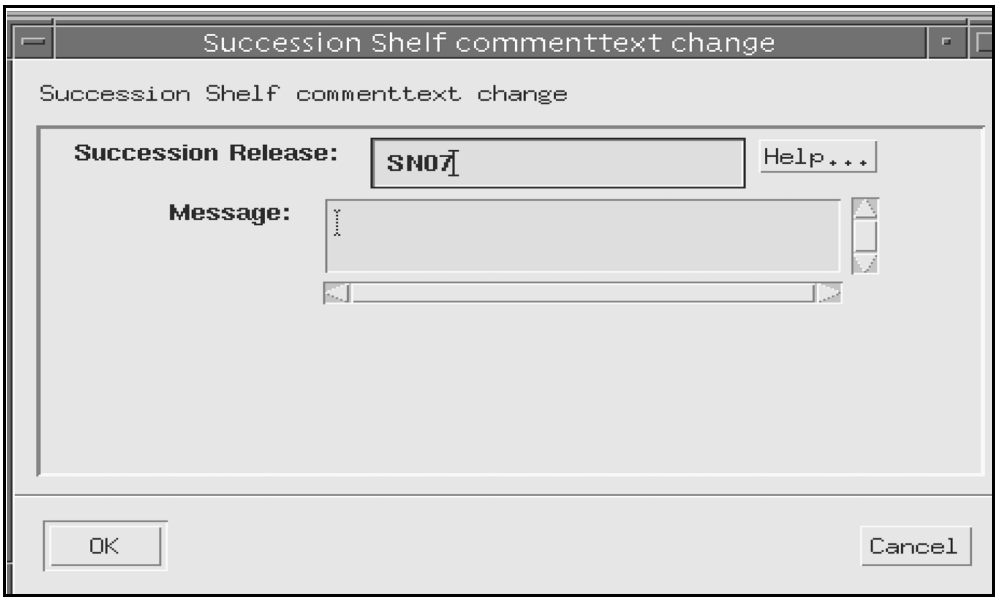
6 Enter the group name (or select) a Multiservice Switch 15000/Media Gateway 15000 group that has configuration privileges.

7 Choose "Group Authentication" under "Security." You must choose the Destination and enter the Userid/Password for the 15K you are authenticating.

8 Click *Execute*.

After you execute the NAT record, The Succession Shelf comment text change window opens. Use the window to enter the new Succession release number.

Use the format: SNxx.y (for example, SN06.2 or SN07) as shown in the example.




***Note:*** To verify that the Succession Release name was added, in the MDM GUI select *Fault*, then *Passport Shelf View* and then click *Shelf*.

9 Click *OK*.

The Multiservice Switch 15000/Media Gateway 15000 *Shelf CommentText* attribute on the target node is updated with the Succession release name being displayed before the rest of the information in the *Shelf CommentText* field.

If you click *Cancel*, the process is cancelled and the *Shelf CommentText* attribute remains unchanged.

# Setting the Succession release name for Multiservice Switch 15000 in VoA

When the SASM tool migrates the Multiservice Switch 15000 in Core ATM network, a customized version of the NAT tool is displayed to the operator running the SASM tool. This version of NAT has Succession pre-scripts and post-scripts to validate the Multiservice Switch 15000 state before and after the migration. When the post-activation script is finished, tool prompts the operator performing the migration to enter the Succession release name.

## Prerequisites

- The Multiservice Switch 15000 hitless software migration must have been performed using the Preside SASM tool. See NN10070-461 *Upgrading Nortel Networks Multiservice Switch 15000 in Succession Networks PT-AAL1/UA-AAL1*.

### Procedure 3 Setting the Succession release name for Multiservice Switch 15000 in VoA

***From the Preside MDM server***

1 The SASM tool post-activation script prompts you for the new Succession release name.




2 Enter the new Succession release name that you want displayed in the *Shelf CommentText* field.

Use the format: SNxx.y (for example, SN06.2 or SN07)

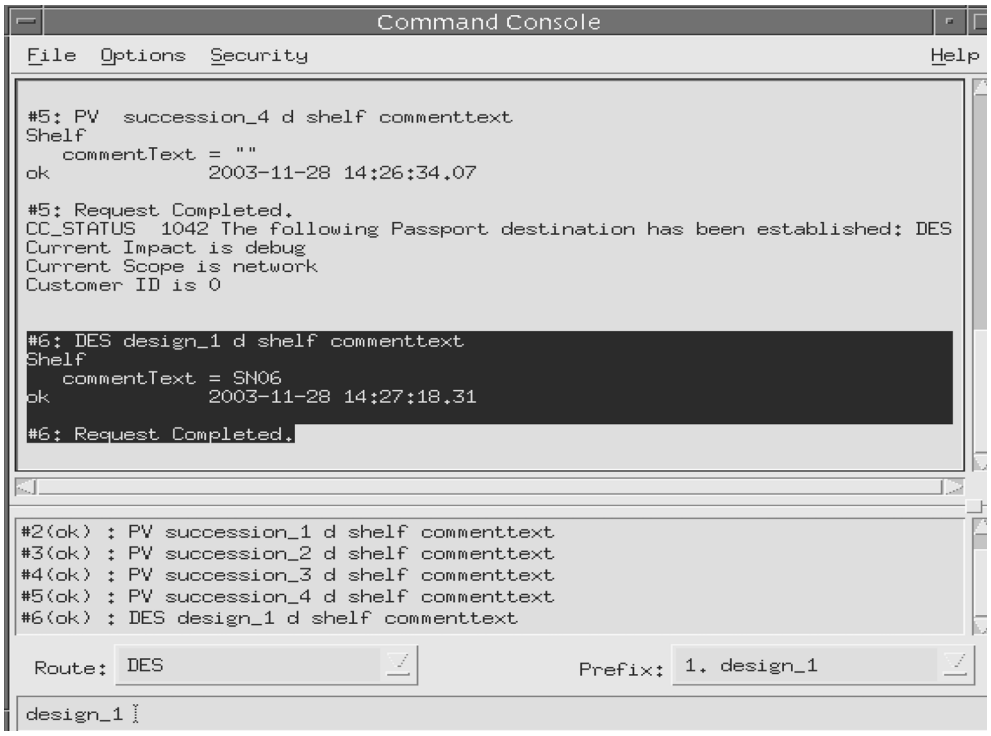
If you click *Cancel*, the process is cancelled and the *Shelf CommentText* attribute remains unchanged.

**3** Click *OK*.

A NAT record is created and the NAT window is displayed for a second time since SASM started.

This time it activates the service data (the only change is the *Shelf CommentText*) with no pre- and post-checks.

The Multiservice Switch 15000 *Shelf CommentText* attribute on the target node is updated. The Succession release name is displayed in front of the information in the *Shelf CommentText* field.




## Starting the Data Sync Server

Perform the following procedure to start the Data Sync Server if it does not start after you upgrade from Preside MDM 14.3 to 15.1.

### Prerequisites

- You must have performed the procedure Installing Preside MDM software from a CD-ROM on page 491 or Installing Preside MDM software release from a downloaded software version on page 494.
- Root user privileges

### Procedure 4 Starting the Data Sync Server

***From the Preside MDM server***

1 Login as root - see Logging into Preside MDM servers on page 522.

2 Open a Unix window or terminal.

3 Start a C-Shell session:

**>csh**

4 Set the DISPLAY environment variable:

**setenv DISPLAY <workstation name>:0.0**

5 Launch the MDM toolset:

**/opt/MagellanNMS/bin/nmstool &**

6 From the MDM toolset select *System* > *Administration* > *Server Administration tool*:.

The Server Administration tool opens.

7 From the *Security* menu, select *Authorize*.

The authorization dialog box opens.

8 Enter the password if required and click *OK*.

9 Click *Data Sync Server*, and then right-click and select *Stop*.

10 From the terminal window, change to the *cfg* directory:

**cd /opt/MagellanNMS/cfg/**

11 Open the *DataSync.cfg* file with your preferred editor. For example, using vi editor:

**vi DataSync.cfg**

12 Set the port number in the *DataSync.cfg* file to port="5050" as shown:

**<PPConfigServer host="localhost" dataDir="/opt/MagellanNMS/data/fps" port="5050"/>**

13 Save the changes and exit the file.

**14** From the terminal window, run the *Data Synchronization Migration* tool:

**/opt/MagellanNMS/bin/dbsyncmigrate**

The tool will then automatically migrate the content of the file **/opt/MagellanNMS/cfg/DataSync.cfg** to the MDM 15.1 format.

**15** From the Server Administration tool, click *Data Sync Server*, and right click and select *Start*.

# Activating new features for Preside MDM SN07

***Note:*** Before activating the SN07 features, Nortel Networks Preside Multiservice Data Manager (MDM) Succession features listed in the Preside MDM Succession feature baseline on page 144 must have been activated.

The new Preside MDM SN07 features include:

- MDP Administration enhancements
- Shelf view enhancements
- Server Administration enhancements
- Succession Release Name GUI
- Network Time Protocol (NTP) support

***Note:*** If the upgrade is from release MDM 14.3 to 15.1, the MDP Administration enhancements, Shelf view enhancements, and the Server Administration enhancement features have already been activated and no further activation is required for these features.

After installing Preside MDM software and patches, you must perform some additional configuration to set up:

- MDP Administration enhancements
- Shelf view enhancements
- Network Time Protocol (NTP) support

Before you activate the new features for SN07, ensure you have installed the software and have reviewed the Impact of MDP administration enhancements on page 511.

The following features are activated automatically:

- Server Administration extensions
- Succession Release Name GUI

## Activating new features for Preside MDM SN07

Nortel Networks Preside Multiservice Data Manager (MDM) SN07 features can be activated in any order once the upgrade is completed successfully.

- Adding an MDP server using the Server Administration tool on page 513
- Adding the psvagent on page 515
- Removing the Command Console (CC) Agent on page 517

However, you should review the following sections carefully before you re-order a server or change the release number on Preside MDM software or Nortel Networks Multiservice Switch nodes.

- Server Administration enhancements on page 518
- Setting the Succession release number on page 521
- Network Time Protocol (NTP) support on page 519

## Activating MDP administration enhancements

To activate the MDP administration enhancements, you must perform the procedure Adding an MDP server using the Server Administration tool on page 513.

**Prerequisites:**

Before activating the MDP administration enhancements, read the Impact of MDP administration enhancements on page 511 section carefully.

**Impact of MDP administration enhancements**

When you are using the Server Administration tool to manage the MDP servers, the servers must be started in the following sequence:

- MDP Disk Manager (mdpdiskmgr)
- MDP File Mover Manager (mdpfmmgr)
- MDP Passport Data Model Manager (mdpdmm)
- MDP Passport File Manager (mdppmgr)
- MDP File Prober Manager (mdpfpmgr)

While some servers do not have any server dependencies, others do (mostly to manage file acquisition from Multiservice Switch nodes and to handle disk cleanup so that the work station does not run out of file space).

The following servers have no inter-dependencies:

- MDP Disk Manager (mdpdiskmgr)
- MDP File Mover Manager (mdpfmmgr)
- MDP Passport Data Model Manager (mdpdmm)

The MDP Passport File Manager (mdpdmm) has the following dependencies:

- requires mdpfpmgr to acquire node data
- mdpdiskmgr to manage disk space
- mdpfmmgr to transfer files to OSS

The MDP File Prober Manager (mdpfpmgr) requires:

- mdpdmm
- HGDS

- mdpppmgr for conversion of node files from FMIP to BDF
- mdpfmmgr to transfer files to OSS



**CAUTION**
**Ensure the HGDS and the MDP Data Model Manager are running before you start the MDP File Prober Manager.**
The HGDS and the mdpdmm must be running before the mdpfpmgr server is started.

Other factors that may impact MDP configuration files depend on the individual customer deployment. Any configuration information that was configured in special files must be ported to HGDS before the MDP servers are started. See *Preside Multiservice Data Manager Release 15.1 Supplement* for more details on migrating configuration files.

After the MDP servers are started, HGDS is used by MDP to connect to Nortel Networks Multiservice Switch nodes.

# Adding an MDP server using the Server Administration tool

Use the following procedure to add an MDP server using the Server Administration tool.

### Adding an MDP server

***From the Preside MDM server***

1 Login to the server using the “mdpadmin” user ID used to start the MDP servers. See Logging into Preside MDM servers on page 522.

2 Open a Preside MDM window:

**/opt/MagellanNMS/bin/nmstool &**

3 Click *OK* to close the copyright dialog.

4 From the Preside MDM window System menu, select Administration > Server Administration.

5 From the Security menu, select *Authorize*.

6 Enter the password in the SVM Enter Authorization Password dialog.

7 From the Edit menu, select *New server*.

8 From the SVM New Server Selection list, open the Accounting/Data Collection folder.

9 Select the MDP Disk Manager (mdpdiskmgr) from the list and click *Select server.*

In the SVM New Server dialog, ensure that “Automatic startup at reboot time” is selected.

10 Click OK and save the new server setting.

11 Repeat steps 9 and 10 from the Accounting/Data Collection folder for the remaining servers:

- MDP File Mover Manager (mdpfmmgr)
- MDP Passport Data Model Manager (mdpdmm)
- MDP Passport File Manager (mdppmgr)
- MDP File Prober Manager (mdpfpmgr)

***Note:*** The order in which you add a new server is important.

12 In the SVM New Server Selection tool, click *Close*.

13 From the Server Administration tool start all the servers in the following order:

- MDP Disk Manager (mdpdiskmgr)
- MDP File Mover Manager (mdpfmmgr)
- MDP Passport Data Model Manager (mdpdmm)
- MDP Passport File Manager (mdppmgr)
- MDP File Prober Manager (mdpfpmgr)

by right-clicking and selecting *Start.*

14 Close the Server Administration tool.

**Variable values**

| Variable | Value |
|---|---|
| <svadm password> | The password for Server Administration authorization. |

## Activating shelf view enhancements

To activate the shelf view enhancements, perform the procedures:

- Adding the psvagent on page 515
- Removing the Command Console (CC) Agent on page 517

## Adding the psvagent

Use the following procedure to add the Shelf View Agent (psvagent) to the Server Administration tool.

***From the Preside MDM server***

1 Login — see Logging into Preside MDM servers on page 522.

2 Open a Preside MDM server window:
**/opt/MagellanNMS/bin/nmstool &**

3 Click *OK* to close the copyright dialog box.

4 From the Preside MDM window System menu, select Server Administration.

5 View the list of servers and verify that the Shelf View Agent is present and running.

***Note:*** The server name displayed will be PP Shelf View Agent if the server was configured before the migration to Preside MDM 15.1. Otherwise, the server name will display as Fault Dev Access Agent.

6

| If | Do |
|---|---|
| the server is not present | Perform steps 7 through 14 inclusive |
| the server is present but not running | Go to step 13. |
| the server is running | This procedure is complete. |

7 From the Security menu, select *Authorize*.

8 Enter the password in the SVM Enter Authorization Password dialog box and click *OK.*

9 From the Edit menu, select *New Server*.

The SVM New Server Selection dialog opens.

10 From the SVM New Server Selection list, select and open the *Fault* folder.

11 Select the *Fault Device Access Agent (psvagent)* from the list and click *Select server*.

12 In the SVM New Server dialog box, select *Automatic startup at reboot time* and click *Save*.

13 From the Server Administration window, select *Shelf View Agent Server*.

14 From the Options menu select *Start*.

The server should now indicate that it is running.

**Variable values**

| Variable | Value |
|---|---|
| <svadm password> | The password for Server Administration authorization. |

## Removing the Command Console (CC) Agent

Adding the Fault Dev Access Agent to the server administration makes the CC agent redundant. If applicable, remove the CC agent by performing the following procedure.

### Prerequisites

Perform Adding the psvagent on page 515 before you remove the CC agent.

***From the Preside MDM server***

1. Login — see Logging into Preside MDM servers on page 522.
2. Open a Preside MDM window:
   **/opt/MagellanNMS/bin/nmstool &**
3. Click *OK* to close the copyright dialog.
4. From the Preside MDM window System menu, select Administration > Server Administration.
5. View the list of servers and determine if the CC agent is present.
6. If the CC agent is present, go to the Security menu, and select *Authorize*.
7. Enter the password in the SVM Enter Authorization Password dialog, and click *OK.*
8. Select the server from the list.
9. From the Edit menu, select **Remove Server**.
10. Click *OK* in the SVM New Server Selection dialog.
11. Verify that the server is no longer present in the Server Administration tool.

## Server Administration enhancements

The Server Administration (SVM) tool enhancements simplify Nortel Networks Preside Multiservice Data Manager (MDM) server administration and configuration by allowing users to add or delete servers from a server list and providing context-sensitive help on the servers. Servers can be re-ordered in the list.



**CAUTION**
**Use caution when re-ordering a server sequence.** Only an expert Preside MDM administrator should re-order servers. Consult 241-6001-310 *Preside MDM Server Reference Guide.*

The SVM tool enhancements also provides a launch point for configuration editors associated with servers.

# Network Time Protocol (NTP) support

Network Time Synchronization (NTS) refers to the synchronization of the time-of-day on Preside MDM servers and Multiservice Switch 15000 switches. Use the NTP software supplied with Solaris as part of the SUNWnptr and SUNWnptu packages to perform Network Time Synchronization.

The executable is located in */etc/init.d/xntpd*. The configuration for the process is defined in */etc/init/ntp.conf*. The process is automatically started at reboot by */etc/rc2.d/S74xntpd* if the file */etc/inet/ntp.conf* exists.

### Network Time Protocol (NTP) protocol

***From the MDM***

**1** Login — see Logging into Preside MDM servers on page 522.

**2** Copy the file ntp.server to ntp.conf:

**cp/etc/inet/ntp.server /etc/inet/ntp.conf**

**3** Edit the ntp.conf file to set a particular server as the timing reference:

**a** Locate the line that begins with “server 127.127”. Change it to: **server <IP address> prefer**

For example, where the IP address is 127.127.1.1, as follows: server 127.127.1.1 prefer

**b** Add references to any other servers the MDM can obtain time synchronization information from. In Succession, this is usually the higher level element manager.

**c** The Preside MDM server can be in a peer relationship, also known as a server set, with another MDM server. In that case, the ntp.conf file must exist on each of the MDM servers. Each ntp.conf file must specify the IP addresses of both MDM servers. Use the syntax:

```
peer <ip address of MDM server 1>
peer <ip address of MDM server 2>
```

**4** Use the comment character (#), to comment out the line that begins with “fudge 127.127”.

**5** Use the comment character (#), to comment out the line that begins with “broadcast”.

**6** Use the comment character (#), to comment out the lines that contain the encryption keys.

If you do not comment out these key lines, the default value of 0 allows anyone to access the workspace and set the clock.

**7** Save the file.

Example ntp.conf file:

```
server <ip address of clocking source> prefer
peer <ip address of MDM server 1>
peer <ip address of MDM server 2>
driftfile /var/ntp/ntp.drift
#fudge 127.127.XType.0 stratum 0
#broadcast 224.0.1.1 ttl 4
#trustedkey 0
#requestkey 0
#controlkey 0
```

**8** Set up the drift file.

The drift file contains the oscillator frequency offset of the clocking source. If you know the oscillator frequency, enter it in this file. Otherwise, enter 0, and the XNTP daemon determines it automatically. It just takes a little longer for the time to stabilize to a consistent value.

**a** Edit the drift file: **/etc/inet/ntp.drift** (this step is optional)

**b** Enter the value of the oscillator frequency offset, if you know it. Otherwise, enter 0.

**c** Save the file.

**9** Set up permissions for the configuration and drift files.

**a** Change the privileges to npt.conf, ntp.drift to 500 with an owner of root.

**b** Change the owner of both the files to root.

**10** Start the server or XNTP daemon: **/etc/init.d/xntpd start**

***Note:*** The command “ntpq” allows you to query the ntpd configuration and its status. See Sun documentation for more information.

For more information on how Network Time Synchronization system is configured, see the NN10225-512 *Nortel Networks Multiservice Switch 15000 and Media Gateway 15000 in Succession Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP*.

## Setting the Succession release number

This feature adds two utilities to the Nortel Networks Preside Multiservice Data Manager (MDM) toolset that allows operators to set the Succession release name in the Preside MDM tool launcher window, and the *CommentText* attribute of the Multiservice Switch node.

See the Setting the Succession release name for Multiservice Switch 15000/Media Gateway 15000 in VoIP on page 502.

# Appendix A - Preside MDM access procedures

These procedures describe how to log into Nortel Networks Preside Multiservice Data Manager (MDM) servers and open the toolset menu.

## Logging into Preside MDM servers

The Network Activation tool (NAT) starts.

To login to a Preside MDM server, perform the following steps.

***From the Preside MDM server***

1 Login as the root user.

2 Enter the root password when prompted.

## Opening the Preside MDM window

Open a Preside Multiservice Data Manager (MDM) window before beginning the upgrade process.

***From the Preside MDM server***

1 If the window does not automatically open at login, open the window with the following command:

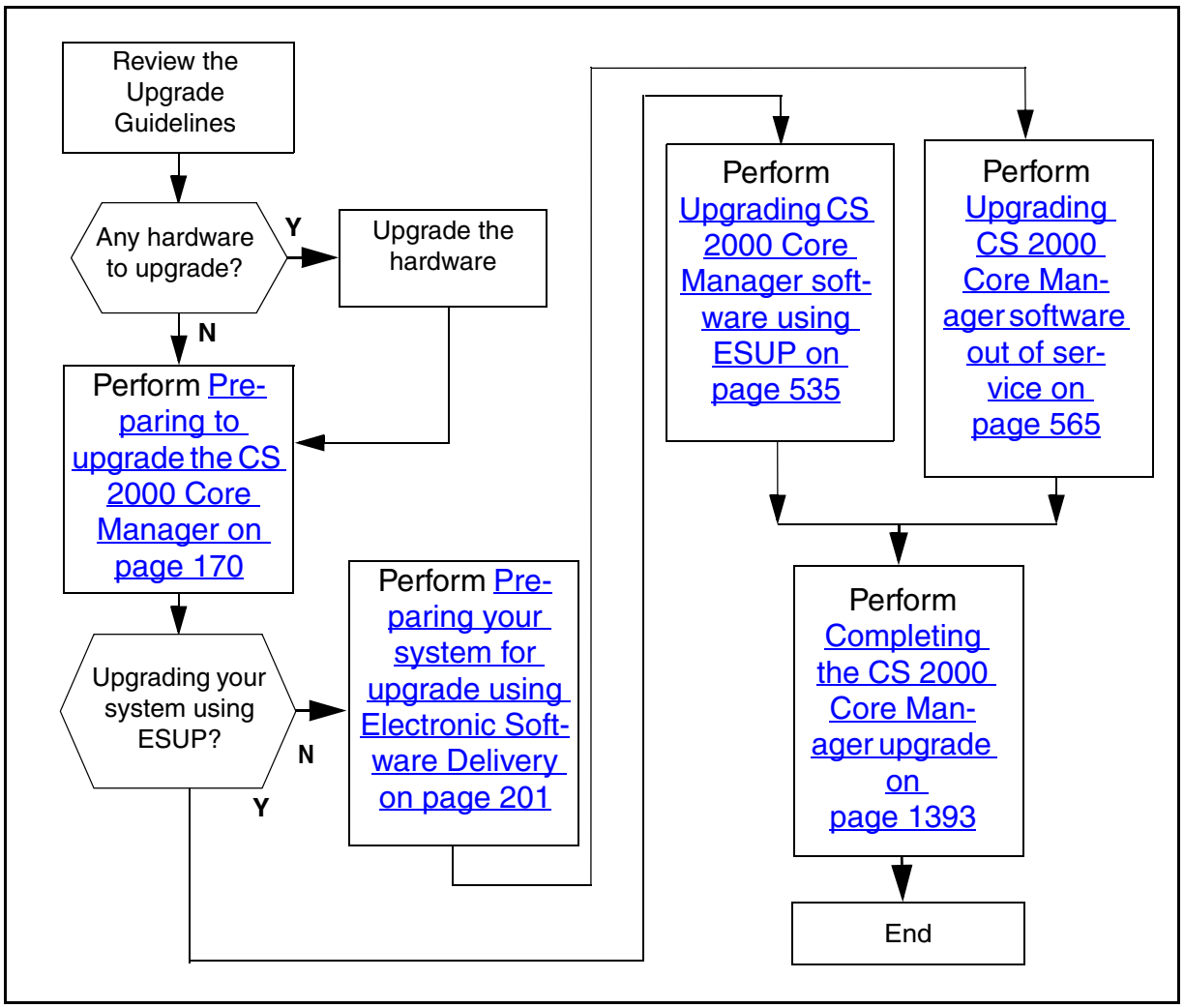
**/opt/MagellanNMS/bin/nmstool &**

The copyright dialog opens, followed by the Preside MDM window. Click *OK* to close the copyright dialog.

# Upgrading the CS 2000 Core Manager

The following flowchart provides a summary of the upgrade process. Use the instructions in the specific procedures to complete each task.

**Task flow for upgrading the CS 2000 Core Manager**



## Upgrade strategy

The Succession Networks upgrade strategy is based on end-to-end upgrades that provides the following.

- an upgrade that provides a carrier grade solution and has no impact to stable calls
- a solution that does not isolate network components
- a solution that allows third party components
- a solution that introduces new functionality across many components without affecting network stability

The CS 2000 Core Manager component lies at the highest level of Succession upgrades and must be upgraded before other components.

**ATTENTION**
Once the CS 2000 Core Manager is upgraded, you cannot provision Gateway Controllers (GWC) until the CS 2000 Management (CS2M) software package is installed and configured on the CS 2000 Management Tools server.

New software is made available through the following methods:

- non-computing load (NCL), a major release of the software scheduled once or twice a year, delivered on tape or electronically
- maintenance non-computing load (MNCL), a maintenance release scheduled approximately every three months for the first year of a released NCL, delivered on tape or electronically
- CS2000 Core Manager patching, fix filesets delivered electronically as soon as they are available

## Tools and utilities

The information in this document provides procedures using common upgrade tools and utilities for:

- CS2000 Core Manager platform software upgrades available from tape or electronic software delivery (ESD): SDM Out of Service (OOS) Upgrade Procedure and enhanced SDM upgrade procedure (ESUP)
- Client application upgrades, including ASCII Terminal Access (ATA), Enhanced Terminal Access (ETA), Secure File Transfer (SFT) and others
- Hardware upgrades to the latest CPU modules

## Upgrade process overview

Task flow diagrams and detailed instructions for specific upgrade procedures are provided in this document.

**ATTENTION**

For an MNCL upgrade, check the release notes.

If you have an MNCL upgrade to install, refer to the MNCL release notes for instructions. This procedure only provides information on NCL upgrade installation.

# Upgrade guidelines

Nortel Networks offers several Network Service Solution packages to assist you with the upgrade of CS 2000 Core Manager software. The level of design, planning, configuring, and installation that Nortel Networks performs for you depends on the options that your company purchased.

## Upgrade methods

There are two methods of upgrading the CS 2000 Core Manager to the CS2E0070 software release:

- Out of Service (OOS) Upgrade Procedure via Electronic software delivery (ESD) or tape: This procedure busies the CS 2000 Core Manager and upgrades both domains at the same time.
- Enhanced SDM upgrade procedure (ESUP): This procedure breaks the root volume group (rootvg) mirror, applies new filesets to domain 1 rootvg, busies and reboots the system, then integrates rootvg disks.

  ESUP upgrades can be performed in the following ways, using a:

  — telnet connection (only for upgrades to SDM20/CS2E0070 or later)

  — remote console connection (modem, terminal server, etc.) (all releases)

  — local console connection (vt100 terminal/emulation) (all releases)

### When to use each method

The following table indicates when to use the OOS Upgrade Procedure or ESUP method to upgrade your CS 2000 Core Manager to the CS2E0070 release:

| If you are upgrading... | OOS Upgrade Procedure | ESUP |
|---|---|---|
| a rootvg-only system | x | |
| a rootvg/datavg system | x | x |
| the software and CPU hardware | | |

## Hardware baseline

The table Hardware baseline on page 528 indicates the supported hardware to upgrade to the CS2E0070 release.

**Hardware baseline**

| PEC | Description |
|---|---|
| CPU | |
| NTRX50NB | Arthur 750 - 400MHz/512MB |
| Disk/DAT and LAN PM | |
| NTRX50ND | 9G + DAT (rootvg)<br><br>***Note:*** Replacements for the NTRX50ND will be filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NM replaces the NTRX50ND. |
| NTRX50FS | LAN personality module |
| Disk expansion | |
| NTRX50NC | 9G + 9G (datavg)<br><br>***Note:*** Replacements for the NTRX50NC will be filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NL replaces the NTRX50NC. |
| Core connectivity | |
| NTRX50GX | DS-512 controller module |
| NTRX50GH | DS-512 personality module |
| X.25 connectivity (optional) | |
| NTRX50FY | X.25 controller module |
| NTRX50FZ | X.25 personality module |
| NTRX50NN | X.25 personality module for UMFIO |

You can have different MFIO/UMFIO datavg and rootvg combinations configured on your system. The following table lists the combinations that are supported for the CS2E0070 release.

**Supported MFIO and UMFIO, datavg and rootvg configurations**

| Configuration | Domain 0 | | Domain 1 | | Total disk storage |
|---|---|---|---|---|---|
| | Rootvg | Datavg | Rootvg | Datavg | |
| Most basic (not recommended) | NTRX50GN 4-Gbyte | N/A | NTRX50GN 4-Gbyte | N/A | 4-Gbyte (rootvg only) |
| Moderate | NTRX50GN 4-Gbyte | NTRX50GP 8-Gbyte | NTRX50GN 4-Gbyte | NTRX50GP 8-Gbyte | 12-Gbyte |
| Largest with 4-Gbyte disk | NTRX50GN 4-Gbyte | NTRX50GP (8-Gbyte) + (expansion chassis) NTRX50GP (8-Gbyte) 16-Gbyte | NTRX50GN 4-Gbyte | NRTX50GP (8-Gbyte) + (expansion chassis) NTRX50GP (8-Gbyte) 16-Gbyte | 20-Gbyte |
| Basic with 9-Gbyte disk | NTRX50ND 9-Gbyte[1] | N/A | NTRX50ND 9-Gbyte1 | N/A | 9-GByte (rootvg only) |
| Moderate | NTRX50ND 9-Gbyte1 | NTRX50NC 18-Gbyte[2] | NTRX50ND 9-Gbyte1 | NTRX50NC 18-Gbyte2 | 27-Gbyte |
| Largest with 9-Gbyte disk | NTRX50ND 9-Gbyte1 | NTRX50NC (18-Gbyte)2 + (expansion chassis) NTRX50NC (18-Gbyte) 36-Gbyte | NTRX50ND 9-Gbyte1 | NTRX50NC (18-Gbyte)2 + (expansion chassis) NTRX50NC (18-Gbyte) 36-Gbyte | 45-Gbyte |
| 4-Gbyte/ 9-Gbyte mix | NTRX50GN 4-Gbyte | NTRX50NC 18-Gbyte2 | NTRX50GN 4-Gbyte | NTRX50NC 18-Gbyte2 | 22-Gbyte |
| Basic with 36-Gbyte disk | NTRX50NM 36-Gbyte | N/A | NTRX50NM 36-Gbyte | N/A | 36-Gbyte |

**Supported MFIO and UMFIO, datavg and rootvg configurations**

| Configura-tion | Domain 0 | | Domain 1 | | Total disk storage |
|---|---|---|---|---|---|
| | Rootvg | Datavg | Rootvg | Datavg | |
| Largest with only 36-Gbyte disk | NTRX50NM 36-Gbyte | NTRX50NL 72-Gbyte | NTRX50NM 36-Gbyte | NTRX50NL 72-Gbyte | 108-Gbyte |
| 4-Gbyte/ 36-Gbyte mix | NTRX50GN 4-Gbyte | NTRX50NL 72-Gbyte | NTRX50GN 4-Gbyte | NTRX50NL 72-Gbyte | 76-Gbyte |
| 9-Gbyte/ 36-Gbyte mix | NTRX50ND 9-Gbyte1 | NTRX50NL 72-Gbyte | NTRX50ND 9-Gbyte1 | NTRX50NL 72-Gbyte | 81-Gbyte |

***Note 1:*** The maximum number of NTRX50GP MFIOs allowed in a system is four. The expansion shelf is required for this configuration.

***Note 2:*** NTRX50GN and NTRX50GP will not be supported after November 2004. These disks should be replaced by NTRX50GP and NTRX50NM.

***Note 3:*** The maximum number of NTRX50NC MFIOs allowed in a system is four. The expansion shelf is required for this configuration.

***Note 4:*** The maximum number of NTRX50NL UMFIOs allowed in a system is two. Disk expansion shelf is not required in this configuration.

***Note 5:*** MFIOs and UMFIOs must be deployed in matched pairs. MFIO and UMFIO modules cannot be intermixed; a volume group must have all of one or the other. For example, a pair of 4-Gbyte MFIO modules can be mixed with a pair of 9-Gbyte MFIOs in datavg. A pair of 9-Gbyte MFIOs cannot be mixed with a pair of 36-Gbyte UMFIOs in datavg.

***Note 6:*** A single 4-Gbyte MFIO module cannot be mixed with a single 9-Gbyte module or a 36-Gbyte module to form a pair.

1. Replacements for the NTRX50ND will be filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NM will be the replacement for the NTRX50ND.
2.Replacements for the NTRX50NC will be filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NL will be the replacement for the NTRX50NC.

## Software baseline

You must have the latest maintenance non-CM load (MNCL) release installed on the CS 2000 Core Manager before you upgrade to the new NCL release.

As of the release of this information, the latest MNCL for each release is as follows:

- CS2E0004.3
- CS2E0005.2
- CS2E0006.0.1

When a new MNCL is released for the CS 2000 Core Manager, a technical bulletin is issued with a Notification of Availability. Check whether any technical bulletins with a Notification of availability in the title have been issued to determine if a later MNCL exists for your release. If you need to upgrade to the latest MNCL, refer to the MNCL release notes for instructions.

The Communication Server 2000 core must be at the CSP17 release or higher to upgrade the CS 2000 Core Manager to the CS2E0070 release.

# Filesets to solution mapping

This module provides information on the filesets included in the CS2E0070 load.

The following table lists CS2E0070 filesets and provides the following information

- the solutions that use each fileset
- the DCE requirements for each fileset

**Fileset-to-solution mapping (Sheet 1 of 3)**

| Fileset | Description | Succession Solutions | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | IAC | IAW | PT-AAL1 | PT-IP | UA-AAL1 | UA-IP | DCE? |
| SDM_VERSION.info | CS2E0070 7.0 | Y | Y | Y | Y | Y | Y | N |
| SDM_AFT.DMS500 | SBA Automatic File Transfertime | N | N | N | N | N | N | N |
| SDM_ASG.accessd | Passwerks Access Daemon Runtime | Y | Y | Y | Y | Y | Y | N |
| SDM_ATA.client | ASCII Terminal Access Client | Y | Y | Y | Y | Y | Y | Y |
| SDM_BASE.client | Client Common Resources | Y | Y | Y | Y | Y | Y | Y |
| SDM_BASE.dfquery | Check disks and disk drives | Y | Y | Y | Y | Y | Y | N |
| SDM_BASE.fts | File Transfer Service | Y | Y | Y | Y | Y | Y | N |
| SDM_BASE.gdd | Generic Data Delivery | Y | Y | Y | Y | Y | Y | N |
| SDM_BASE.logs.client | Log Delivery Service Client | Y | Y | Y | Y | Y | Y | N |
| SDM_BASE.logs | Log Delivery Service | Y | Y | Y | Y | Y | Y | N |
| SDM_BASE.mtce | Platform Maintenance | Y | Y | Y | Y | Y | Y | N |

***Note:*** Y= required, N=not required, O=optional

**Fileset-to-solution mapping (Sheet 2 of 3)**

| Fileset | Description | Succession Solutions | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | IAC | IAW | PT-AAL1 | PT-IP | UA-AAL1 | UA-IP | DCE? |
| SDM_BASE.omsl | OM Access Service | Y | Y | Y | Y | Y | Y | N |
| SDM_BASE.tasl | Table Access Service | Y | Y | Y | Y | Y | Y | N |
| SDM_BMI.bmi | Base Maintenance Interface | Y | Y | N | Y | Y | Y | N |
| SDM_DDMS.ossaps | OSS and Application Svcs | Y | Y | N | Y | Y | Y | N |
| SDM_DDMS.osscomms | OSS Comms Svcs | Y | Y | N | Y | Y | Y | N |
| SDM_DMA.dma | DMS Maintenance Application | Y | Y | N | Y | Y | Y | N |
| SDM_DNBD.dnbd | DNBD Call Data Delivery | Y | Y | Y | Y | Y | Y | N |
| SDM_DNBD.osidp | ONE FTAM Software | Y | Y | Y | Y | Y | Y | N |
| SDM_DTS_PROVIDERS.dts | DCE DTS Time providers for global servers | Y | Y | Y | Y | Y | Y | Y |
| SDM_ESUP.esup | ESUP Tools | Y | Y | Y | Y | Y | Y | N |
| SDM_ETA.eta | Enhanced Terminal Access | Y | Y | Y | Y | Y | Y | Y |
| SDM_ETA.client | Enhanced Terminal Access Client | Y | Y | Y | Y | Y | Y | Y |
| SDM_GR740PT.gr740pt | GR740 Pass Through | Y | Y | Y | Y | Y | Y | O |
| SDM_IMAGEDUMP.rte | Image Dump Service | Y | Y | Y | Y | Y | Y | N |
| SDM_INEO.ssh-sftp | Ineo SSH Secure File Transfer | Y | Y | Y | Y | Y | Y | N |
| SDM_INSTALL_inst | SDM Tools | Y | Y | Y | Y | Y | Y | N |
| SDM_LOGS.mdm | Passport Log Streamer | N | N | Y | Y | Y | N | N |

***Note:*** Y= required, N=not required, O=optional

**Fileset-to-solution mapping (Sheet 3 of 3)**

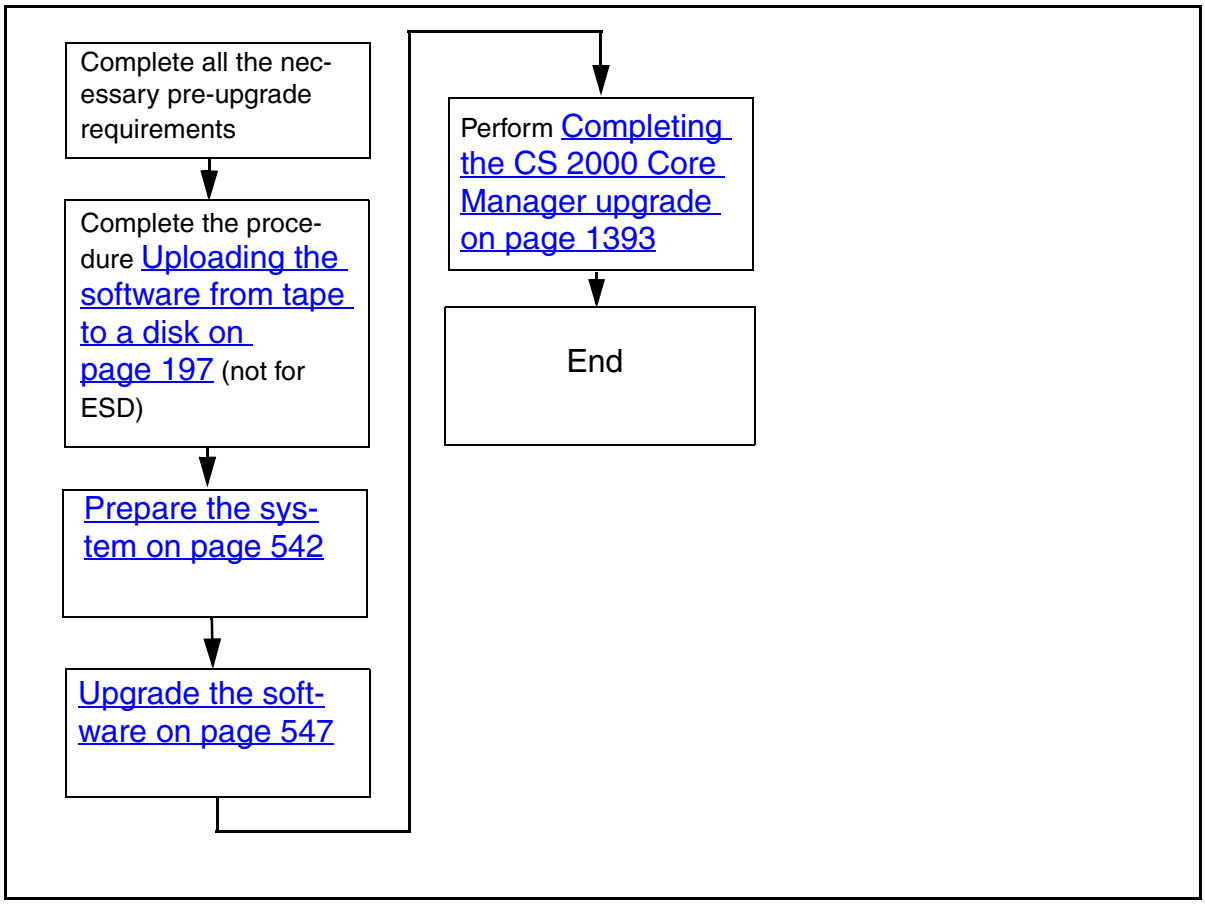
| Fileset | Description | Succession Solutions | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | IAC | IAW | PT-AAL1 | PT-IP | UA-AAL1 | UA-IP | DCE? |
| SDM_OMDD.omdd | OM Delivery | Y | Y | Y | Y | Y | Y | N |
| SDM_OpenSSH.base | Open SSH ver. 3.4p1 | Y | Y | Y | Y | Y | Y | N |
| SDM_PRECHECK.sysaudit | System pre-check tools | Y | Y | Y | Y | Y | Y | N |
| SDM_REACHTHRU.rttl1 | Reach Through SPM | Y | Y | Y | Y | Y | Y | N |
| SDM_SBA.DMS500 | SDM Billing Application | Y | Y | Y | Y | Y | Y | N |
| SDM_SCM.scm | Succession SAM21 Manager<br><br>***Note:*** This fileset is only required for SN05 to SN07 upgrades. | Y | Y | N | Y | Y | Y | N |
| SDM_SFT.client | Secure File Transfer Client | Y | Y | Y | Y | Y | Y | O |
| SDM_SFT.sft | Secure File Transfer | Y | Y | Y | Y | Y | Y | O |
| SDM_SWLD.swld | BOOTP Loading Service | Y | Y | N | Y | Y | Y | N |
| SDM_UPGRADE.tools | UPGRADE Tools | Y | Y | Y | Y | Y | Y | N |

***Note:*** Y= required, N=not required, O=optional

# Upgrading CS 2000 Core Manager software using ESUP

Use the following task flow to upgrade the CS 2000 Core Manager using the enhanced software upgrade procedure (ESUP).

**Task flow for upgrading CS 2000 Core Manager software using ESUP**



**ATTENTION**
Nortel Networks recommends the usage of the system console (SP0) for the upgrade. When upgrading the software using ESUP via TELNET, ensure that the device used to connect to the console port (modem, VDU - Visual Display Unit or VT-100 terminal, terminal server, dual input VDU, etc.) is configured with flow control off. Failure to turn off flow control may cause the SDM to hang during the reboot conducted at the end of each upgrade.

## Purpose

This procedure provides information about upgrading your CS 2000 Core Manager software from the latest CS2E0004, CS2E0005, or CS2E0006 release to the CS2E0070 release using an enhanced SDM upgrade procedure (ESUP).

***Note:*** This procedure does not apply to rootvg-only systems.

This procedure references other procedures in the CS 2000 Core Manager Upgrades, Fault Management, Configuration Management, Accounting, and Security and Administration documents. Ensure that you have access to those documents while performing this procedure.

You can perform this procedure from a VT100 console. You can also use this procedure if you are able to telnet to the CS 2000 Core Manager through the LAN (local area network).

During the ESUP upgrade, the rootvg mirror is broken, the system is busied for a short time, then rootvg disks are re-integrated. The procedure takes approximately 2.5 hours. Datavg does not break mirror during this procedure; therefore, it does not undergo re-integration.

***Note:*** This procedure provides on-screen information and instructions. Please read all displayed messages carefully and use them together with this document to successfully complete the upgrade.

## Pre-upgrade requirements

Before starting this procedure, complete the following activities:

- Ensure the latest MNCL release is installed on your system.

  Refer to “Upgrade guidelines” in *Upgrading the CS 2000 Core Manager,* NN10060-461. for the software baseline.

  ***Note:*** If you need to upgrade to the latest MNCL, refer to the MNCL release notes for instructions.

- Verify that the pre-check tasks described in the procedure Preparing to upgrade the CS 2000 Core Manager on page 170 were successfully completed seven days before starting this upgrade.
- Perform a system image backup.

  **ATTENTION**

  Nortel Networks recommends that you perform a system image backup before you upgrade the base software. Use the procedure “Creating system image backup tapes (S-tapes) manually” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

  Performing a system image backup does not back up billing data. Ensure that billing is operating properly before starting.

  If you need to revert to a prior release during an out-of-service upgrade, refer to “Performing a full restore of the software from S-tape” in *CS 2000 Core Manager Fault Management*, NN10082-911.

- Obtain the password for the root user.

  Because you must log on to the CS 2000 Core Manager using the root user ID and password to perform the upgrade, you will need to obtain the password for the root user before you begin. Failure to log on as the root user may cause your upgrade to fail.

- Ensure that no other users are logged on during the upgrade. Only the user at the VT100 console or the upgrade telnet session should be logged on.
- Obtain the IP address for the CS 2000 Core Manager.
- Execute a ‘querysdm config’ command and record the output.

- Obtain the following information from your network administrator:
  - if your system has SAM21 element manager installed, verify whether DNS is supported on SAM21 EM client workstations
  - the host name of the CS 2000 Management Tools server that is configured to run the Login Application
  - the CommonName from the certificate on the CS 2000 Management Tools server that is configured to run the Login Application
  - the IP address of the CS 2000 Management Tools server

  ***Note:*** Record the information for reference purposes.

- If upgrading from tape, ensure that you have the tape labeled "CS2E0070 NCL 7.x (1 of 1)".

  ***Note:*** Nortel Networks recommends that you upgrade your system directly from tape only if you are unable to complete the procedure Uploading the software from tape to a disk on page 197.

- If upgrading via Electronic Software Delivery (ESD), ensure that the required files are in the directory you will be upgrading from, which may be the "/swd/sdm/esd" directory.

  ***Note 1:*** If necessary, contact your next level of support, or refer to the procedures "Preparing your system for upgrade via Electronic Software Delivery" in *Upgrading the CS 2000 Core Manager,* NN10060-461 and "Transferring and retrieving files using SFT" in *CS 2000 Core Manager Administration and Security*, NN10170-611.

  ***Note 2:*** If you need to determine the list of required filesets for your Succession solution, refer to "Filesets to solution mapping".

- Install and configure the pserver application on the Preside MDM. This applies to Succession offices where the CS 2000 Core Manager needs to communicate with the Preside MDM for fault data using the Passport log streamer application. Refer to the Passport 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting, NN10198-912, for instructions on how to configure the pserver application.
- Ensure that the system is equipped with a datavg. The CS 2000 Core Manager must be equipped with a data volume group (datavg). You can check the presence of a datavg through the maintenance interface under the storage level (sdmmtc storage).

- Check the root logical volume file system - potential disk space error. Make sure the root logical volume “/” file system does not exceed 70% of its total size. If the “/” file system exceeds the 70% mark, you must make more room on the “/” file system for the upgrade to be successful. For more details, contact your next level of support.
- Ensure the CS 2000 Core Manager is alarm free.
  If any alarms are present, refer to the Fault section of this document for alarm-clearing procedures.
- Ensure that you either
  - — Have VT100 terminal emulation.
    Before you perform this procedure, it is recommended that you ensure that your terminal is capable of VT100 terminal emulation and that you can establish a VT100 connection to SP0.

    or
  - — Have a PC or UNIX workstation connected to the LAN.
    Ensure that you have access to a PC or UNIX workstation from which you are able to telnet and access the CS 2000 Core Manager through the LAN. Also, verify that telnet is enabled on the CS 2000 Core Manager.
- If you have SBA on your system, query the status of RTB for each billing stream for which RTB is configured.
  Record all RTB streams that are InSv for reference purposes.

  ***Note:*** If required, refer to the procedure “Querying the status of RTB for a billing stream” in the Accounting document.
- Nortel Networks recommends that you deliver unprocessed billing files to a downstream destination. Ensure that no more than one unprocessed billing file remains on the system. The following table lists each task and the procedure in the Accounting document to complete the task.

**Accounting procedure for each task and file transfer mode**

| Task | File transfer mode | Accounting procedure |
|---|---|---|
| Close billing files | All | “Closing billing files” |
| Send billing files downstream | Outbound file transfer (OFT) | “Sending billing files from disk” |

**Accounting procedure for each task and file transfer mode**

| Task | File transfer mode | Accounting procedure |
|---|---|---|
| | Inbound file transfer (IFT) | "Retrieving billing files for a stream set to inbound file transfer" |
| | Real time billing (RTB) | "Sending billing files from disk" |
| | Automatic file transfer (AFT) | No manual action is required. Wait for SBA to deliver pending billing files to the downstream destination. There should be no pending files (at least, no more then one) for each AFT session.<br>Use the following commands to query AFT sessions: **`billmtc, appl, aft, aftconfg, list`**.<br>To verify which billing files for each session are still pending, enter the following commands: **`billmtc, appl, aft, query <session_name>`**.<br>***Note:*** Press the Enter key after each command. |

***Note:*** To display the details about a stream, refer to the procedure "Listing billing streams" in the Accounting document. To list all files currently stored in a stream, refer to the procedure "Listing billing files" in the Accounting document.

If you are unable to send billing files to a downstream destination and you want to proceed with the upgrade, Nortel Networks recommends that you backup the billing files to a DAT tape. If required, refer to the procedure "Copying billing files to tape (backup)" in the Accounting document.

***Note:*** If you need to restore the billing files from tape and you have AFT or IFT configuration, contact your next level of support for instructions. For any other configuration, you can send the billing files from tape following the procedure "Sending billing files from tape" in the Accounting document.

## Upgrade notices



**CAUTION**
**Possible upgrade failure**
Do not login into any of the /alt_inst file systems at any stage of the upgrade. This may cause the upgrade to fail and start an automatic recovery.

**ATTENTION**
Some applications are automatically removed.

If the Exception Reporting, Alarm Conduit, SDM Corba Framework, and Remote Registration System filesets are present, they are automatically removed when upgrading to CS2E0070.

**ATTENTION**
Some obsolete applications in SN07 are automatically removed. If Remote Registration system fileset is present, it is automatically removed when upgrading to CS2E0070.

**ATTENTION**
In case of fallback...

You can abort this procedure at every prompt. If you choose to abort before the system reboots, follow the on-screen instructions to recover the system. If you choose to abort after the system reboots, complete the procedure “Recovering the system from an ESUP failure” in *Upgrading the CS 2000 Core Manager,* NN10060-461.

If the CS 2000 Core Manager system initiates an automatic fallback during this procedure, contact your next level of support before attempting the recovery procedure.

## Prepare the system

**ATTENTION**
Read the Pre-upgrade requirements and Upgrade notices sections, and complete any necessary activities before you proceed with the upgrade.

This procedure can be performed from either a VT100 console or a telnet session.

| If you choose | Do |
|---|---|
| telnet session | step 1 |
| VT100 console | step 2 |

***At the PC or UNIX workstation***

**1** Establish a telnet connection to the CS 2000 Core Manager by completing the following substeps.

**a** Open a terminal window that is VT100 compatible.

**b** Log onto the CS 2000 Core Manager from the terminal window prompt:

```
telnet <ip_address>
```

where

**<ip_address>**
is the IP address of the CS2000 Core Manager

**c** Keep window size at 80x24.

***At the VT100 console or telnet session***

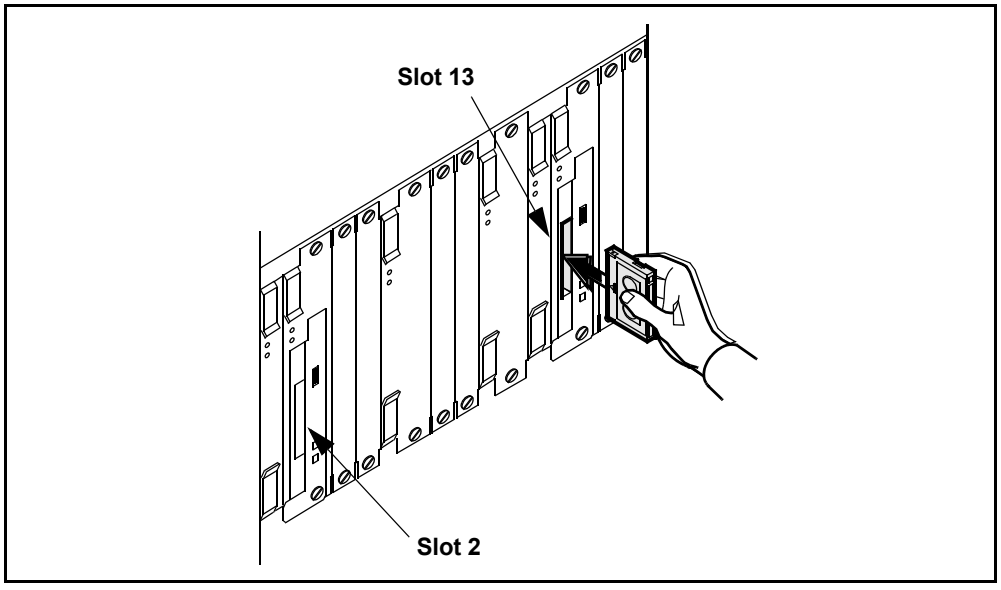
**2** Log on to the CS 2000 Core Manager using the root user ID and password

**3** If you are upgrading from tape (not from ESD), verify that the procedure Uploading the software from tape to a disk on page 197 has been completed. If not, perform the procedure now.

**4** Use the following table to determine your next step.

| If you are upgrading from | Do |
|---|---|
| a directory<br><br>***Note:*** A directory created during ESD or during procedure Uploading the software from tape to a disk on page 197 | step 5 |
| directly from tape (not recommended; use this option only if you are unable to upload the software from tape to a disk) | insert the tape labeled "CS2E0070 NCL 7.x (1 of 1)" into the tape drive in slot 13 (DAT1) as shown in the following figure, and continue with step 5.<br><br>***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed. |

**Main chassis tape drive**




**5** Perform the following substeps to remove all archived filesets from the system, which will free up disk space:

**a** Access the Details level:

```
# sdmmtc details
```

**b** Show all software:

```
> filter off
```

c Select all archived filesets:

```
> select all
```

***Note:*** If there are no archived filesets to remove, go to step 6.

d Remove all archived filesets:

```
> remove all
```

***Note:*** System will automatically select appropriate files to remove.

e Confirm the command:

```
> y
```

***Note:*** Once you remove the archived filesets, the state of the CS 2000 Core Manager changes to in-service trouble (ISTb), and the status of the Backup Status alarm indicates *Required*. If the backup Required alarm is disabled, the alarm will not be raised. If the alarm is enabled, perform a backup of your new system image using procedure "Creating system image backup tapes (S-tape) manually" in the Security and Administration section. If you choose not to perform a backup, you can force-clear the alarm using procedure "Clearing a system image backup Required or Failed alarm" in the Fault section.

6 Exit the maintenance interface:

```
> quit all
```

7 Use the following table to determine your next step.

| If you | Do |
|---|---|
| have pre-loaded the software from tape, as described in procedure Uploading the software from tape to a disk on page 197 | go to step 10 |
| are upgrading your system from an ESD directory (not after tape pre-loading) | go to step 9 |
| are upgrading your system directly from tape inserted in slot 13 | go to step 8 |

8 Install the Upgrade Tools fileset:

```
# installp -ad /dev/rmt1 SDM_UPGRADE.tools
```

***Note:*** When prompted, press the Enter key again.

Go to step 10.

**9** Install the Upgrade Tools fileset:

```
# installp -ad <directory> SDM_UPGRADE.tools
```

where

**<directory>**
is the directory where the software is located

***Note:*** When prompted, press the Enter key again.

**10** Install the ESUP software by completing the following substeps.

**a** Begin the installation:

```
# esupinstall
```

**b** When prompted, select the location of the software load: one of the following values:

- `0` - if you are upgrading directly from tape inserted in slot 2

  ***Note:*** Nortel Networks recommends that you do not use slot 2. Use slot 13 instead.

- `1` - if you are upgrading directly from tape inserted in slot 13
- `D` - if you are upgrading from a directory (ESD or pre-loaded from tape)
- **`ABORT`** - if you wish to abort the procedure

| If you entered | Do |
|---|---|
| `D` | step c |
| `0, 1, or ABORT` | step d |

**c** When prompted, enter the directory path where the software load is located.

**d** Wait until the system completes the installation (up to 10 min). When completed, the following message is displayed:

```
SUCCESSFULLY INSTALLED SOFTWARE FOR ESUP
```

**11** Verify the Sysdump devices by completing the following steps.

Start the verification:

**# sysdumpdev -l**

| If the following message is displayed | Do |
|---|---|
| primary /dev/sysdump0<br>secondary /dev/sysdumpnull<br>copy directory /var/adm/ras<br>forced copy flag FALSE<br>always allow dump FALSE<br>dump compression OFF | step 12 |
| primary /dev/sysdump0<br>secondary /dev/sysdump1<br>copy directory /var/adm/ras<br>forced copy flag FALSE<br>always allow dump FALSE<br>dump compression OFF | step 13 |

**12** Change the sysdump devices to sysdump1:

**#sysdumpdev -P -s /dev/sysdump1**

The following message is displayed.

```
primary/dev/sysdump0
secondary/dev/sysdump1
copy directory/var/adm/ras
forced copy flagFALSE
always allow dumpFALSE
dump compressionOFF
```

**13** You have completed this procedure.

## Upgrade the software

**ATTENTION**
All application filesets are upgraded during this procedure, except the SDM Billing Application (SBA), the SBA Automatic File Transfer (AFT) application, the DNBD Call Data Delivery (LI) application, and the ONE FTAM Software (LI) application filesets. If required, upgrade these application filesets after the ESUP portion of this procedure.

This procedure can be performed from either a VT100 console or a telnet session.

| If you choose | Do |
|---|---|
| telnet session | step 1 |
| VT100 console | step 2 |

***At the PC or UNIX workstation***

**1** Establish a telnet connection to the CS 2000 Core Manager by completing the following substeps.

**a** Open a terminal window that is VT100 compatible.

**b** Log onto the CS 2000 Core Manager from the terminal window prompt:

```
telnet <ip_address>
```

where

**<ip_address>**
is the IP address of the CS2000 Core Manager

**c** Keep window size at 80x24.

***At the VT100 console or telnet session***

**2** When prompted, enter the login ID and password for the root user.

**3** Begin the upgrade:

```
# esup
```

The system lists all stages of the upgrade and gives you the choice to continue the upgrade or to abort (go/abort).

4 To continue, type

```
> go
```

5 When prompted to select the media type, use the following table to determine your next step.

| If you are upgrading from | Do |
|---|---|
| a directory (ESD or pre-loaded from tape) | type 2 and press the Enter key, then go to step 9 |
| directly from tape | type 1 and press the Enter key, then go to step 6 |

***Note:*** If you wish to abort, enter 0.

6 The system displays the following response:

```
The following device has been selected to
perform the upgrade:

Media Type: TAPE /dev/rmt1

Continue (yes or no)>
```

***Note:*** /dev/rmt1 is the device name for the tape drive in slot 13 (DAT1).

Verify that the displayed media type is correct and continue the upgrade:

```
> yes
```

The system reports all automatic sub-processes that are taking place during this stage, as well as the start time for each process. Also displayed is an estimated duration for each process.

***Note:*** The estimated time may not be exact. Allow some additional time. However, if the process continues much longer than the estimate, contact your next level of support.

7 When prompted to insert the tape, use the following table to determine your next step.

| If at this point the tape | Do |
|---|---|
| is not inserted | insert the tape labeled “CS2E0070 NCL 7.x (1 of 1)” into the tape drive in slot 13, enter **go** and press the Enter key |
| is inserted | make sure that the tape is in the correct drive, enter **go** and press the Enter key |

8 The system verifies the content of the tape and informs you if the wrong tape is inserted.

| If the inserted tape is | Do |
|---|---|
| correct | step 13 |
| not correct | replace it with the tape labeled “CS2E0070 NCL 7.x (1 of 1)”, enter **go** and press the Enter key, then go to step 13 |

9 The system confirms that you have selected Media Type: DISK. Continue the upgrade:

```
> yes
```

***Note:*** If you wish to abort the procedure, enter **no**.

The system reports all automatic sub-processes that are taking place during this stage, as well as the start time for each process. Also displayed is an estimated duration for each process.

***Note:*** The estimated time may not be exact. Allow some additional time. However, if the process continues much longer than the estimate, contact your next level of support.

**10** When prompted to enter the directory location for the new NCL load, use the following table to determine your next step.

| If the CS2E0070 load files | Do |
|---|---|
| are located in the default ESD directory /swd/sdm/esd | enter `go` and press the Enter key |
| are not located in the default directory, or are located in the directory created during the procedure Uploading the software from tape to a disk on page 197. | enter the directory path where the files are located, then press the Enter key |

**11** The system verifies the content of the directory and informs you if you entered the wrong path.

| If the directory is | Do |
|---|---|
| correct | step 12 |
| not correct | re-type the directory path, press the Enter key, then go to step 12 |

**12** When prompted to enter directory location for additional OS filesets, use the following table to determine your next step.

| If the additional OS filesets | Do |
|---|---|
| are located in the default ESD directory /swd/sdm/esd | enter `go` and press the Enter key |
| are not located in the default ESD directory, or are located in the directory created during the Uploading the software from tape to a disk procedure | enter the directory path where the files are located, then press the Enter key. |

The system continues the upgrade procedure until it prompts you to busy the SDM.

**13**

**ATTENTION**

Before the system prompts you to busy the SDM it automatically sets AFT and SBA applications into offline state. ESUP will automatically brings them back in service after the SDM reboots and is returned into service.

***At the PC or UNIX workstation***

**14** Establish a telnet connection to the CS 2000 Core Manager by completing the following substeps.

**a** Open a terminal window that is VT100 compatible.

**b** Log onto the CS 2000 Core Manager from the terminal window prompt:

```
telnet <ip_address>
```

where

**<ip_address>**
is the IP address of the CS 2000 Core Manager

**c** Keep window size at 80x24.

**d** When prompted, enter the login ID and password for the root user.

**15** If your office is equipped with a third-party Call Agent, continue with step 16. Otherwise, go to step 17.

**16** Busy the CS 2000 Core Manager by completing the following substeps.

**a** Access the SDM maintenance level by typing

```
# sdmmtc;mtc
```

**b** Busy the CS 2000 Core Manager by typing

```
> bsy
```

**c** Confirm the busy request by typing

```
> y
```

**d** Continue with step 18.

***At the MAP display***

**17** Busy the CS 2000 Core Manager level at the MAP display by completing the following substeps.

**a** Access the SDM level of the MAP display:

```
> mapci;mtc;appl;sdm
```

**b** Busy the CS 2000 Core Manager:

```
> bsy
```

**c** Confirm the busy request:

```
> y
```

***At the MAP display***

**18** Verify that each billing stream has entered the active backup mode by posting and querying each of your billing streams.

```
> sdmbil;post<stream>;query
```

***At the VT100 console or telnet session***

**19** Continue the procedure, by typing

```
> go
```

***Note:*** Until the CS 2000 Core Manager is fully busy, the system displays the following message: `Waiting for SDM BSY`.

The system automatically reboots. This process can take up to ten minutes.

***Note:*** If the upgrade is being done via telnet, the system reboot will close the telnet session.

**20** Wait until the system has finished rebooting. Use the following table to determine your next step:

| If you are using | Do |
|---|---|
| VT100 console | go to step 23 |
| Telnet session | go to step 21 |

The upgrade automatically continues.

***At the PC or UNIX workstation***

**21** The reboot process closed the previous telnet session. Re-establish a new telnet session by:

**a**

```
telnet <ip_address>
```

where

**<ip_address>**
is the IP address of the SDM

**b** Keep window size at 80x24

***At the VT100 console or telnet session***

**22** When prompted, enter the login ID and password for the root user.

**23** Continue the upgrade:

```
# esup
```

**24** Use the following table to determine your next step.

| If you are | Do |
|---|---|
| prompted to configure DDMS clients | step 25 |
| not prompted to configure DDMS clients | step 31 |

**25** Follow sub-steps a through c to configure the DDMS clients.

***Note 1:*** The DDMS clients are the CS 2000 Management tools servers with the SESM load.

***Note 2:*** To display a list of existing client IP addresses, from the DDMS Clients Configuration menu select option “3. List existing clients”. You can then add clients as required.

**a** Add a new client:

```
> 1
```

**b** When prompted, enter the IP address for each of the CS 2000 Management tools servers. Press the Enter key after each entry and type “done” once you have entered all the IP addresses.

**c** Exit the DDMS clients configuration screen:

```
> 0
```

***Note:*** You can reconfigure the OSS Comms Svcs at any time through the sdmmtc config level.

**26** Use the following table to determine your next step.

| If your office | Do |
|---|---|
| is equipped with a third-party Call Agent | step 27 |
| is not equipped with a third-party Call Agent | step 35 |

***At the PC or UNIX workstation***

**27** Access the Application level of the CS 2000 Core Manager maintenance interface:

```
# sdmmtc appl
```

**28** Locate and busy the OSS Comms Svcs application:

```
> bsy <x>
```

where

**<x>**
is the number next to the OSS Comms Svcs fileset

**29** Return the OSS Comms Svcs application to service:

```
> rts <x>
```

where

**<x>**
is the number next to the OSS Comms Svcs fileset

**30** Continue with step 31 (the system automatically returns to service).

***At the VT100 console or telnet session***

**31** Use the following table to determine your next step.

| If your office | Do |
|---|---|
| is equipped with a third-party Call Agent | continue with step 34 (the system automatically returns to service) |
| is not equipped with a third-party Call Agent | when prompted to return the SDM to service, go to step 35 |

***At the PC or UNIX workstation***

**32** The reboot process closed the previous telnet session. Re-establish a new telnet session by completing the following substeps:

**a** Connect to the SDM from the terminal window prompt:

```
telnet <ip_address>
```

where

**<ip_address>**
is the IP address of the SDM

**b** Keep window size at 80x24

***At the VT100 console or telnet session***

**33** When prompted, enter the login ID and password for the root user.

**34** Continue the procedure:

```
# esup
```

*The upgrade continues until you are prompted to return the SDM to service.*

***At the MAP display***

**35** When prompted, return the CS 2000 Core Manager to service by completing the following substeps.

**a** Access the SDM level of the MAP display:

```
> mapci;mtc;appl;sdm
```

**b** Return the CS 2000 Core Manager to service:

```
> rts
```

***At the VT100 console or telnet session***

**36** Continue by typing

```
> go
```

***Note:*** "Waiting for SDM RTS" message will appear until the system is fully in service. It will take 2 to 10 minutes for the CS 2000 Core Manager to return to service.

***At the MAP display***

**37** Verify that all billing streams are either in-service or in recovery on the CS 2000 Core Manager side:

```
> sdmbil;post<stream>;query
```

**38** Use the following table to determine your next step.

| If your system | Do |
|---|---|
| has SAM21 EM application, and you are upgrading from CS2E0005 to CS2E0070 or from CS2E0006 to CS2E0070 loads | step 39 |
| does not have SAM21 EM application | step 40 |

***At the PC or UNIX workstation***

**39** Configure SAM21 EM application by completing the following substeps.

***Note:*** Before you begin, have your records from the Pre-upgrade requirements section ready for reference.

**a** Access the Config level:

```
# sdmmtc config
```

**b** Start the configuration process:

```
> config <x>
```

where

**<x>**
is the number next to the SAM21 Manager application

**c** When prompted whether DNS is supported on SAM21 EM workstations, enter **Y** (yes) or **N** (no), and press the Enter key.

| If you enter | Do |
|---|---|
| **Y** (yes) | substep d |
| **N** (no) | substep e |

**d** When prompted, enter the CommonName from the certificate on the CS 2000 Management Tools server that is configured to run the Login Application, and press the Enter key.

**e** When prompted, enter the host name of the CS 2000 Management Tools server that is configured to run the Login Application, and press the Enter key.

**f** Exit the maintenance interface:

```
> quit all
```

***At the VT100 console or telnet session***

**40** The system displays a message confirming that the CS 2000 Core Manager has been upgraded successfully. Read the message and follow the on-screen instructions. Use the following table to determine your next step.

| If you wish to | Do |
|---|---|
| continue the upgrade | step 41 |
| abort the upgrade | type **`abort`** and press the Enter key. Complete the procedure “Recovering the system from an ESUP failure” in *Upgrading the CS 2000 Core Manager*, NN10060-461. |

**41** Use the following table to determine your next step.

| If you | Do |
|---|---|
| have SBA on your system | step 42 |
| do not have SBA on your system | step 45 |

***At the PC or UNIX workstation***

**42** Establish a telnet connection to the SDM by completing the following substeps.

**a** Open a terminal window that is VT100 compatible.

**b** Log onto the SDM from the terminal window prompt:

```
telnet <ip_address>
```

where

**<ip_address>**
is the IP address of the SDM

**c** Keep window size at 80x24.

**d** When prompted, enter the login ID and password for the root user.

**43** Query the status of each RTB stream that was InSv before the upgrade (refer to your records from the Pre-upgrade requirements section). If none were recorded, continue with step 45.

***Note:*** If required, refer to the procedure “Querying the status of RTB for a billing stream” in the Accounting document.

**44** If the status of RTB for any stream changed from InSv to ManB, manually return each of these RTB stream instances to service. Refer to the procedure “Returning RTB stream instance to service” in the Accounting document.

***At the VT100 console***

**45**



**CAUTION**
**Possible loss of service**
Once you begin the re-integration process, you cannot use the abort command to return to the previous version of the CS 2000 Core Manager software. If you decide to return to the previous version of the CS 2000 Core Manager software after the reintegration process, you must take the CS 2000 Core Manager off-line and restore the previous version of the CS 2000 Core Manager software from an S-tape. There is a loss of service for several hours when you restore the previous software.

Begin the integration process:

```
> go
```

When the system confirms that the upgrade is complete, go to step 46.

**46** Complete any post-upgrade commissioning:

```
# sdmconfig auto
```

**47** If you have the SDM Billing Application (with or without the SBA Automatic File Transfer application), proceed to the section Upgrade the SBA and AFT applications on page 562, and then return to step 48.

**48** If you have the DNBD Call Monitoring Application on your system, upgrade it by following the appropriate procedure in the International Lawful Intercept ISN06/MMP, NN10194, and then return to step 49.

**49** Use the following table to determine your next step.

| If you | Do |
|---|---|
| need to install new CS2E0070 applications and services | step 50 |
| do not need to install new CS2E0070 applications and services | step 51 |

**50** Install new CS2E0070 applications and services using the procedures in the CS 2000 Core Manager suite of information modules that correspond to the applications or services you want to install. When complete, return to this procedure and proceed to step 51.

***Note 1:*** Only install the required Succession applications. For a list of applications required for each Succession solution, refer to Filesets to solution mapping on page 532.

***Note 2:*** Install new applications and services from the VT100 console.

**51** You have completed this procedure. Return to Task flow for upgrading CS 2000 Core Manager software using ESUP on page 535.

## Apply the SDM_Base.dfquery fileset

This fileset must be manually applied after an upgrade.

***At the VT100 console or telnet session***

**1** Access the maintenance interface:

```
# sdmmtc
```

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

| If upgrading from | Do |
|---|---|
| a directory (ESD or pre-loaded from tape) | step a |
| directly from tape | step c |

**a** List the filesets:

```
> apply <directory_path>
```

where

**<directory_path>**
is the directory where the filesets are located

***Note:*** <directory_path> may be the /swd/sdm/esd directory.

**b** Go to 3.

**c** List the filesets:

```
> apply <domain_number>
```

where

**<domain_number>**
indicates the domain where you inserted the tape. Type 1.

**3** Select the SDM_BASE.dfquery fileset;

```
> select <x>
```

where

**<x>**
is the number next to the SDM_BASE.dfquery fileset

**4** Apply the SDM_BASE.dfquery fileset:

```
> apply
```

Example response

```
You have selected to install the following new
filesets or fileset updates.

SDM_BASE.dfquery xx.xx.xx.x

Do you wish to proceed?

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

5 When prompted, confirm the apply command:

```
> Y
```

6 You have completed this procedure.

7 Go to Completing the CS 2000 Core Manager upgrade on page 1393.

## Upgrade the SBA and AFT applications

Complete this procedure only if you have the SDM Billing Application (with or without the SBA Automatic File Transfer application) on your system.

***Note:*** If you do not have the SBA Automatic File Transfer (AFT) application, disregard any references to AFT.

**ATTENTION**
The following steps stop the SBA for approximately 20 minutes. Ensure that adequate backup space is available on the Communication Server 2000 core before continuing with these steps. To determine the amount of backup space required, refer to “Disk space requirements in “Preparing for SBA installation and configuration” in the Accounting document. To set up the backup space, refer to procedure “Configuring the SBA on the Communication Server 2000 core” in the Accounting document.

***At the VT100 console or telnet session***

**1** Access the maintenance interface:

```
# sdmmtc
```

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

| If upgrading from | Do |
|---|---|
| a directory (ESD or pre-loaded from tape) | step a |
| directly from tape | step c |

**a** List the filesets:

```
> apply <directory path>
```

where

**<directory_path>**
is the directory where the filesets are located

***Note:*** <directory path> may be the /swd/sdm/esd directory.

**b** Go to 3.

**c** List the filesets:

```
> apply <domain_number)
```

where

**<domain_number>**
indicates the domain where you inserted the tape. Type 1.

3 Select all versions of the SDM Billing Application filesets and, if required, the SBA Automatic File Transfer filesets:

```
> select <x> <y>...
```

where

**<x> <y> . . .**
are the numbers next to the SDM Billing Application filesets and the SBA Automatic File Transfer filesets

***Note:*** If you do not have the SBA Automatic File Transfer application on your system, do not select the AFT filesets.

4 Apply the SDM Billing Application fileset and, if required, the SBA Automatic File Transfer fileset:

```
> apply
```

***Note:*** The system automatically selects the SDM_ACE fileset, which is required by the SBA and AFT applications. When you confirm the apply command, the system will automatically install the ACE fileset first.

Example response

```
You have selected to install the following new
filesets or fileset updates.

SBA Automatic File Transfer xx.xx.xx.x
SDM Billing Application xx.xx.xx.x

You did not select the following filesets that
are required by some of the selected filesets.
If you proceed, they will be applied
automatically before the selected filesets.

SDM ACE distribution x.x.x.x

Do you wish to proceed?
Please confirm ("YES", "Y", "NO", or "N")
```

5 When prompted, confirm the apply command:

```
> y
```

6 Exit the maintenance interface:

```
> quit all
```

7 If applicable, restart the AFT application as follows:

**a** Access the billing maintenance interface:

```
# billmtc
```

**b** Restart the AFT application:

```
> start <session_name>
```

*where*

**<session_name>**
is the name of the AFT session

**c** Exit the billing maintenance interface:

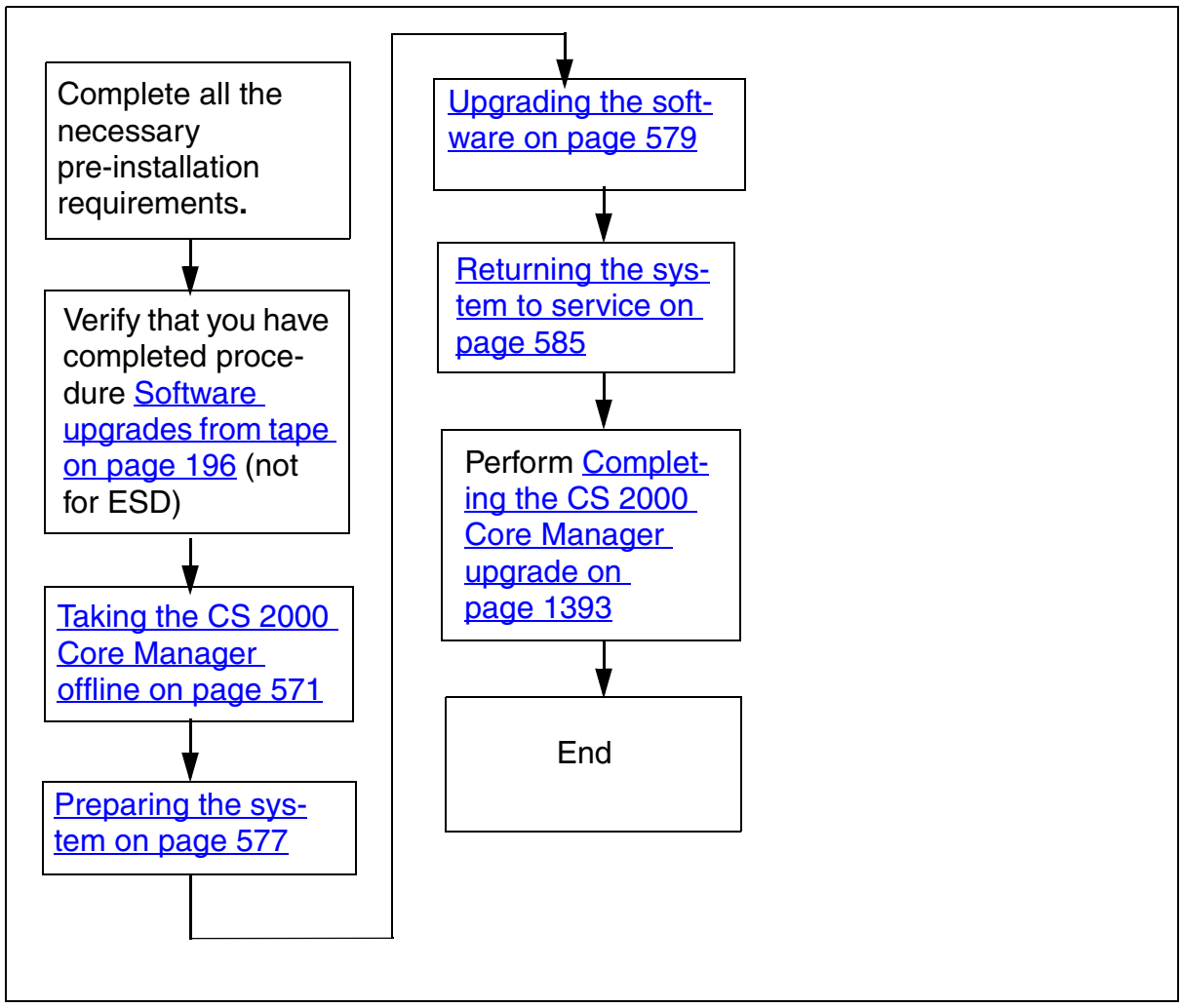
```
> quit all
```

8 Go back to step 47.

# Upgrading CS 2000 Core Manager software out of service

Use the following task flow to upgrade CS 2000 Core Manager software out of service.

**Task flow for upgrading CS 2000 Core Manager software out of service**



## Purpose

This procedure provides information about upgrading your CS 2000 Core Manager software from the latest CS2E0004, CS2E0005, or CS2E0006 release to the CS2E0070 release using the OOS Upgrade Procedure.

***Note:*** This procedure references other procedures in the CS 2000 Core Manager Upgrades, Fault Management, Configuration Management, Accounting, and Security and Administration NTPs. Ensure that you have access to those documents while performing this procedure.

During the upgrade, the system is busied and both domains are upgraded at the same time.

## Pre-upgrade requirements

Before starting this procedure, complete the following activities:

- Ensure that the latest MNCL release is installed on your system.

  Refer to “Upgrade guidelines” in *Upgrading the CS 2000 Core Manager*, NN10060-461 for the software baseline.

  ***Note:*** If you need to upgrade to the latest MNCL, refer to the MNCL release notes for instructions.

- Verify that the pre-check tasks described in the Preparing to upgrade the CS 2000 Core Manager on page 170 procedure were successfully completed seven days before starting this upgrade.
- Perform a system image backup.

  **ATTENTION**

  Nortel Networks recommends that you perform a system image backup before you upgrade the base software. Use the procedure “Creating system image backup tapes (S-tapes) manually” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

  Performing a system image backup does not back up billing data. Ensure that billing is operating properly before starting.

  If you need to revert to a prior release during an out-of-service upgrade, refer to “Performing a full restore of the software from S-tape” in *CS 2000 Core Manager Fault Management*, NN10082-911.

- Obtain the password for the root user.

You must log on to the CS 2000 Core Manager using the root user ID and password to perform the upgrade, therefore, obtain the password for the root user before you begin. Failure to log on as the root user may cause your upgrade to fail. Furthermore, ensure that no other users are logged on during the upgrade. Only the user at the VT100 console should be logged on. For a procedure used to determine who is logged on, refer to the section, “Accessing the CS 2000 Core Manager” in the Basics NTP for your core manager.

- Obtain the following information from your network administrator:
  - if your system has SAM21 element manager installed, verify whether DNS is configured on SAM21 EM client workstations
  - the host name of the CS 2000 Management Tools server that is configured to run the Login Application
  - the CommonName from the certificate on the CS 2000 Management Tools server that is configured to run the Login Application
  - the IP address of the CS 2000 Management Tools server

  ***Note:*** Record the information for reference purposes.

- Obtain the right tape if upgrading from tape. Ensure that you have the tape labeled “CS2E0070 NCL 7.x (1 of 1)”.
- If upgrading via Electronic Software Delivery (ESD), ensure the required files are in the directories you will be upgrading from, which may be the “/swd/sdm/esd” directory.

  ***Note:*** If necessary, contact your next level of support, or refer to the procedures “Preparing your system for upgrade via Electronic Software Delivery” in *Upgrading the CS 2000 Core Manager*, NN10060-461 and “Transferring and retrieving files using SFT” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

- Ensure the pserver application is installed and configured on the Preside MDM server prior to upgrading the CS 2000 Core Manager. This applies to Succession offices where the CS 2000 Core Manager needs to communicate with the Preside MDM for fault data, using the Passport log streamer application. Refer to the Passport 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting, NN10198-912, for instructions on how to configure the pserver application.
- Check the root logical volume file - potential disk space error. Make sure the root logical volume “/” file does not exceed 70% of its total size. If the “/” file system exceeds the 70% mark, you must make

more room on the “/” file system for the upgrade to be successful. For more details, contact your next level of support.

- Check for the presence of a datavg if required.
  If upgrading a rootvg-datavg, ensure datavg is present. You can check the presence of a datavg through the maintenance interface under the storage level (sdmmtc storage).
- Make sure the CS 2000 Core Manager is alarm free. If any alarms are present, refer to the Fault Management NTP for alarm-clearing procedures.
- Have VT100 terminal emulation. Before you perform this procedure, make sure that your terminal is configured for VT100 terminal emulation and that you can establish a connection to SP0 either locally or remotely through modem or terminal server.

## Upgrade notices

**ATTENTION**

Some applications are automatically removed.

If the Exception Reporting, Alarm Conduit, SDM Corba Framework, and Remote Registration System filesets are present, they are automatically removed when upgrading to CS2E0070.

## Procedures

**ATTENTION**

Read the instructions in Pre-upgrade requirements on page 566 and Upgrade notices on page 568, and complete any necessary activities before you proceed with the upgrade.

**ATTENTION**

Nortel Networks recommends that you deliver unprocessed billing files downstream. Ensure that no unprocessed billing file remains on the system.

**ATTENTION**

Nortel Networks recommends that you complete the entire upgrade procedure in one session, without interruption, to avoid any unnecessary disruption in billing file processing.

## Preparing for a software upgrade from tape

### *At the VT100 console*

1 If you are upgrading from tape, verify that the procedure Software upgrades from tape on page 196 has been completed.

2 You have completed this procedure.

## Taking the CS 2000 Core Manager offline

***At the console connected to SP0 (local VT100 terminal or remote access)***

**1** Log on to the CS 2000 Core Manager using the root user ID and password.

**2** If the SuperNode Billing Application (SBA) is installed on your system, determine the operational status of the SBA application and then record this status for future reference; you will be asked to return the SBA application to this operational state later on in this procedure. Use the following table to determine your first step.

| If the SBA application | Do |
|---|---|
| is installed on your system and is not busy or offline | step 3 |
| is installed on your system, but is busy or offline | step 23 |
| is not installed on your system | step 24 |

***At the MAP display***

**3** Busy all billing streams on the core. Post the required billing stream:

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

*where*

**<stream>**
is the name of the billing stream

***Note:*** To display the details about a stream, refer to the procedure “Listing billing streams” in the Accounting NTP. To list all files currently stored in a stream, refer to the procedure “Listing billing files” in the Accounting NTP.

**4** Busy the posted stream:

```
> bsy
```

**5** Confirm the request to **bsy**:

```
> y
```

**6** Verify that the status of the posted stream changed to ManB (manual busy):

```
> status
```

**7** Repeat steps 3 through 6 for each billing stream.

**8** Examine the SDMB 621 logs to determine the volume names and backup file names for each billing stream:

```
> logutil;open sdmb 621:back 10
```

In response to the command, the system displays the sdmb 621 logs.

Example sdmb 621 log:

```
BRW_CENTREX  SDMB621  AUG03  14:19:05  4500  INFO SDM BILLING BACKUP
            STREAM=  AMA:   Backup started to record to file.
            VOLUME=  S00DAMA        FILE=  BACK01AMA_01
```

**9** For each configured billing stream, verify that at least one backup file exists on at least one of the configured backup volumes.

Display the names of the backup volumes configured for the specified billing stream:

```
> mapci;mtc;appl;sdmbil;conf view <stream>
```

*where*

**<stream>**
is the name of the billing stream

**10** Verify that SBA backup file exists on at least one of the displayed backup volumes:

| If the backup disk type is | Enter command |
|---|---|
| DDU | > **dskut;liv <volume name> all** |
| IOP | > **diskut;lf <volume name>** |
| SLM | > **diskut;lf <volume name>** |

***Note:*** The name of each backup file begins with “BK”.

**11** Repeat steps 9 and 10 for each billing stream.

***At the console connected to SP0 (local VT100 terminal or remote access)***

**12** Close all unprocessed billing files by performing the procedure “Closing billing files”, located in your Accounting NTP.

**13** Send downstream all unprocessed billing files. Use the following table to determine the procedure to perform.

| File transfer mode | Procedure in the Accounting NTP |
|---|---|
| Outbound file transfer (OFT) | "Sending billing files from disk" |
| Inbound file transfer (IFT) | "Retrieving billing files for a stream set to inbound file transfer" |
| Real-time billing (RTB) | "Sending billing files from disk" |
| Automatic file transfer (AFT) | No manual action is required. Wait for SBA to deliver pending billing files to the downstream destination. There should be no pending files for each AFT session.<br>Use the following commands to query AFT sessions: **`billmtc, appl, aft, aftconfg, list`**.<br>To verify which billing files for each session are still pending, enter the following commands: **`billmtc, appl, aft, query <session_name>`**. |

***Note 1:*** To display the details about a stream, refer to the procedure "Listing billing streams" in the Accounting NTP. To list all files currently stored in a stream, refer to the procedure "Listing billing files" in the Accounting NTP.

***Note 2:*** If you are unable to send billing files to a downstream destination and you want to proceed with the upgrade, Nortel Networks recommends that you backup the billing files to a DAT tape. If required, refer to the procedure "Copying billing files to tape (backup)" in the Accounting NTP.

***Note 3:*** If you need to restore the billing files from tape and you have AFT or IFT configuration, contact your next level of support for instructions. For any other configuration, you can send the billing files from tape using the procedure "Sending billing files from tape" in the Accounting NTP.

**14** Access the APPL level of the maintenance interface:

```
> sdmmtc appl
```

| If the AFT application | Do |
|---|---|
| is installed on your system | step 15 |
| is not installed on your system | step 19 |

**15** Determine the current operational status of the AFT application and then record this status for future reference; you will be asked to return the AFT application to this operational state later on in this procedure. Use the following table to determine your next step.

| If the AFT application | Do |
|---|---|
| is in service | step 16 |
| is busy | step 18 |
| is offline | step 19 |

**16** Busy the AFT application:

```
> bsy <application_number>
```

*where*

**<application_number>**
is the number next to the Automatic File Transfer application

**17** Confirm the command:

```
> y
```

**18** Offline the AFT application:

```
> offl <application_number>
```

*where*

**<application_number>**
is the number next to the Automatic File Transfer application

**19** Busy the SuperNode Billing Application (SBA):

```
> bsy <application_number>
```

*where*

**<application_number>**
is the number next to the SuperNode Billing Application

**20** Confirm the command:

```
> y
```

**21** Take the SBA offline:

```
> offl <application_number>
```

*where*

**<application_number>**
is the number next to the SuperNode Billing Application

**22** Exit from SDMMTC:

```
> quit all
```

Go to step 24

***At the console connected to SP0 (local VT100 terminal or remote access)***

**23** Use the following table to determine your next step.

| If the SBA application | Do |
|---|---|
| is busy | step 21 |
| is offline | step 24 |

***At the console connected to SP0 (local VT100 terminal or remote access)***

**24** Use the following table to determine your next step.

| If your core manager | Do |
|---|---|
| is connected to a CS 2000 - Compact | step 25 |
| is not connected to a CS 2000 - Compact | step 26 |

**25** Busy the CS 2000 Core Manager.

**a** Access the MTC level of the maintenance interface:

```
> sdmmtc mtc
```

**b** Check that the CS 2000 Core Manager is in a fault-free state. If the CS 2000 Core Manager is not in a fault-free state, correct all faults and alarms before continuing this procedure. Refer to the Fault Management NTP for alarm-clearing procedures. If you have alarms or faults that you cannot clear, stop and contact your next level of support.

**c** Busy the CS 2000 Core Manager:

```
> bsy
```

**d** Confirm the busy request:

```
> y
```

**e** Offline the CS 2000 Core Manager:

```
> offl
```

**f** Exit from SDMMTC:

```
> quit all
```

**g** Go to step 31.

***At the MAP display***

**26** Access the SDM level of the MAP display:

```
> mapci;mtc;appl;sdm
```

**27** Check that the CS 2000 Core Manager is in a fault-free state. If the CS 2000 Core Manager is not in a fault-free state, correct all faults and alarms before continuing this procedure. Refer to the Fault Management NTP for alarm-clearing procedures. If you have alarms or faults that you cannot clear, stop and contact your next level of support.

**28** Busy the CS 2000 Core Manager:

```
> bsy
```

**29** Confirm the busy request:

```
> y
```

**30** Take the CS 2000 Core Manager offline:

```
> offl
```

**31** You have completed this procedure.

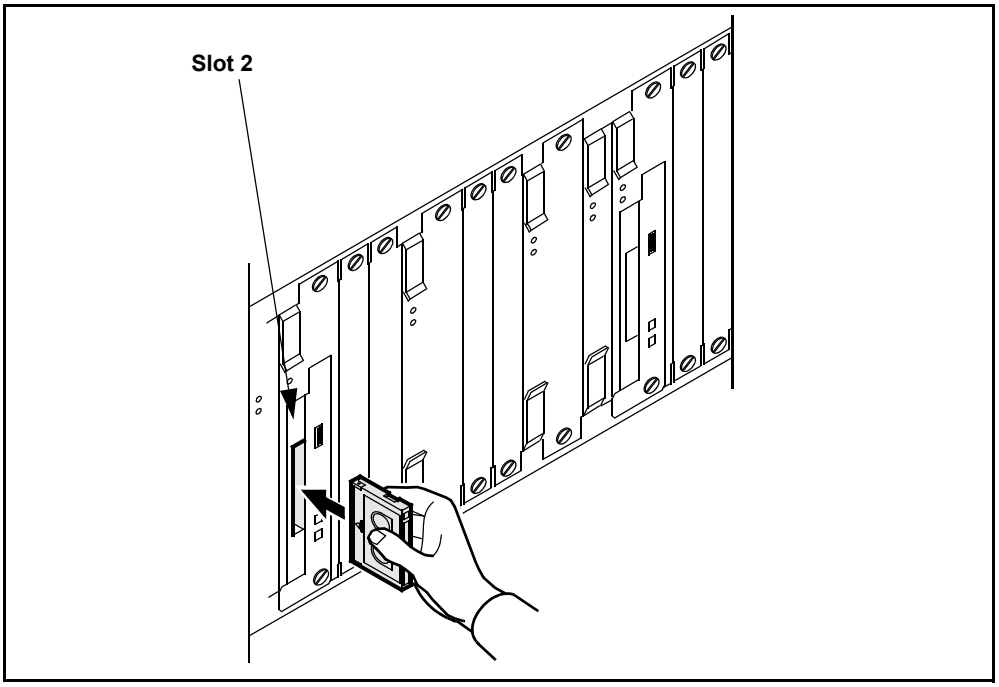
## Preparing the system

### *At the local VT100 console*

**1** Use the following table to determine your next step.

| If you are upgrading | Do |
|---|---|
| from a directory created during ESD or during the procedure Software upgrades from tape on page 196 | step 3 |
| directly from tape (not recommended; use this option only if you are unable to upload the software from tape to a disk) | insert the tape labeled "CS2E0070 NCL 7.x (1 of 1)" into the tape drive in slot 2 as shown in the following figure, and continue with step 2.<br>***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed. |

**Inserting a tape into the tape drive**




**2** If you are upgrading from the CS2E0006 release, verify the version of the tape. Otherwise, continue with step 3.

Verify the version of the tape:

```
# querytape dat0
```

*Example response*

```
SDM_VERSION.info: CS2E0070.0 : 20.87.7.0
```

The displayed product name (in this example, CS2E0070.0) must match the label on the tape that you inserted in step 1.

3 Remove all archived filesets from the system, to free up disk space. Access the Details level:

```
# sdmmtc details
```

4 Show all software:

```
> filter off
```

5 Select all archived filesets:

```
> select all
```

6 Remove all archived filesets:

```
> remove all
```

***Note:*** The system will automatically select appropriate files to remove.

7 Confirm the command:

```
> y
```

8 You have completed this procedure.

## Upgrading the software

***At the console connected to SP0 (local VT100 terminal or remote access)***

**1** From the “sdmmtc details” level, use the following table to determine your next step.

| If you are upgrading | Do |
|---|---|
| from a directory created during ESD or during the procedure Software upgrades from tape on page 196 | list the filesets: **`> apply <directory path>`**<br>***Note:*** <directory path> is the directory where your filesets are located. The directory depends on whether you are upgrading after ESD or after tape pre-loading. |
| directly from tape (not recommended; use this option only if you are unable to upload the software from tape to a disk) | list the filesets: > apply 0 and go to step 2 |

**2** Select all the new application filesets:

```
> select new
```

**3** Apply all the new software:

```
> apply
```

**4** Confirm the apply command:

```
> y
```

***Note:*** The upgrade can take up to 2.5 hours, depending on which release you are upgrading from, and how many filesets require upgrading. Wait until the upgrade is complete before you proceed.

| If the command response | Do |
|---|---|
| indicates any errors | contact your next level of support before you proceed with this procedure |
| does not indicate any errors | step 5 |

5 Use the following table to determine your next step.

| If you are | Do |
|---|---|
| prompted to configure “OSS Comms Svcs” | step 6 |
| not prompted to configure “OSS Comms Svcs” | step 8 |

6 Press the space bar to display the DDMS Clients Configuration menu.

***Note:*** To display a list of existing client IP addresses, from the DDMS Clients Configuration menu select option “3. List existing clients”. You can then add clients as required.

7 Follow sub-steps a through c to configure the DDMS clients.

***Note:*** The DDMS clients are the CS 2000 Management tools servers with the SESM load.

**a** Add a new client:

```
> 1
```

**b** When prompted, enter the IP address for each of the CS 2000 Management tools servers. Press the Enter key after each entry and type “done” once you have entered all the IP addresses.

**c** Exit the DDMS clients configuration screen:

```
> 0
```

***Note:*** You can reconfigure the OSS Comms Svcs at any time through the sdmmtc config level.

8 Use the following table to determine your next step.

| If you are | Do |
|---|---|
| prompted to configure the SAM21 EM | step 9 |
| not prompted to configure the SAM21 EM | step 10 |

9 Configure SAM21 EM application by completing the following substeps.

***Note:*** Before you begin, have your records from the Pre-upgrade requirements on page 566 section ready for reference.

**a** When prompted whether DNS is supported on SAM21 EM workstations, enter **Y** (yes) or **N** (no), and press the Enter key.

| If you enter | Do |
|---|---|
| **Y** (yes) | substep b |
| **N** (no) | substep c |

**b** When prompted, enter the CommonName from the certificate on the CS 2000 Management Tools server that is configured to run the Login Application, and press the Enter key.

**c** When prompted, enter the host name of the CS 2000 Management Tools server that is configured to run the Login Application, and press the Enter key.

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

| If the system | Do |
|---|---|
| prompts you to reboot | step 11 |
| does not prompt you to reboot | press Enter, and continue with step 16 |

**11** When prompted, confirm the system reboot:

```
> y
```

**12** Once the system has finished rebooting, log into the CS 2000 Core Manager using the root user ID and password.

**13** Wait until all cards at the hardware level are in service before you proceed. Monitor the status of the cards as described in steps 14 and 15.

**14** Access the hardware level of the maintenance interface:

```
# sdmmtc hw
```

**15** Check that no faults exist on the CS 2000 Core Manager:

```
> querysdm flt
```

***Note:*** An SDM300 report, which indicates “Connection has been lost to core via DS512 CM link down. Heartbeat stopped on SDM”, will be present since the CS 2000 Core Manager is

out of service. When you bring the CS 2000 Core Manager back in to service, the link and heartbeat are re-established.

| If | Do |
|---|---|
| faults are present (with the exception of the SDM300 report) | correct the faults using the procedures in the Fault Management NTP, and return to this procedure |
| no faults are present | step 16 |

**16** Use the following table to determine your next step.

***Note:*** To verify if you have X.25, refer to your notes from the "Basic pre-checks" list in Preparing to upgrade the CS 2000 Core Manager on page 170.

| If you | Do |
|---|---|
| have X.25 | step 17 |
| do not have X.25 | proceed to the procedure Returning the system to service on page 585 |

**17** Use the following table to determine your next step.

| If you are upgrading | Do |
|---|---|
| from a directory created during ESD or during the procedure Software upgrades from tape on page 196 | list the filesets: **`> apply <directory path>`**<br>***Note:*** <directory path> may be the /swd/sdm/esd directory. |
| directly from tape (not recommended; use this option only if you are unable to upload the software from tape to a disk) | list the filesets: > apply 0 |

**18** Install the X.25 software:

```
> apply bundle x25
```

If you are upgrading directly from tape, the system prompts you to confirm the apply command.

| If you are | Do |
|---|---|
| prompted to confirm the apply command | step 19 |
| not prompted to confirm the apply command | step 25 |

**19** Confirm the apply command:

```
> y
```

Response

```
Command completed with no errors
```

| If you are | Do |
|---|---|
| prompted to reboot the system | step 20 |
| not prompted to reboot the system | press Enter and continue with step 25 |

**20** Confirm the system reboot:

```
> y
```

**21** Once the system has finished rebooting, log into the CS 2000 Core Manager using the root user ID and password.

**22** Wait until all cards at the hardware level are in service before you proceed. Monitor the status of the cards as described in steps 23 and 24.

**23** Access the hardware level of the maintenance interface:

```
# sdmmtc hw
```

**24** Check that no faults exist on the CS 2000 Core Manager:

```
> querysdm flt
```

***Note:*** An SDM300 report, which indicates “Connection has been lost to core via DS512 CM link down. Heartbeat stopped on SDM”, will be present since the CS 2000 Core Manager is

out of service. When you bring the CS 2000 Core Manager back in to service, the link and heartbeat are re-established.

| If | Do |
|---|---|
| faults are present (with the exception of the SDM300 report) | correct the faults using the procedures in the Fault Management NTP, and return to this procedure |
| no faults are present | step 25 |

**25** You have completed this procedure.

## Returning the system to service

**26** After returning your CS 2000 Core Manager to service, consult the notes you recorded about the pre-upgrade operational status of the SBA application in step 2 and about the pre-upgrade operational status of the AFT application in step 15 of the procedure, Taking the CS 2000 Core Manager offline on page 571.

***At the console connected to SP0 (VT100 or remote access)***

**27** Use the following table to determine your next step.

| If your core manager | Do |
|---|---|
| is connected to the CS 2000 - Compact | step 28 |
| is not connected to the CS 2000 - Compact | step 29 |

**28** Return the CS 2000 Core Manager to service.

**a** Access the MTC level of the maintenance interface:

```
> sdmmtc mtc
```

**b** Busy the CS 2000 Core Manager:

```
> bsy
```

**c** Return the CS 2000 Core Manager:

```
> rts
```

**d** Exit from SDMMTC:

```
> quit all
```

**e** Go to step 32

***At the MAP display***

**29** Access the SDM level of the MAP display:

```
> mapci;mtc;appl;sdm
```

**30** Change the state of the CS 2000 Core Manager from offline to busy:

```
> bsy
```

**31** Return the CS 2000 Core Manager to service:

```
> rts
```

***Note:*** It will take at least 5 minutes for the CS 2000 Core Manager to return to service on the Communication Server 2000 core side.

***At the console connected to SP0 (local VT100 terminal or remote access)***

**32** Use the following table to determine your next step.

| If the SBA application | Do |
|---|---|
| was not offline prior to the upgrade | step 33 |
| was offline prior to the upgrade | step 46 |
| is not installed on your system | step 46 |

**33** Access the APPL level of the maintenance interface:

```
# sdmmtc appl
```

**34** Wait until the Table Access Service application is in service (InSv), then continue with the procedure. If the application does not return to service after 15 minutes, contact your next level of support.

**35** Busy the SBA:

```
> bsy <application_number>
```

*where*

**<application_number>**
is the number next to the SuperNode Billing Application

**36** Confirm the command:

```
> y
```

| If the SBA application | Do |
|---|---|
| was in service prior to the upgrade | step 37 |
| was busy prior to the upgrade | step 46 |

**37** Return the SBA to service:

```
> rts <application_number>
```

*where*

**<application_number>**
is the number next to the SuperNode Billing Application

| If the AFT application | Do |
|---|---|
| is installed on your system | step 38 |
| is not installed on your system | step 42 |

**38** Use the following table to determine your next step.

| If the AFT application | Do |
|---|---|
| was not offline prior to the upgrade | step 39 |
| was offline prior to the upgrade | step 42 |

**39** Busy the AFT application:

```
> bsy <application_number>
```

*where*

**<application_number>**
is the number next to the Automatic File Transfer application

**40** Confirm the command:

```
> y
```

| If the AFT application | Do |
|---|---|
| was in service prior to the upgrade | step 41 |
| was not in service prior to the upgrade | step 42 |

**41** Return the AFT application to service:

```
> rts <application_number>
```

*where*

**<application_number>**
is the number next to the Automatic File Transfer application

***At the MAP display***

**42** Return all billing streams to service. For each stream, post the required billing stream:

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

*where*

**<stream>**
is the name of the billing stream

**43** Return the posted stream to service:

```
> rts
```

**44** Repeat steps 42 and 43 for each billing stream.

***Note:*** Check to ensure that all billing streams are either in-service or in recovery on the core side before continuing.

***At the console connected to SP0 (local VT100 terminal or remote access)***

**45** Verify that billing is collecting records:

```
# query <stream_name>
```

where

**<stream_name>**
is the name of the billing stream, for example, ama.

Note the number of records, wait approximately 10 seconds, and repeat the query command for each billing stream.

| If the number of records | Do |
|---|---|
| increased from the first query command (meaning billing is working) | step 46 |
| did not increase from the first query command (meaning billing is not working) | contact your next level of support |

**46** Use the following table to determine your next step.

| If you | Do |
|---|---|
| need to install new CS2E0070 applications and services | step 47 |
| do not need to install new CS2E0070 applications and services | step 48 |

**47** Install new CS2E0070 applications and services using the procedures in the CS 2000 Core Manager information modules that correspond to the applications or services you want to install. When complete, return to this procedure and proceed to step 48.

***Note 1:*** Only install the required Succession applications. For a list of applications required for each Succession solution, refer to Filesets to solution mapping on page 532 in the Upgrades section.

***Note 2:*** Install new applications and services from the console connected to SP0 (local VT100 terminal or remote access).

**48** You have completed this procedure. Go to Completing the CS 2000 Core Manager upgrade on page 1393.

# Upgrading the CS 2000 Core Manager with software patches

## Purpose

The information that follows indicates how to upgrade your CS 2000 Core Manager with software patches, and includes the following procedures:

- Setting the schedule to apply fixes automatically
- Applying fix filesets manually
- Changing the default fixes directory

**Attention**
Before applying the fixes fileset you should capture the session file. See Preparing to upgrade the CS 2000 Core Manager on page 170.

Upgrading your CS 2000 Core Manager with software fixes involves replacing entire filesets. Fix filesets are delivered to you electronically from the Regional Patch Selector (RPS).

***Note:*** Patches for the CS 2000 Core Manager are referred to in this document as fix filesets.

The Regional Patch Selector (RPS) is an automated patch management and delivery system. RPS maintains information about patches and offices, calculates which patches are required in each office, and uploads the patches to the required sites.

Once your office information is entered in RPS, you will receive any fix filesets that apply to the CS 2000 Core Manager configuration for that office. The fix filesets you receive replace installed versions of the same filesets on your CS 2000 Core Manager.

***Note:*** If you have multiple CS 2000 Core Manager locations, you can choose to have each location set up in RPS, or have only one location set up in RPS. When you choose to have a single location set up in RPS, you are responsible for propagating any fix filesets to the other CS 2000 Core Manager locations if and when required.

Fix filesets are sent to the location specified in RPS, which can be the CS 2000 Core Manager itself or an intermediate server that has a connection to the CS 2000 Core Manager. When the fix filesets are sent directly to the CS 2000 Core Manager, they are placed in a configured directory (refer to Location of fix filesets on page 593 for more details

on the configured directory). When the fix filesets are sent to an intermediate server, they are placed in a dropbox.

A release notes file is sent with each fix fileset. This file is in ASCII format and contains information about the fix.

RPS collects the “<clli>.informfile” from the CS 2000 Core Manager itself or from the dropbox on the server at configurable intervals, and delivers any fix filesets to your office as soon as they are available in RPS.

If your office is set up with an intermediate server connected to the CS 2000 Core Manager, you need to move or copy the fix filesets from the dropbox on the server to the configured directory on the CS 2000 Core Manager. You also need to ensure that your latest “<clli>.informfile”, located in “/swd/sdm”, is available in the dropbox on the server when RPS is scheduled to collect it.

> ***Note:*** You can transfer the fix filesets from the dropbox to the CS 2000 Core Manager, and the “<clli>.informfile” (ASCII file) from the CS 2000 Core Manager to the dropbox using file transfer protocol (FTP), Secure file transfer (SFT), or SFT2. To use SFT, refer to the procedure “Transferring and retrieving files using SFT” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

You are notified through e-mail when fix filesets have been successfully delivered to your site.

Once the fix filesets are accessible in the configured directory on the CS 2000 Core Manager, they need to be applied. Fix filesets that do not require user intervention can be applied automatically according to a set schedule. Refer to Automatic installation of fix filesets on page 592. Fix filesets that require user intervention need to be applied manually. Refer to Manual installation of fix filesets on page 593.

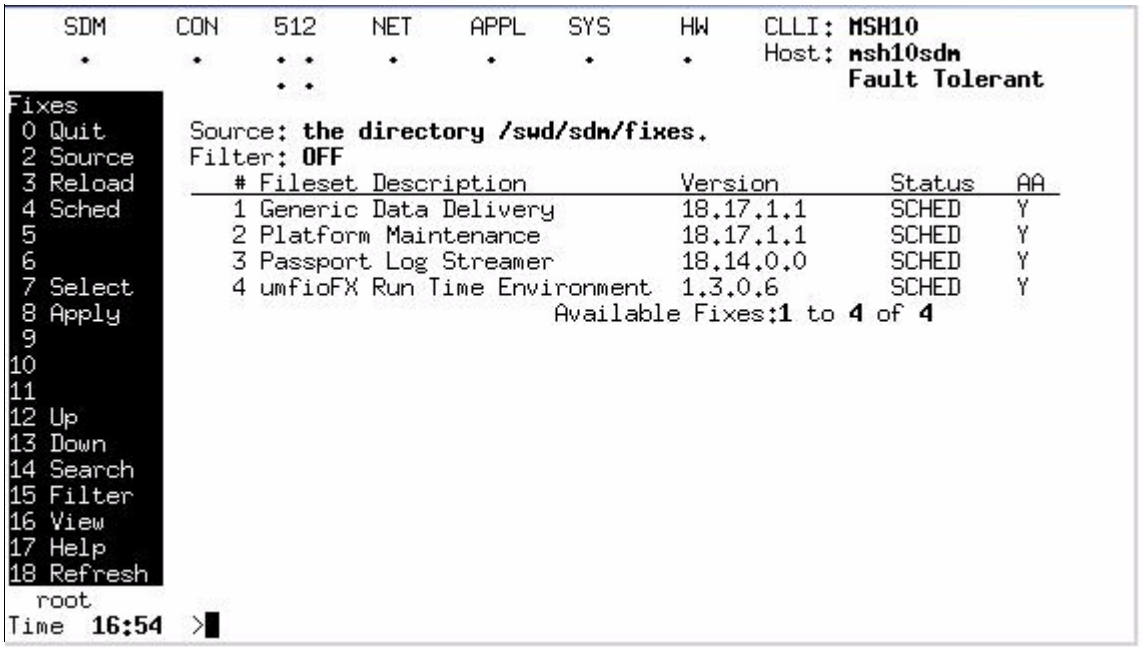
Once the fix filesets have been successfully applied, either automatically or manually, they are deleted from the configured directory. The associated release notes, if present, are also deleted.

At any time, you can remove a fix fileset and restore a previous version of the fileset using the remove command at the Details level of the maintenance interface.

## Automatic installation of fix filesets

You can set the scheduled time for when you want fix filesets to be automatically applied from the Fixes level. The fix filesets that can be auto-applied have “Y” under header “AA” (auto apply), and the fix filesets that are scheduled to be auto-applied have a status of “SCHED” under header “Status”, as shown in the following figure.

### Fixes level screen




***Note:*** If any fix filesets have a status of “INCOMP” (incomplete), meaning that the fix fileset has dependencies that have not been installed and are not available, contact your Nortel Networks representative.

Fix filesets that are scheduled to be applied automatically can only be applied from the configured directory on the CS 2000 Core Manager. Refer to Location of fix filesets on page 593 for more details on the configured directory.

You can apply fix filesets manually outside of the specified schedule. Refer to Manual installation of fix filesets on page 593.

***Note:*** The system generates log SDM610 when a fix fileset, scheduled to be applied automatically, is applied successfully or fails to apply. If you receive this log because a fix fileset failed to apply, contact your Nortel Networks representative.

## Manual installation of fix filesets

You need to manually apply fix filesets that require a reboot or have prerequisite filesets that need to be installed and require a reboot. The fix filesets that you need to apply manually have “N” under header “AA” (auto apply), and “AVAIL” under header “Status”.

## Location of fix filesets

The directory path to the fixes default directory on your CS 2000 Core Manager, is “/swd/sdm/fixes”. You can change the default fixes directory using the procedure that follows.

***Note:*** The directory must have a minimum of 200 MB of available space. The recommended amount of available space is 400 MB, which is the default.

## Procedures

### Applying fix filesets manually

***At the CS 2000 Core Manager***

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

**2** Access the SWIM level:

```
# sdmmtc swim
```

**3** Access the Fixes level:

```
> fixes
```

***Note:*** Ensure the fix filesets are accessible in the configured directory on the CS 2000 Core Manager (refer to Location of fix filesets for more details on the configured directory).

**4** Select the fix fileset you want to apply:

```
> select <n>
```

*where*

**<n>**
is the number next to the fix fileset you want to apply

**5** Apply the fix fileset:

```
> apply
```

**6** You have completed this procedure.

## Setting the schedule to apply fixes automatically

### *At the CS 2000 Core Manager*

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

2 Access the SWIM level:

```
# sdmmtc swim
```

3 Access the Fixes level:

```
> fixes
```

***Note:*** If you are accessing the Fixes level for the first time, you are prompted to enter the size of the fixes source directory, and the path of a new logical volume to be created for fixes. The minimum size is 200 MB and the maximum size is 1000 MB. The recommended size is 400 MB, which is the default.

*Response*

```
The /swd/sdm/fixes directory has been
successfully created.
Press ENTER to continue.
```

4 Press the Enter key to continue.

***Note:*** If the system responds with the message: `The directory /swd/sdm/fixes does not exist or cannot be read`, stop the procedure and contact your next level of support. Otherwise, continue with the following step.

5 To set the time interval, enter the schedule level:

```
> sched
```

*Example response*

```
Choose the interval desired:

1. Monthly
2. Weekly
3. Daily
4. None

Enter a number from 1 to 4 to make your choice
or type abort:
```

6 Enter the number that is next to the interval you want, press the Enter key, and complete the prompts for the specified interval.

7 When prompted, confirm your entry:

```
> y
```

*Response*

```
Auto fix schedule has been updated.

Press Enter...
```

8 Press Enter to return to the Fixes level.

9 You have completed this procedure.

## Changing the default fixes directory

### *At the CS 2000 Core Manager*

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

2 Access the swim level:

```
# sdmmtc swim
```

3 Access the Options level:

```
> options
```

4 Change the value of the default fixes directory:

```
> change 2
```

5 Enter the new value for the default fixes directory, and press the Enter key.

***Note:*** Enter the full directory path when specifying a directory.

*Response*

```
Change 2 - Command complete
```

6 Access the Fixes level:

```
> fixes
```

7 Press Enter to confirm the changed default fixes directory.

8 You have completed this procedure.

# Upgrading the CPU controller modules

## Purpose

Use this procedure when you want to upgrade the CPU controller modules independently from the CS 2000 Core Manager software.

**ATTENTION**
This procedure requires the complete shutdown of the CS 2000 Core Manager and all its applications. Upgrading a pair of CPUs can require two to four hours of a maintenance window to complete.

Refer to “Hardware baselines” in *Upgrading the CS 2000 Core Manager, NN10060-461*. for a list of the CPU modules that are supported.

## Prerequisites



**CAUTION**

**Risk of service disruption**

This upgrade stops the CS 2000 Core Manager billing Application. Ensure that adequate backup space is available on the core before continuing with this procedure. To determine the amount of backup space required, refer to “Disk space requirements in “Preparing for SBA installation and configuration” in the Accounting document. To set up the backup space, refer to “Configuring the SBA on the Communication Server 2000 core” in the Accounting document.

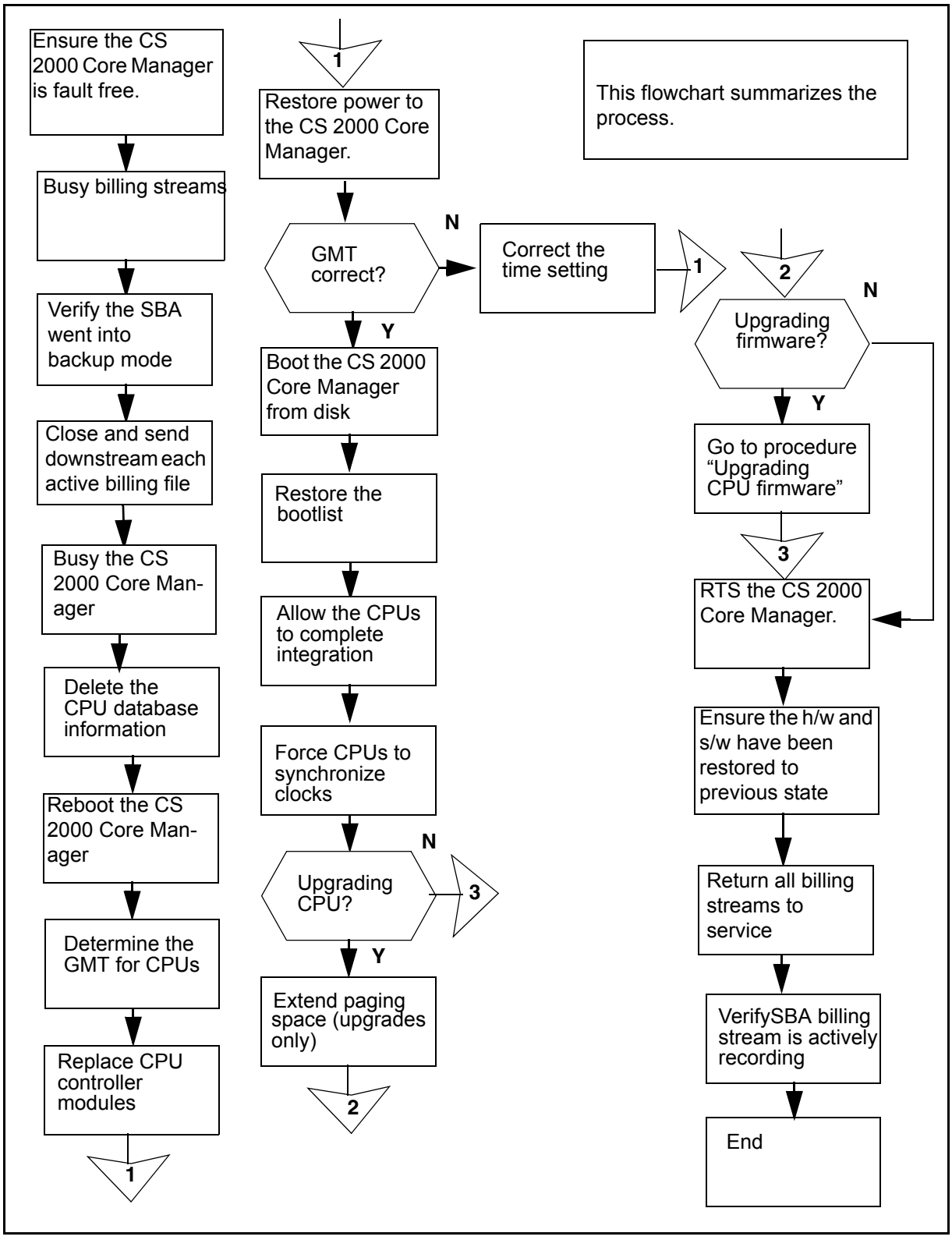
**ATTENTION**

Nortel Networks recommends that you perform a system image backup before you upgrade the CPUs. Refer to the procedure “Creating system image backup tapes (S-tapes) manually” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

## Task flow diagram

The following task flow diagram provides an overview of the upgrade process. Use the instructions in the procedures that follow the flowchart to complete the tasks.

## Task flow for Upgrading the CPU controller modules



# Procedure

## Upgrading the CPU controller modules

### *At the MAP display*

1 Ensure that you have configured adequate backup space and performed a system image backup.

2 Ensure that the CS 2000 Core Manager hardware and software applications are fault-free, or that faults are understood and acceptable.

***Note:*** Any alarms that recur after a CPU upgrade should be understood, and any new alarms should be recognized and resolved without delay. If this does not occur, contact your next level of support.

3 Busy all billing streams on the core. Post the required billing stream:

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

*where*

**<stream>**
is the name of the billing stream

4 Busy the posted stream:

```
> bsy
```

5 Repeat steps 3 and 4 for each billing stream.

6 For each configured billing stream, verify that at least one backup file exists on at least one of the configured backup volumes.

Display the names of the backup volumes configured for the specified billing stream:

```
> mapci;mtc;appl;sdmbil;conf view <stream>
```

*where*

**<stream>**
is the name of the billing stream

7 Verify that an SBA backup file exists on at least one of the displayed backup volumes:

```
> diskut;lf <backup_volume>
```

*where*

**<backup_volume>**
is the name of the selected backup volume

***Note:*** The name of each backup file begins with “BACK”.

**8** Repeat steps 6 and 7 for each billing stream.

***At the local or remote VT100 console***

**9** Log on to the CS 2000 Core Manager using the root user ID and password

**10** Close and send downstream all unprocessed billing files. Use the following table to determine your specific method.

| Task | File transfer mode | Procedure in the Accounting document |
|---|---|---|
| Close billing files | All | “Closing billing files” |
| Send billing files downstream | Outbound file transfer (OFT) | “Sending billing files from disk” |
| | Inbound file transfer (IFT) | “Retrieving billing files for a stream set to inbound file transfer” |
| | Real-time billing (RTB) | “Sending billing files from disk” |
| | Automatic file transfer (AFT) | No manual action is required. Wait for SBA to deliver pending billing files to the downstream destination. There should be no pending files (at least, no more then one) for each AFT session.<br>Use the following commands to query AFT sessions: **`billmtc, appl, aft, aftconfg, list`**.<br>To verify which billing files for each session are still pending, enter the following commands: **`billmtc, appl, aft, query <session_name>`**. |

***Note:*** To display the details about a stream, refer to the procedure “Listing billing streams” in the Accounting

document. To list all files currently stored in a stream, refer to procedure “Listing billing files” in the Accounting document.

If you are unable to send billing files to a downstream destination and you want to proceed with the upgrade, Nortel Networks recommends that you back up the billing files to a DAT tape. If required, refer to procedure “Copying billing files to tape (backup)” in the Accounting document.

***Note:*** If you need to restore the billing files from tape and you have AFT or IFT configuration, contact your next level of support for instructions. For any other configuration, you can send the billing files from tape using the procedure “Sending billing files from tape” in the Accounting document.

### *At the MAP display*

**11** Access the CS 2000 Core Manager level of the MAP display:

```
> mapci;mtc;appl;sdm
```

Example response:

```
SDM InSv
```

**12** Busy the CS 2000 Core Manager:

```
> bsy
```

Response:

```
SDM is in service
This command will cause a service interruption.
Do you wish to proceed?
Please confirm ('YES', 'Y', 'N', or 'NO')
```

**13** Confirm the busy command:

```
> y
```

Response:

```
SDM Bsy initiated.
SD Bsy completed.
```

### *At the local or remote VT100 console*

**14** Log in to the CS 2000 Core Manager as the root user.

**15** Display information for the root volume group (rootvg):

```
# lsvg -p rootvg
```

Example response

```
root vg:
PV NAME  PV STATE  TOTAL PPs  FREE PPs  FREE
DISTRIBUTION
hdisk0   active    1013       499
     175..31..00..125
                                        ..168
hdisk7   active    1013       499
     170..137..00..00
                                        ..192
```

**16** Record which hard disks (physical volumes) provide rootvg storage on the CS 2000 Core Manager. (In the example shown in step 15, the hard disks are hdisk0 and hdisk7.)

**17** Delete the CS 2000 Core Manager configuration database information for the CPU controller modules currently installed on the system:

```
# ftcpuclean
```

**18**

**ATTENTION**
Before continuing, verify what keystrokes are required to perform a “Break” on your VT100 console.

Shut down the CS 2000 Core Manager and initiate a reboot:

```
# shutdown -Fr
```

**19** Interrupt the boot process when the “COLD start” message appears by pressing the Break key.

Example response

```
FX-Bug>
```

***Note:*** The “COLD start” message appears within approximately 2 min.

**20** Determine the current Greewich Mean Time (GMT) setting on the existing CPU controller modules:

```
FX-Bug> time
```

Example response

```
FRI NOV 16 18:41:49:00
```

***Note:*** The time setting is the correct GMT setting. It does not necessarily reflect the local date and time.

**21** Record the date and time response.

***Note:*** If you are using a clock set to your local time to set the GMT on the new CPU controller modules, use the response in step 20 to calculate the number of hours that your local time differs from GMT.

***At the modular supervisory panel (MSP)***

**22** Interrupt power to the CS 2000 Core Manager by turning off the MSP breakers. The MSP breakers, located at the front of the MSP, supply power to the CS 2000 Core Manager. Proceed according to the chassis structure of your system.

| If your system contains | Do |
|---|---|
| a main chassis only | turn top two breakers off |
| a main chassis and I/O expansion chassis | turn all four breakers off |

***At the front of the CS 2000 Core Manager***

**23** Replace the CPU controller modules using the procedure “Replacing a CPU controller module during an upgrade” . When complete, return here, and continue with step 24.

***At the MSP***

**24** Restore power to the CS 2000 Core Manager by turning on the MSP breakers. Proceed according to the chassis structure of your system.

| If your system contains | Do |
|---|---|
| a main chassis only | turn top two breakers on |
| a main chassis and I/O expansion chassis | turn all four breakers on |

***Note:*** When you restore power, both LEDs on the CPU controller modules turn on briefly, then off. This action indicates that the module is seated correctly, is receiving power, and has passed its self tests.

***At the local or remote VT100 console***

**25**

> **ATTENTION**
> Before continuing, verify what keystrokes are required to perform a “Break” on your VT100 console.

Interrupt the boot process when the “COLD start” message appears by pressing the Break key.

***Note:*** The “COLD start” message appears within approximately 5 min.

If the following message appears after you press the Break key, press the Break key again after the prompt to stop the self/boots process.

```
Break detected; Self test/boots about to begin;
press <Break> anytime to abort all
```

Example response

```
FX-Bug>
```

**26** Determine the current Greenwich Mean Time (GMT) setting on the new CPU controller modules:

```
FX-Bug> time
```

Example response

```
FRI NOV 16 18:41:49:00
```

**27** Determine if the GMT setting for the new CPU controller modules is correct.

| If the GMT setting is | Do |
|---|---|
| incorrect | step 28 |
| correct | step 29 |

**28**



**CAUTION**

Potential loss of service

Ensure that the GMT setting on the new CPU controller modules is later than the setting on the previous modules (recorded in step 21). Do not reboot the system if the GMT setting is earlier than the time of the shutdown. This action can corrupt the system configuration and status information.

Correct the time setting to the current GMT:

```
FX-bug> set <mmddyyhhmm>
```

**where**

mm is the numeric month of the year (01 to 12)

dd is the numeric day of the month (01 to 31)

yy is the last two digits of the current year (00 to 99)

hh is the current hour

mm is the current minute (00 to 59)

**29** Ensure that the environment parameters are set to the default values:

```
FX-bug> env;d
```

*Response*

```
Update with Auto-Configuration Defaults
Update Non-Volatile RAM (Y/N)?
```

**30** Enter **y** to confirm the NVRAM update.

*Response*

```
Reset Local System (CPU) (Y/N)?
```

**31** Enter **y** to reset the system.

**32** Interrupt the reboot process by pressing the Break key.

*Response*

```
FX-bug>
```

**33** Boot the CS 2000 Core Manager from disk:

```
FX-bug> pboot 1 0
```

***Note:*** During this time, the CPU firmware is automatically upgraded.

| If you | Do |
|---|---|
| return to the FX-bug prompt again | step 34 |
| do not return to the FX-bug prompt again | step 35 |

**34** Boot the CS 2000 Core Manager again:

```
FX-bug> pboot 1 0
```

**35** At the login prompt, log in to the CS 2000 Core Manager as the root user.

**36** Restore the bootlist:

```
# bootlist -m normal <hdiskx> <hdisky>
```

**where**
hdiskx and hdisky are the two physical disks that provide rootvg storage, as recorded in step 16.

**37** Check the CPU firmware for the CPU in domain 0:

```
# ftbugver -l CPU-0
```

***Note:*** The “-l” is a lower-case L.

**38** Check the CPU firmware for the CPU in domain 1:

```
# ftbugver -l CPU-2
```

***Note:*** The “-l” is a lower-case L.

The next three steps allow the CPU controller modules to complete integration.

**39** Access the maintenance interface:

```
# sdmmtc
```

**40** Access the hardware level:

```
> hw
```

**41** Check the CPU integration status:

```
> querysdm flt
```

**42** Once the CPU controller modules have been integrated, exit the maintenance level:

```
> quit all
```

**43** Force each CPU controller module to assume mastership to synchronize their clocks:

```
# ftctl -switch
```

Repeat the command for the other CPU controller module.

**44** Proceed according to whether you have upgraded or downgraded a module.

| If you have | Do |
|---|---|
| upgraded a module | step 45 |
| downgraded a module | step 48 |

**45** View the current paging space to ensure that it is twice the memory size of the CPU:

```
# lsps -a
```

Example response:

```
Page Space  Physical Volume  Volume Group  Size %Used  Active Auto  Type
hd6         hdisk0           rootvg        512MB 1     yes    yes   lv
```

This response is an example of the paging space for a 256-MByte CPU controller module. In the example, the Size column, which represents the memory size, indicates 512MB. This is twice the size of the CPU, which is what it must be.

| If the paging space is | Do |
|---|---|
| twice the size of the CPU | step 48 |
| not twice the size of the CPU | step 46 |

**46** Increase the paging space:

```
# sdmconfig cpu
```

The paging space is now reset at twice the memory size of the CPU.

**47** Verify the paging space has been increased:

```
# lsps -a
```

Example response

```
Page Space  Physical Volume  Volume Group  Size %Used  Active Auto  Type
hd6         hdisk0           rootvg        1024MB 1    yes    yes   lv
```

This response is an example of the paging space for a 512-MByte CPU controller module. In the example, the Size column, which represents the memory size, indicates 1024MB. This is twice the size of the CPU, which is what it must be.

***Note:*** If the paging space did not increase, repeat steps 46 and 47. If after repeating these steps the paging space still does not increase, contact your next level of support.

### *At the MAP display*

**48** Access the SDM level of the MAP display:

```
> mapci;mtc;appl;sdm
```

Example response

```
SDM ManB
```

**49** Return the CS 2000 Core Manager to service:

```
> rts
```

Response

```
SDM RTS initiated.
SDM RTS completed.
```

The system automatically returns all modules to service.

**50** Ensure the CS 2000 Core Manager hardware and software applications have been restored to the previous inservice state (before the upgrade).

**51** Investigate any CS 2000 Core Manager or CM alarms not recorded in pre-checks. For any alarms that cannot be resolved, contact your next level of support.

**52** Return all billing streams to service. For each billing stream, complete steps 53 through 54.

**53** Post the required billing stream:

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

*where*

**<stream>**
is the name of the billing stream

**54** Return the posted stream to service:

```
> rts
```

**55** Post each billing stream again (see step 53) and make sure that each stream is in-service (InSv).

**56** Verify that billing is collecting records:

```
# query <stream_name>
```

where

**<stream_name>**
is the name of the billing stream, for example, ama.

Note the number of records, wait approximately 10 seconds, and repeat the query command.

| If the number of records | Do |
|---|---|
| increased from the first query command (meaning billing is working) | step 57 |
| did not increase from the first query command (meaning billing is not working) | contact your next level of support |

**57** You have completed this procedure.

## Apply the RPM package

Once you have upgraded the software, you must apply the RPM package to the system.

***At the VT100 console or telnet session***

**1** Access the maintenance interface:

```
# sdmmtc
```

**2** Access the SWIM level:

```
> swim
```

**3** List the filesets:

```
> apply <directory path>
```

where

**<directory_path>**
is the directory where the filesets are located

***Note:*** <directory path> may be the /swd/sdm/esd directory.

4 Select the RPM package

```
> select <n>
```

where

**<n>**
is the number next to the RPM fileset.

5 Apply the RPM fileset:

```
> apply
```

6 When prompted, confirm the apply command:

```
> y
```

7 You have completed this procedure.

# Upgrading the CPU firmware

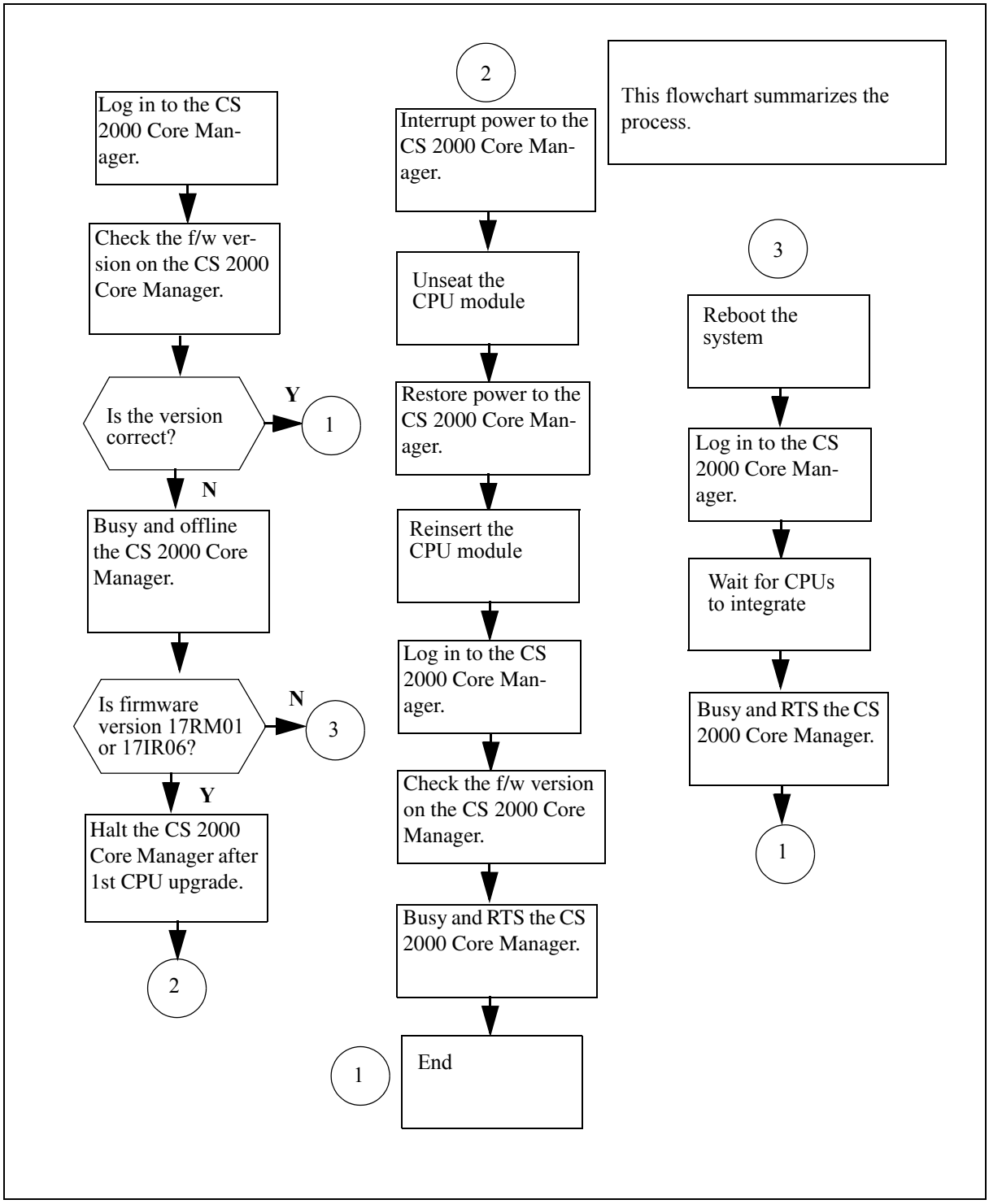
## Purpose

This procedure provides instructions for upgrading the CPU firmware. Once you have upgraded the CPU controller module, you must check the version of the firmware. If the CPUs do not have the current firmware version, you must perform a firmware upgrade. You can also perform this procedure at any time in order to check the status of the CPU firmware.

## Task flow diagram

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedure that follows the flowchart to perform the tasks.

## Task flow for upgrading the CPU firmware



# Procedure

## Upgrading the CPU firmware

### *At the CS 2000 Core Manager local VT100 console*

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

2 Run the firmware process:

```
# sdmfirmware
```

The system runs through the process and indicates whether a firmware upgrade is required. Note the current firmware version.

3 Use the following table to determine your next step.

| If the firmware | Do |
|---|---|
| needs to be upgraded | step 4 |
| does not need to be upgraded | step 29 |

### *At the MAP*

4 Access the SDM level:

```
> mapci;mtc;appl;sdm
```

5 Busy the CS 2000 Core Manager:

```
> bsy
```

6 Confirm the busy command:

```
> y
```

7 Take the CS 2000 Core Manager offline:

```
> offl
```

### *At the CS 2000 Core Manager local VT100 console*

8 Proceed with the firmware upgrade by pressing the Enter key.

9 Use the following table to determine your next step.

| If the firmware version noted in step 2 | Do |
|---|---|
| is 17RM01 | step 18 |
| is not 17RM01 | step 10 |

**10** Print the instructions displayed on the system, so that you can execute them after the system has rebooted.

**11** Press the Enter key to reboot the system, and wait for the FX-Bug prompt.

**12** At the FX-Bug prompt, enter:

```
FX-Bug> switch <cpu> ;h
```

*where*

<cpu>
is the CPU number (0 or 2) from step 10

**13** Boot the system:

```
FX-Bug> gevboot
```

**14** Log into the CS 2000 Core Manager as the root user.

***At the CS 2000 Core Manager VT100 console***

**15** Run the firmware process:

```
# sdmfirmware
```

**16** Wait for the CPU modules to integrate.

**17** Press the Enter key to continue, and go to step 31.

***At the CS 2000 Core Manager VT100 console***

**18** The system prompts you to halt the CS 2000 Core Manager after the firmware upgrade on one CPU is complete. The system also indicates that you must pull the CPU after the halt is complete. Before you halt the CS 2000 Core Manager, note which CPU the system has directed you to pull.

To halt the CS 2000 Core Manager, press the Enter key. Wait for the halt to complete before continuing the procedure.

***Note:*** Under some circumstances, the CS 2000 Core Manager reboots and does not halt. If this happens, wait for the reboot to complete, and then log into the CS 2000 Core Manager. Halt the CS 2000 Core Manager again. Interrupt the reboot process to access the FX-Bug prompt by pressing the Break or Esc key several times. When the CS 2000 Core Manager is at the FX-Bug prompt, you can interrupt the power to the CS 2000 Core Manager safely.

***At the MSP***

**19** Interrupt power to the CS 2000 Core Manager by turning off both of the MSP breakers. The MSP breakers, located at the front of the MSP, supply power to the CS 2000 Core Manager.

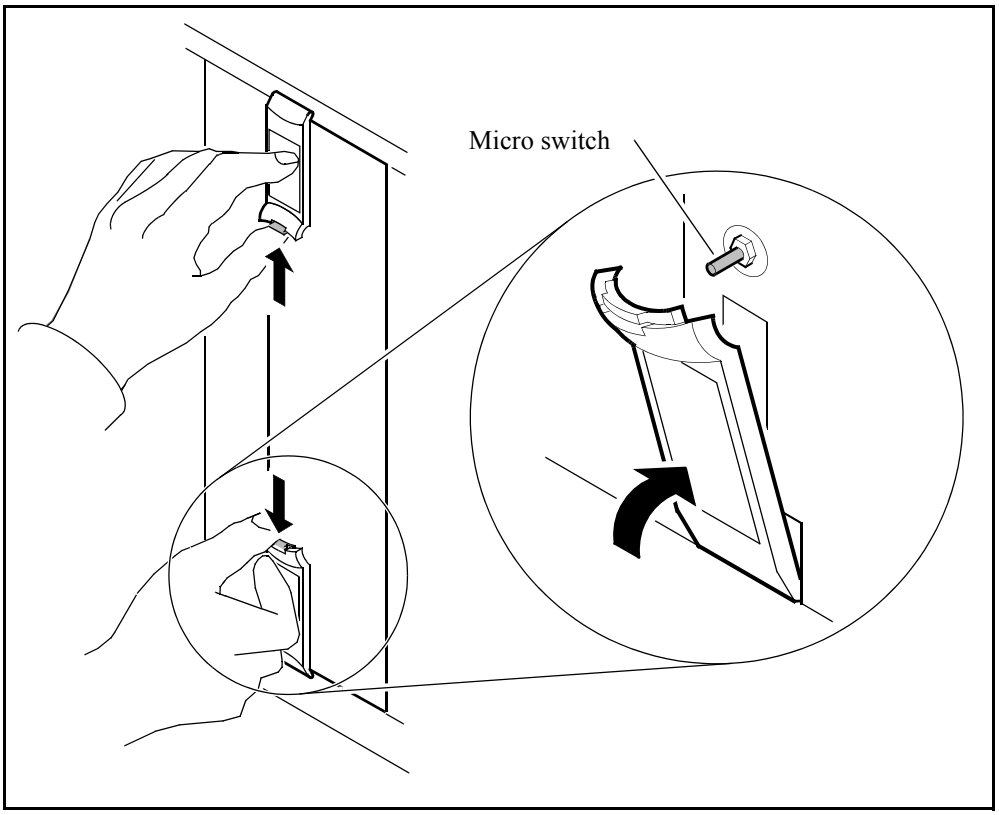
**20** Use the following table to determine your next step.

| If your system contains | Do |
|---|---|
| a main chassis only | turn the top two breakers off |
| a main chassis and I/O expansion chassis | turn all four breakers off |

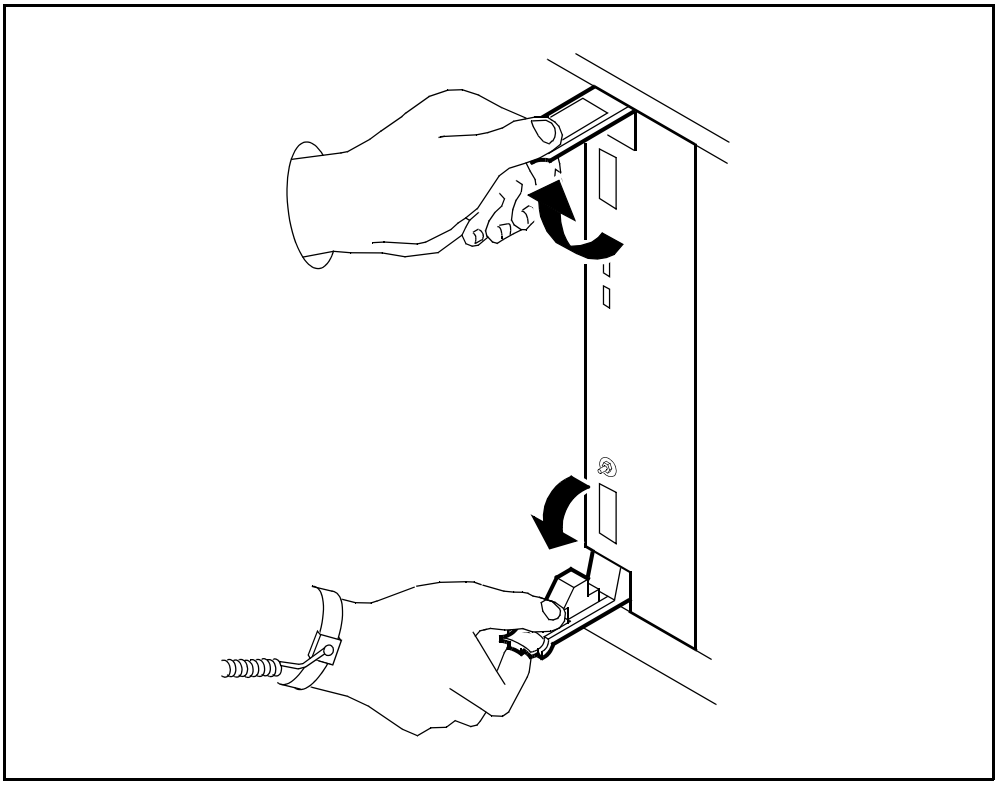
***At the front of the CS 2000 Core Manager***

**21** Unscrew the thumbscrews located on the top and bottom of the CPU module noted in step 18. The thumbscrews are the captive type, and you cannot remove them from the module.

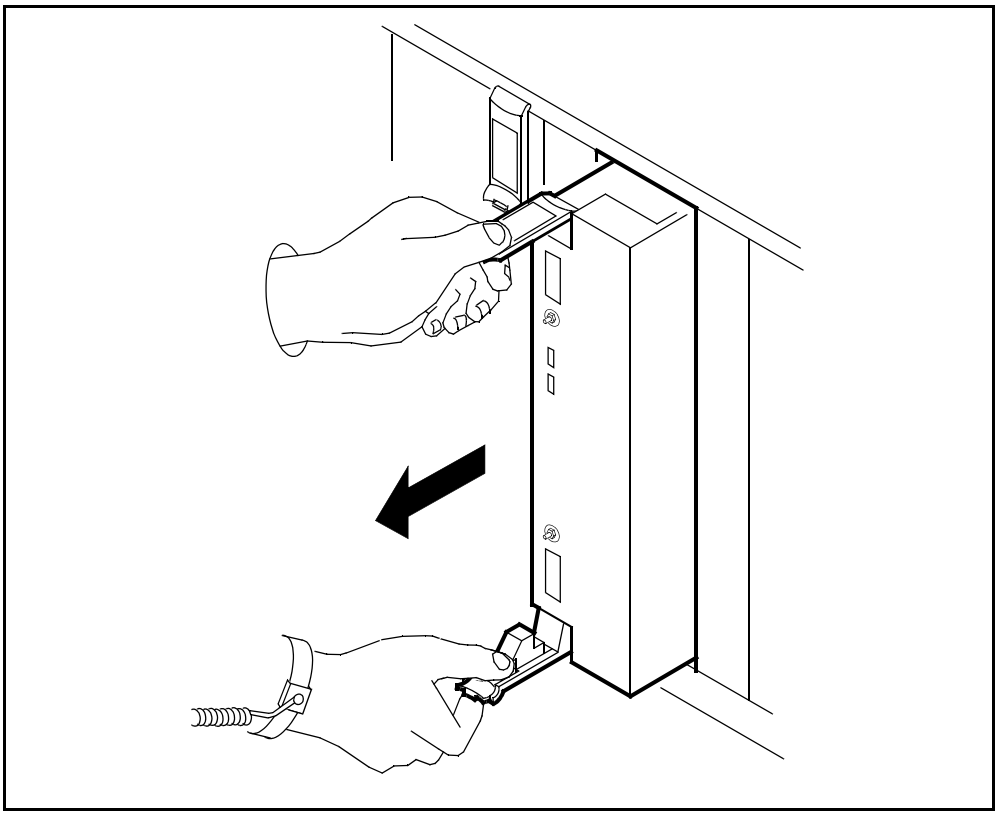
**22** Depress the tips of the locking levers on the face of the CPU module.



**23** Open the locking levers on the face of the module by moving the levers outwards.



**24** While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



***At the MSP***

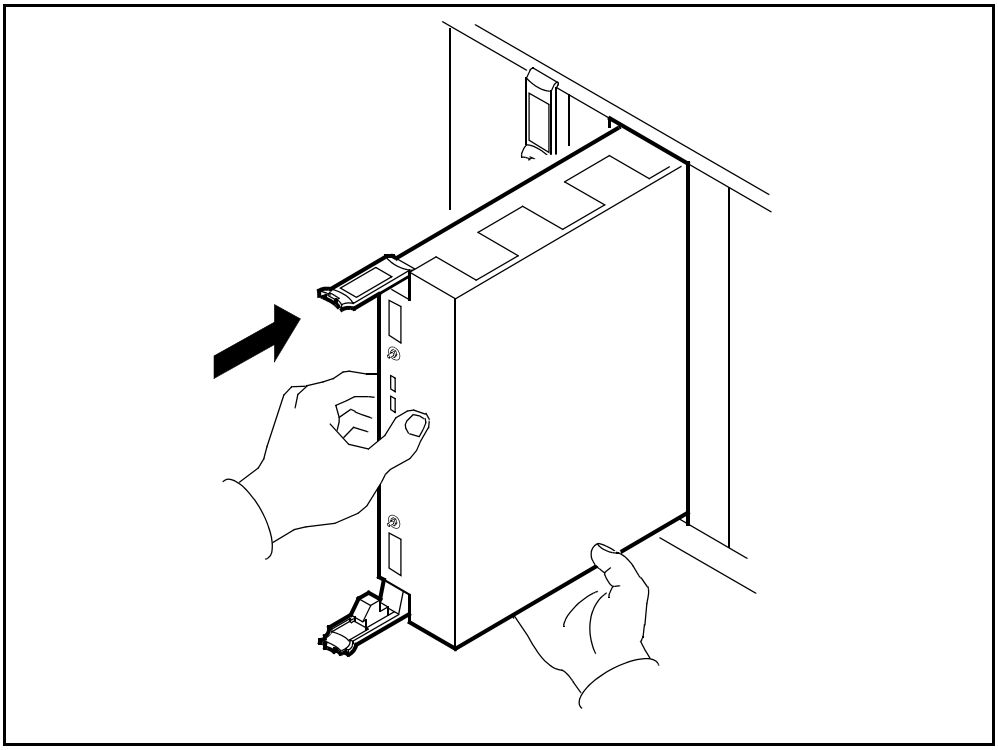
**25** Restore the power to the CS 2000 Core Manager by turning on the MSP breakers, according to the chassis structure of your system.

| If your system contains | Do |
|---|---|
| a main chassis only | turn the top two breakers on |
| a main chassis and I/O expansion chassis | turn all four breakers on |

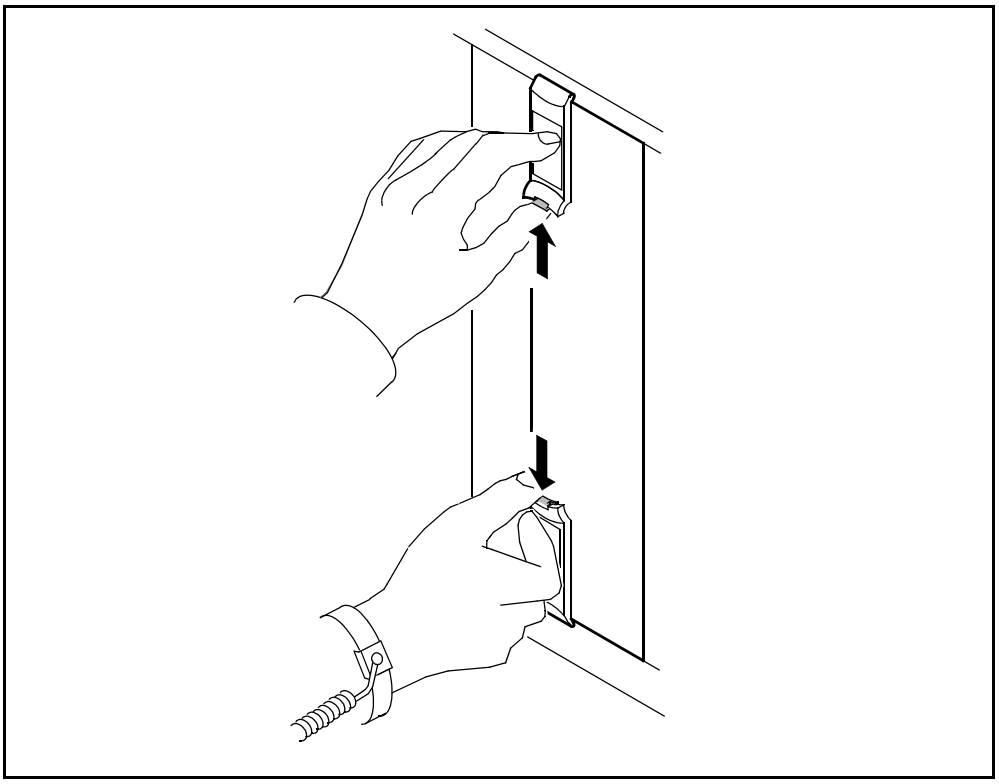
***Note:*** Wait at least 15 seconds before re-inserting the pulled CPU.

***At the front of the CS 2000 Core Manager***

**26** Gently push the CPU module that you pulled out in step 24 back into the slot.



**27** Close the locking lever to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to seat the module properly.



**28** Tighten the thumbscrews on the module.

When you put the CPU controller module back into the slot, both LEDs on the module turn on briefly and then off. This action indicates that

- you have seated the module correctly
- the module is receiving power
- the module has passed all self-tests

***At the local VT100 console***

**29** Log into the CS 2000 Core Manager as the root user.

***Note:*** The firmware on the other CPU is upgraded automatically when you log into the CS 2000 Core Manager. The automatic upgrade of the firmware on the other CPU is dependent on the successful completion of step 8, followed by steps 18 through 28.

**30** The system indicates that the CPU modules have fully integrated with the CS 2000 Core Manager, and that they have

the correct firmware. Press the Enter key to continue the procedure.

**31** Return the CS 2000 Core Manager to service:

```
> rts
```

**32** You have completed this procedure.

# Replacing a CPU controller module during an upgrade

**ATTENTION**
Use this procedure only if you have been directed here from an upgrade procedure to replace a CPU controller module. If you are replacing a CPU controller module outside of an upgrade procedure, refer to procedure “Replacing CPU controller modules” in the Fault section.

## Replacing the CPU controller module

***At the front of the CS 2000 Core Manager***

**1**



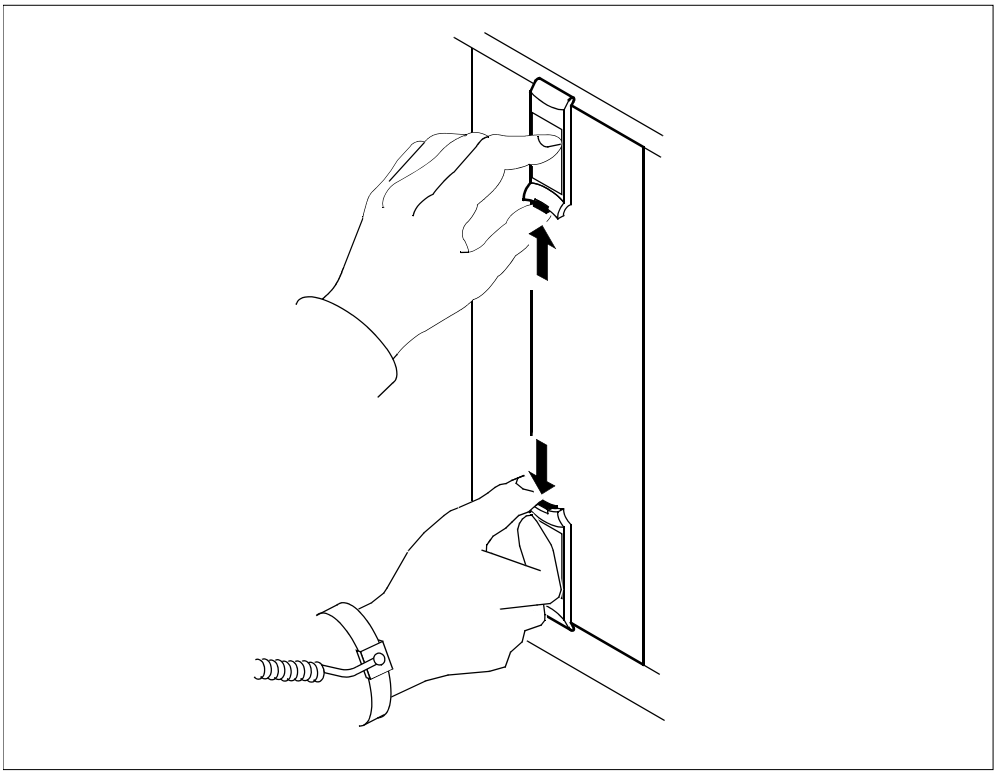
**WARNING**
**Static electricity damage**
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

If you are upgrading the CPU controller module in domain 0, remove the CPU controller module from slots 6 and 7. If you are upgrading the CPU controller module in domain 1, remove the CPU controller module from slots 10 and 11.

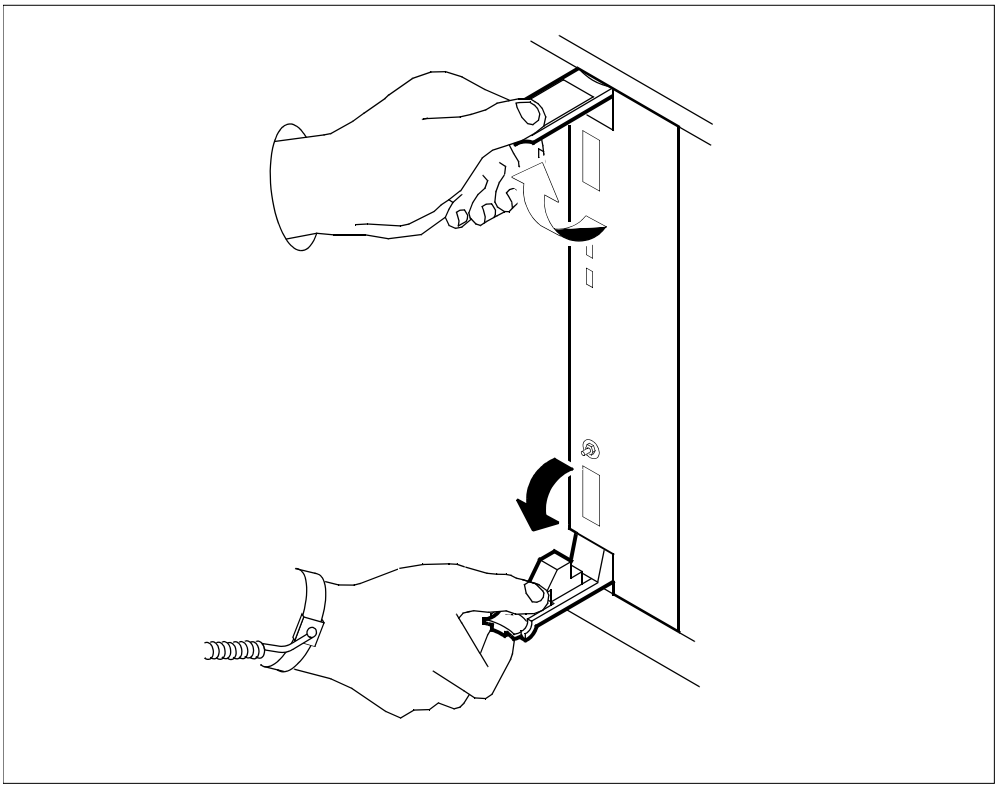
Undo the thumbscrews located on the top and bottom of the CPU controller module.

***Note:*** The thumbscrews are the captive type, and cannot be removed from the module.

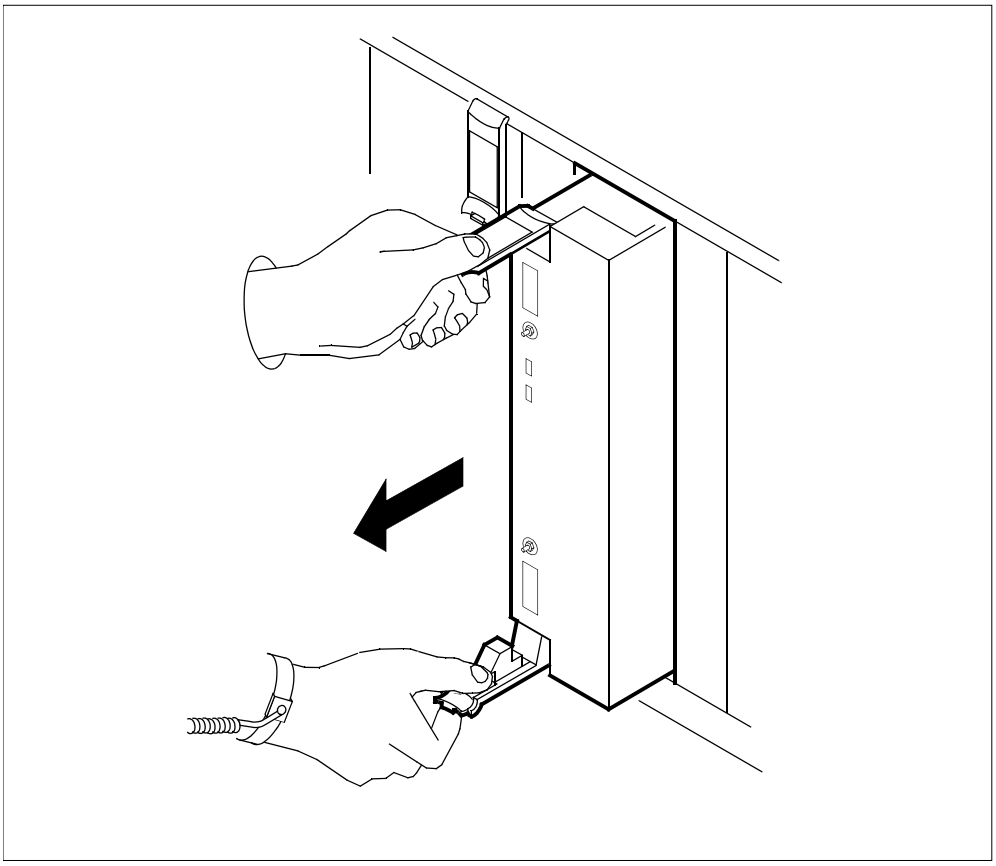
**2** Depress the tips of the locking levers on the face of the CPU controller module.



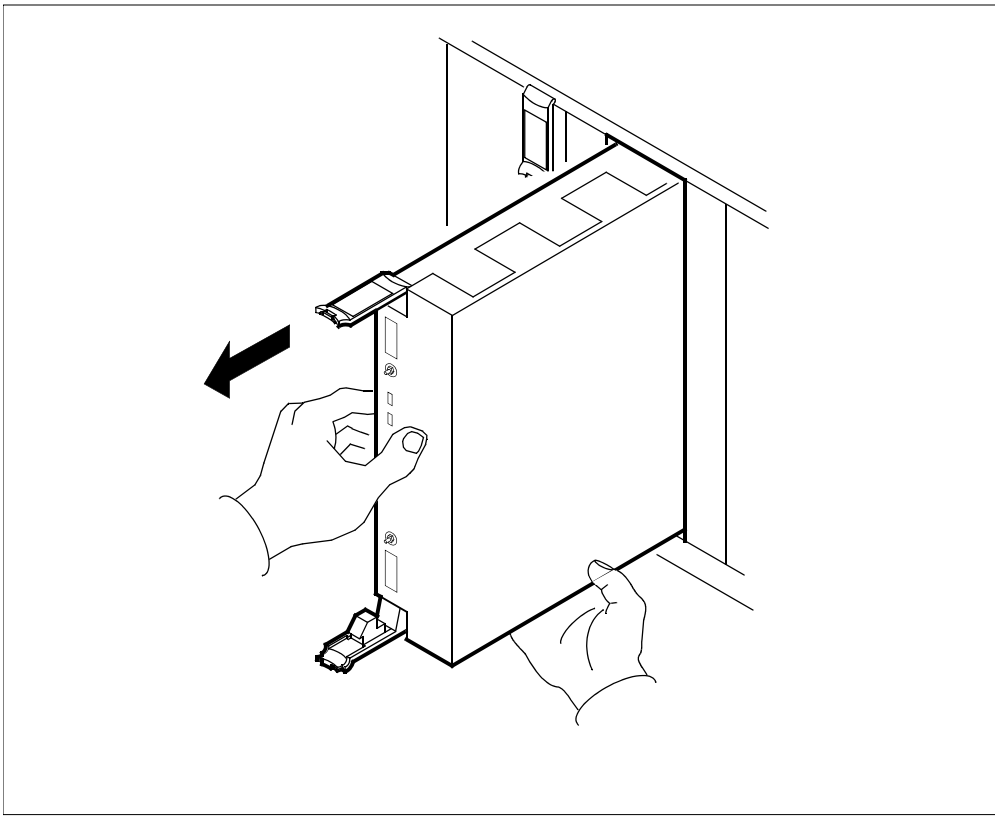
**3** Open the locking levels on the face of the module by moving the levers outwards.



**4** While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the shelf.



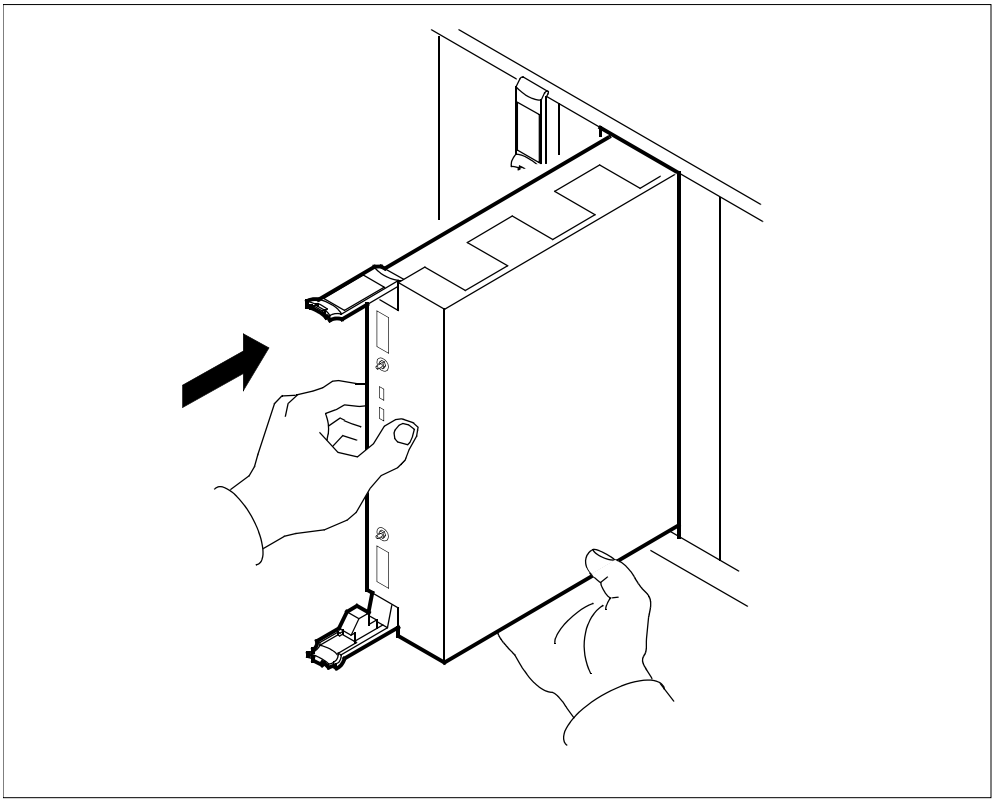
**5** Hold the module by the face plate with one hand while supporting the bottom edge with the other. Gently pull the module toward you until it clears the shelf.



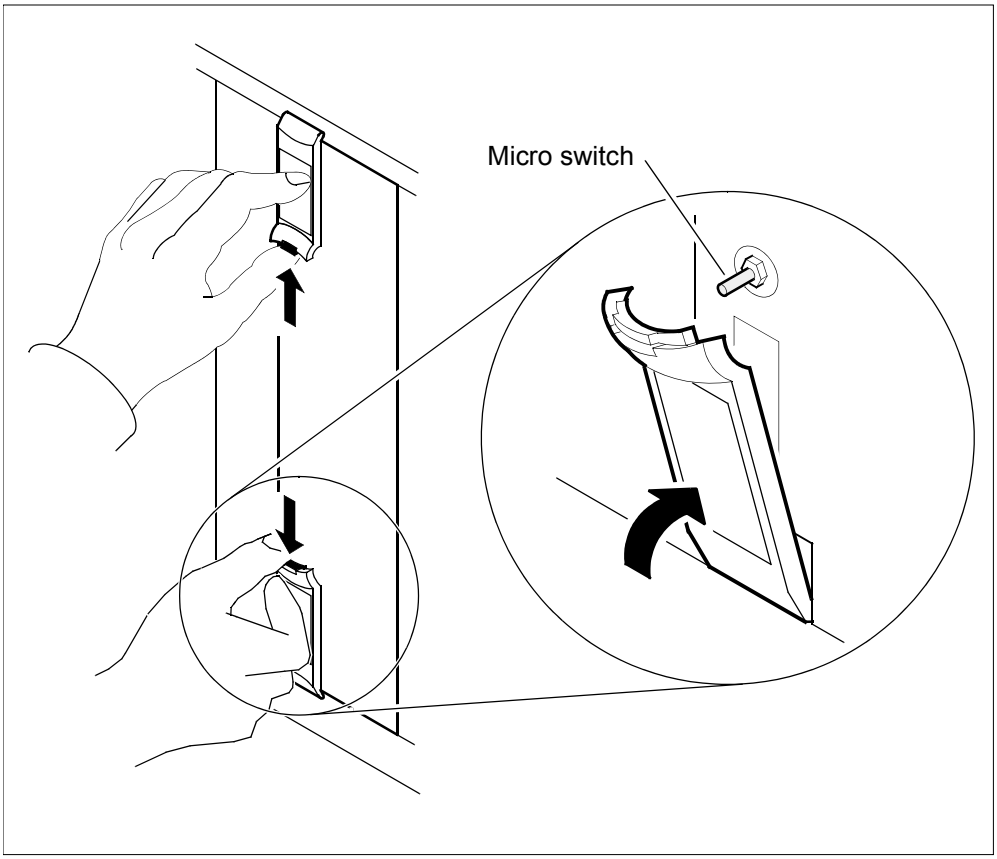
**6** Place the module you have removed in an ESD protective container.

**7** Insert the replacement module into the shelf.

**8** Gently slide the module into the shelf until it is fully inserted.



**9** Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.




**10** Tighten the thumbscrews on the module.

**11** You have completed this procedure. Return to the procedure that sent you to this procedure.

# Commissioning X.25 connectivity

## Purpose

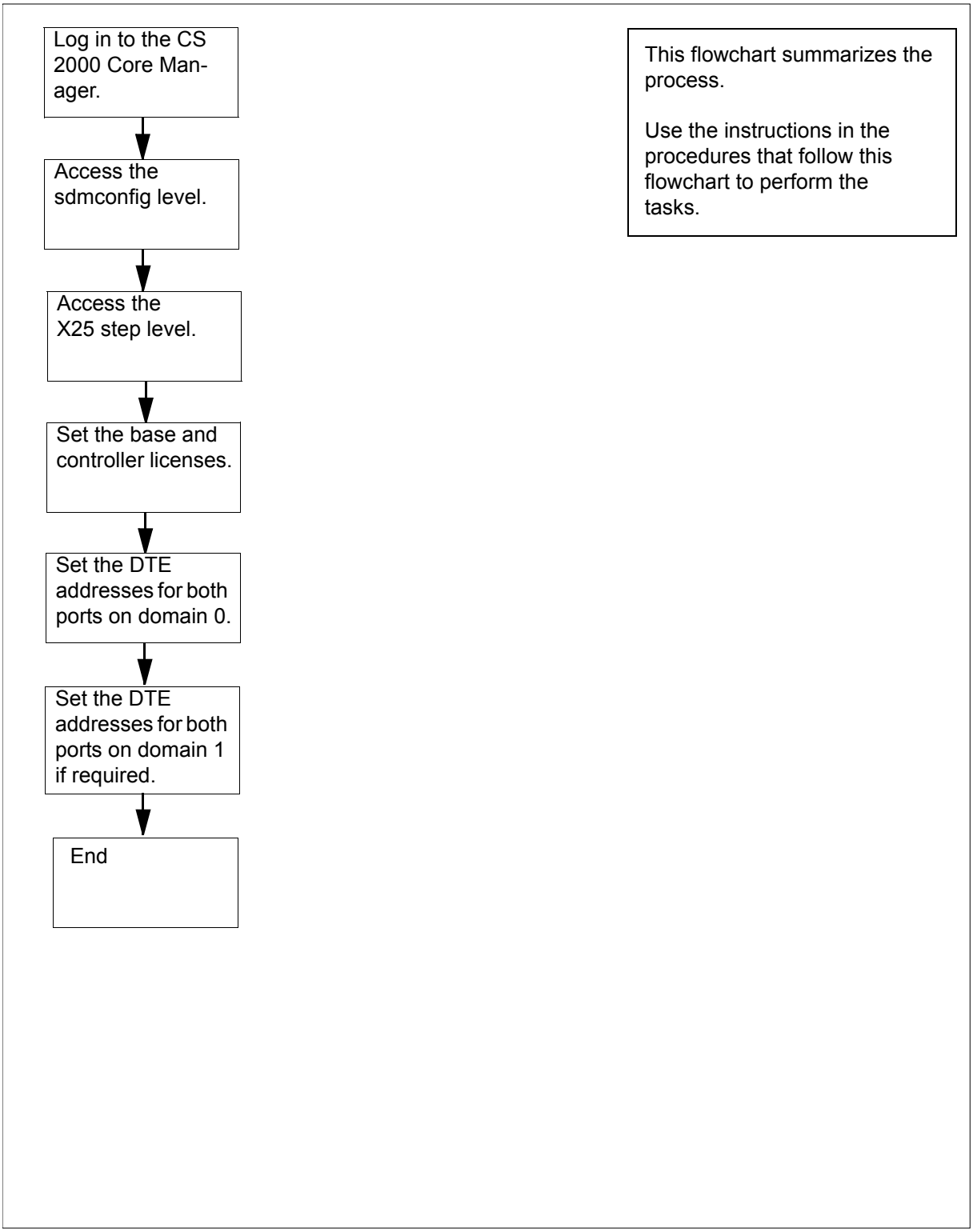
Use this procedure to commission or recommission X.25 connectivity on the CS 2000 Core Manager from the configuration level (sdmconfig).

***Note:*** You can also commission or recommission X.25 from the X25 level of the maintenance interface (sdmmtc x25). The same commands are used at both levels to set the X.25 base and controller licenses, and the Data Terminal Equipment (DTE) addresses for both X.25 ports.

## Task flow diagram

The following task flow diagram provides an overview of the process. Use the instructions in the procedures that follow the flowchart to complete the tasks.

## Task flow for commissioning X25 connectivity



## Procedure

If you are commissioning X.25 connectivity for the first time, follow the instructions in the procedure Configuring X.25 licences below. If you are recommissioning X.25 on domain 0 or domain 1, follow the instructions in Configuring DTE addresses on page 631.

### Configuring X.25 licences

***At the CS 2000 Core Manager***

1 Log in to the CS 2000 Core Manager as the root user.

2 Access the configuration level:

```
# sdmconfig
```

3 Access the X.25 commissioning step level:

```
> step <#>
```

*where*

**#**
is the number next to the X.25 commissioning step.

4 Initiate the configuration process:

```
> change
```

5 When prompted, enter the new Base license key. The Base license key is the 28 alphanumeric character string for the X.25 hardware that you are commissioning.

6 When prompted, enter the new Controller license key. The Controller license key is the 28 alphanumeric character string for the X.25 hardware that you are commissioning.

*Example response*

```
X25 Connectivity values to be changed:

Base license key: 3xcmwj6p4wmnxhyknmnbwvqzr2aa
Controller license key:
5me5q7itsuba5hyknmnbwvqzr2aa

Proceed with these values?
Enter Y to confirm, N to reject, or E to edit:
```

7 When prompted, confirm the values:

```
> y
```

*Response*

```
Change - Command submitted.
```

8 You have completed this procedure. To continue commissioning X.25 connectivity, follow the instructions in the procedure Configuring DTE addresses.

## Configuring DTE addresses

### *At the X.25 commissioning step level*

1 Configure the DTE addresses of the X25 ports on domain 0:

```
> change 0 <port>
```

*where*

**port**
is 0 or 1

2 Enter the DTE address (5 to 15 digits) that corresponds to the port.

*Example response*

```
X25 Connectivity values to be changed:

DTE address for domain 0 port 0: 123456

This action will affect service on the specified
port.

Proceed with these values?
Enter Y to confirm, N to reject, or E to edit:
```

3 Confirm the values:

```
> y
```

*Example response*

```
Change 00 - Command submitted.
```

4 Repeat steps 1 through 3 for the other port.

5 Use the following table to determine your next step

| If the system | Do |
|---|---|
| has an X25 card in domain 1 | step 6 |
| does not have an X25 card in domain 1 | you have completed this procedure |

6 Configure the DTE addresses of the X25 ports on domain 1:

```
> change 1 <port>
```

*where*

**port**
is 0 or 1

**7** Enter the DTE address (5 to 15 digits) that corresponds to the port, and press the Enter key.

*Example response*

```
X25 Connectivity values to be changes:

DTE address for domain 1 port 0: 123456

This action will affect service on the specified
port.

Proceed with these values?
Enter Y to confirm, N to reject, or E to edit:
```

**8** Confirm the values:

```
> y
```

*Example response:*

```
Change 10 - Command submitted.
```

**9** Repeat steps 6 through 8 for the other port.

**10** You have completed this procedure.

# Installing an X.25 controller module and personality module

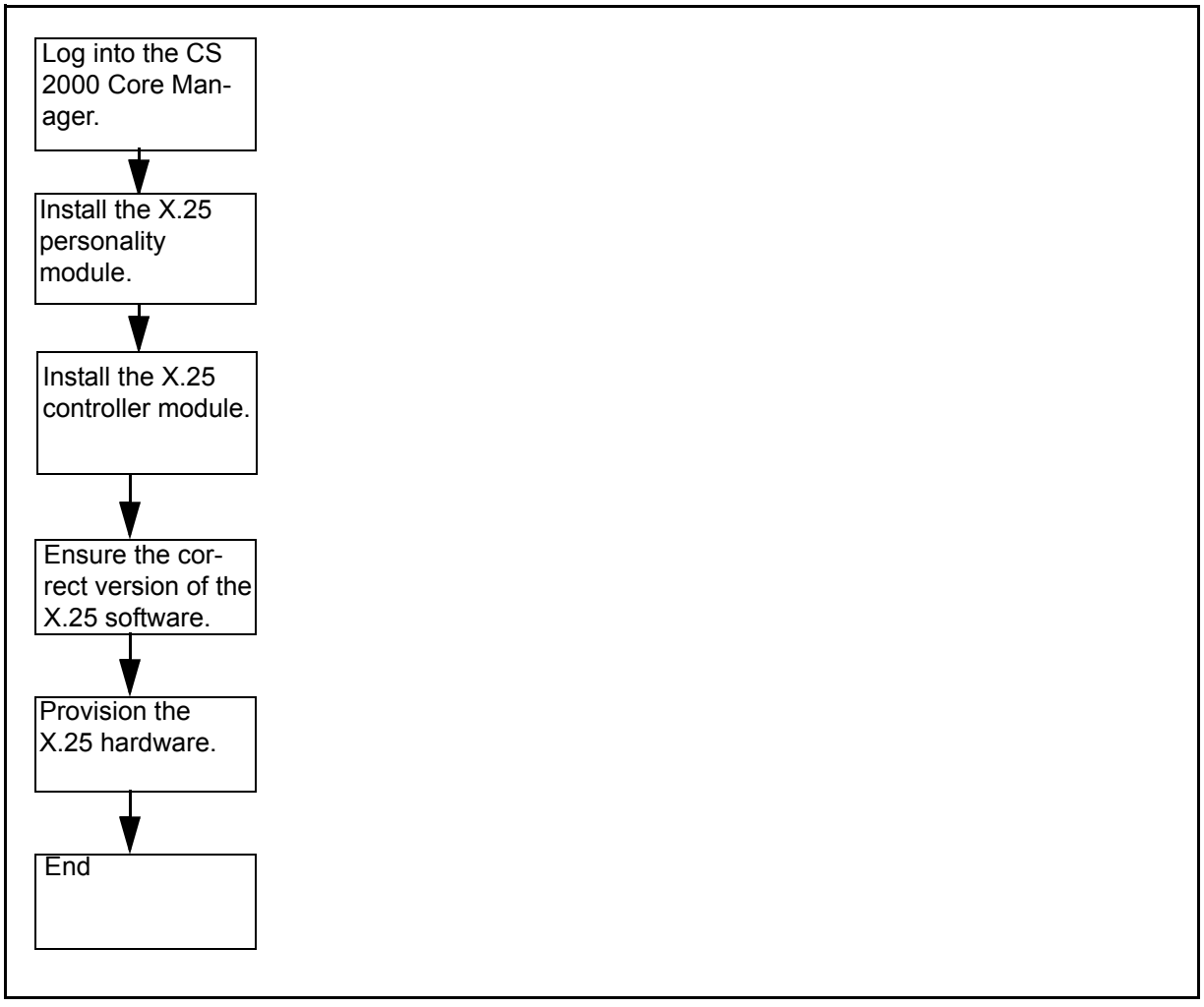
## Purpose

Use this procedure if you have an MFIO hardware module and want to upgrade the CS 2000 Core Manager to incorporate an X.25 controller module (NTRX50FY) and an X.25 personality module (NTRX50FZ).

## Task flow diagram

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedures that follow the flowchart to perform the tasks.

**Task flow for Installing an X.25 controller module and personality module**



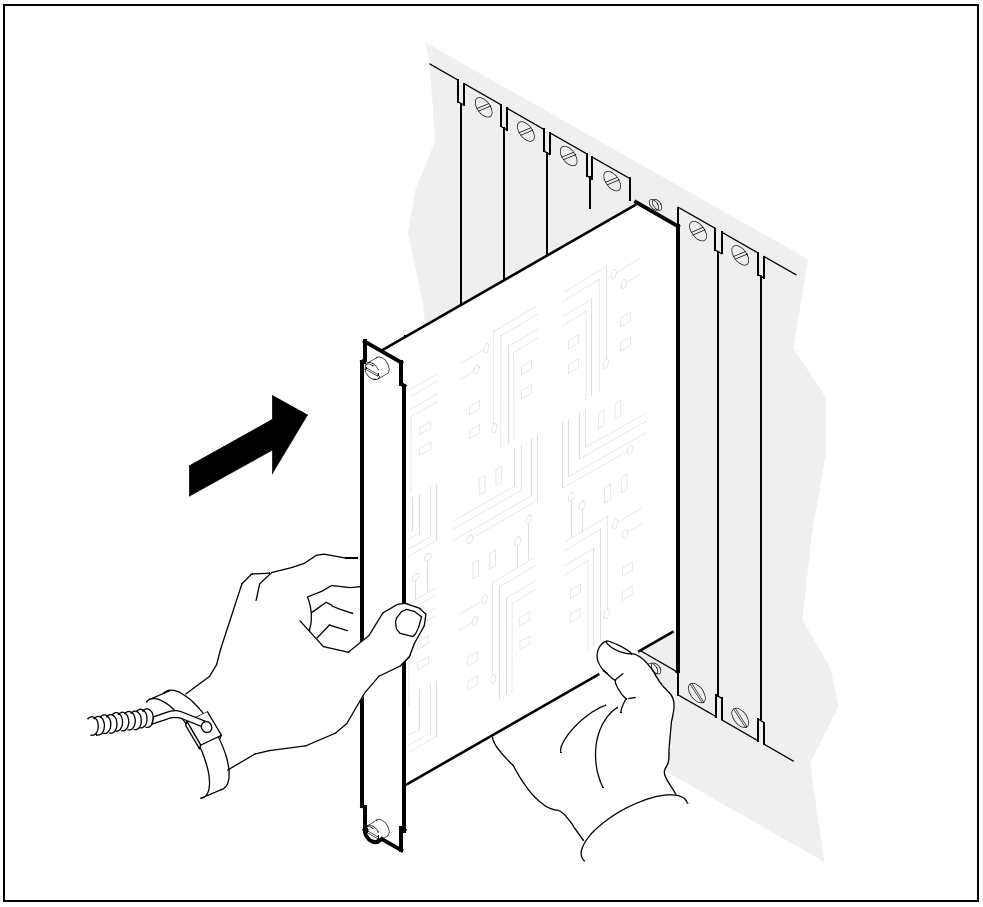
# Procedures

## Installing an X.25 controller module and personality module

### *At the back of the CS 2000 Core Manager*

**1** Insert the new X.25 personality module into the CS 2000 Core Manager shelf.

**2** Gently slide the X.25 personality module into the shelf until it is fully inserted.



**3** Tighten the thumbscrews at the top and bottom of the X.25 personality module.

***At the front of the CS 2000 Core Manager***

**4**



**WARNING**

**Static electricity damage**

Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge grounding wrist strap.

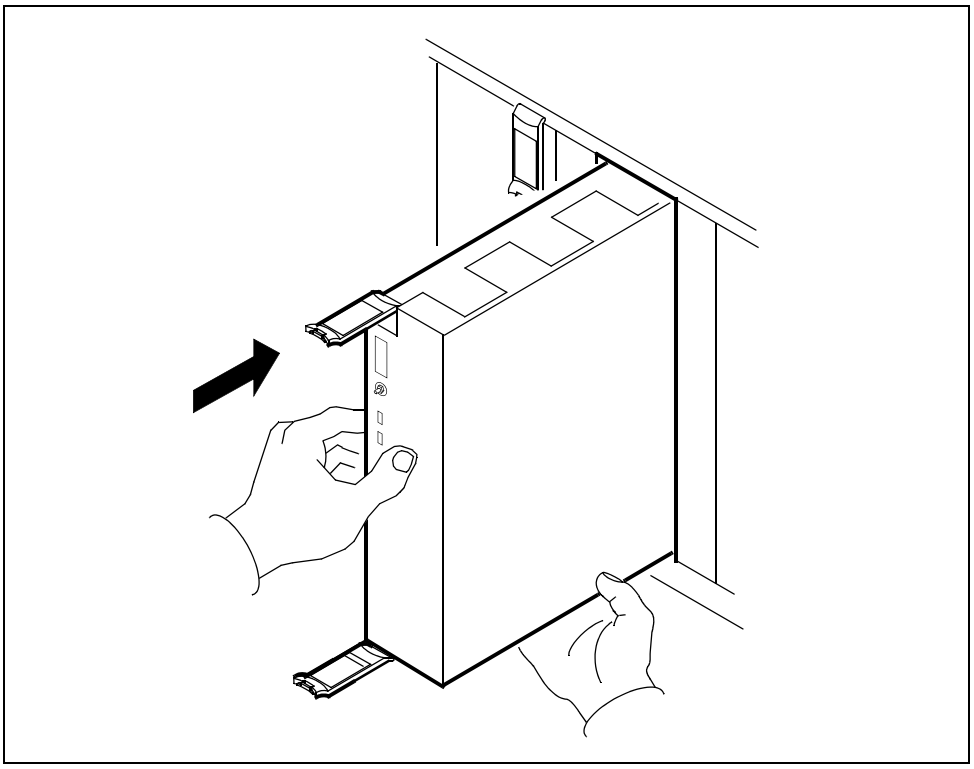
**5** Remove the filler plates covering the slots where you will install the new modules.

**6** Insert the X.25 controller module into the CS 2000 Core Manager shelf.

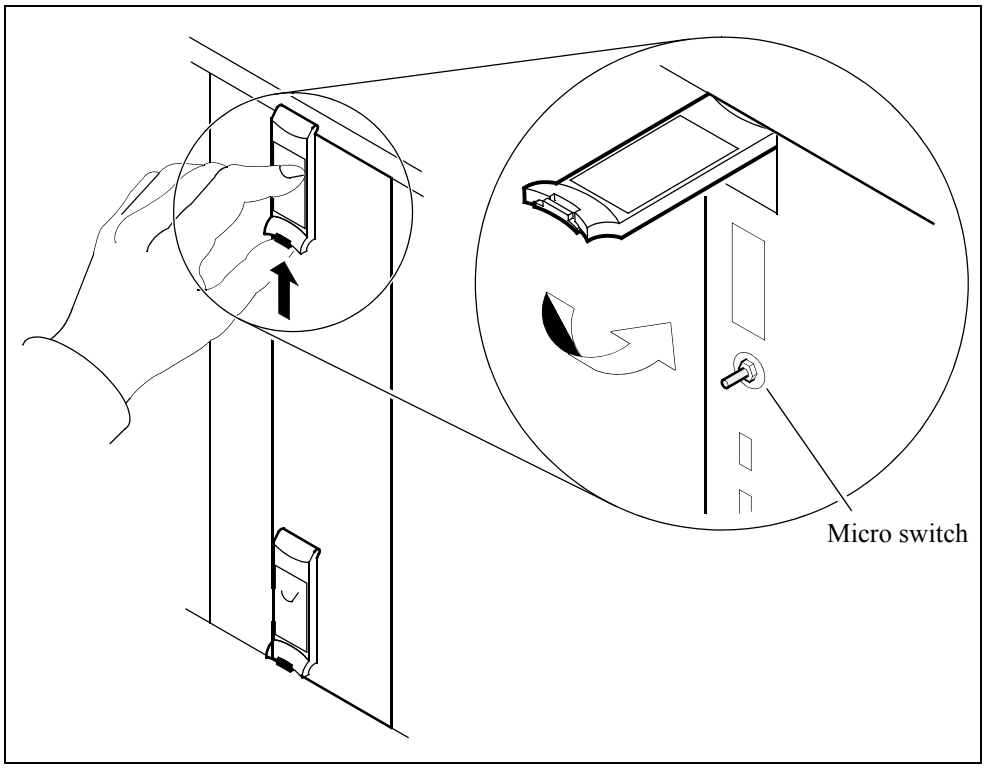
***Note 1:*** If you are installing a single X.25 module, you must install it on domain 0.

***Note 2:*** You can install two X.25 controller modules as a logical pair in either the main or expansion chassis. The two slots used for this must be exactly 8 slot positions apart (for example, slots 1 and 9, or 2 and 10). Both modules in a logical pair must have the same PEC.

**7** Gently slide the module into the shelf until it is fully inserted.



8 Close the locking lever to secure the module. Ensure that the top micro switch is lined up with the locking lever to seat the module properly.




9 You have completed this procedure.

## Provisioning the X.25 hardware

### *At the local or remote VT100 console*

1 Log in to the CS 2000 Core Manager as root.

2 Ensure that the latest version of the X.25 software is available on the system. Insert the tape labeled *CS2E0070 7.x (1 of 1)* into slot 2.

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

3 Access the maintenance interface:

```
# sdmmtc
```

4 Display the contents of the tape:

```
> apply 0
```

5 Install the X.25 software:

```
> apply bundle x25
```

6 Confirm the command:

```
> y
```

*Response*:

```
Command completed with no errors
```

7 Access the Hw level of the Maintenance Interface:

```
> hw
```

8 Add the X.25 hardware:

```
> add <chassis> <slot> <pec> [SIMPLEX]
```

*where*

***chassis***
is *sdmm* for the main chassis, and *sdme* for the expansion chassis

***slot***
is the slot number of the X.25 card in domain 0

***pec***
is the PEC code of the X.25 controller module (NTRX50FY)

**SIMPLEX**
is an optional parameter. Enter this parameter if you are installing only one X.25 module on the system.

*Response*

```
Add sdme 5 ntrx50fy - Command complete.
```

9 You have completed this procedure.

# Upgrading the CS 2000 SAM21 manager GUI client application

## Application

Use this procedure to upgrade the CS 2000 SAM21 manager GUI client application to the latest software release.

## Prerequisites

The CS 2000 SAM21 manager server must have the same software version as the client version to which you are upgrading.

The CS 2000 SAM21 manager is a client/server application. The client runs on a Sun SPARC workstation, and the server runs on the CS 2000 Core Manager.

For SN07, the following requirements must be met for the client:

- The CS 2000 SAM21 manager client requires a Sun SPARC workstation. The workstation must run (at a minimum) the Solaris 2.7 operating system. The CS 2000 SAM21 manager is also supported on the Solaris 2.8 operating system. For optimum performance, Nortel Networks recommends you have a Sun Ultra10 with 512 Mbyte of DRAM and 70 Mbyte or higher of available disk space.
- The latest versions of the following patch IDs are required for Solaris 2.7 systems:
  - Patch 106300
  - Patch 106327
  - Patch 106541
  - Patch 106950
  - Patch 106980
  - Patch 107081
  - Patch 107226
  - Patch 107226
  - Patch 107544
  - Patch 107636
  - Patch 107656
  - Patch 107702
  - Patch 108374

The latest versions of the following patch IDs are required for Solaris 2.8 systems:

— Patch 108652

— Patch 108921

— Patch 108940

For further details see Sun's Solaris Java patch page at: http://java.sun.com/j2se/1.3/install-solaris-patches.html

Patches may be retrieved from Sun's Patchfinder at: http://sunsolve.sun.com

- The latest SAM21 client software version must be installed.
- The CS 2000 SAM21 manager client application requires the client machine to be configured in a pluggable authentication module (PAM) framework.

## Action

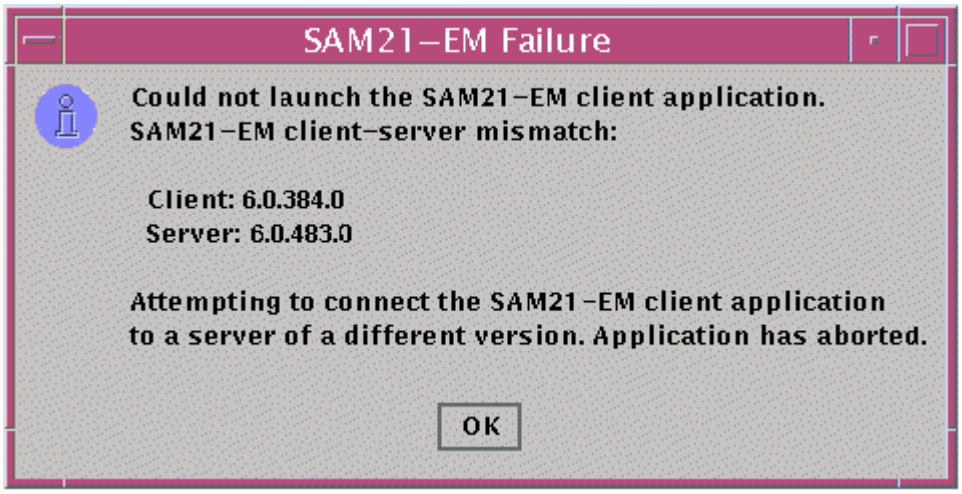
***At the Client Workstation***

**1** Log on the client workstation using the root user ID and password.

***Note 1:*** For all upgrades, the client software must be upgraded to match the server software before it is started.

***Note 2:*** If an attempt was made to launch the CS 2000 SAM21 manager client application (by typing: >sdm/bin/sam21gui), the user would receive a mismatch error. See the Mismatch error figure below. This indicates that the client machine needs to be upgraded to match the version of the manager running on the CS 2000 Core Manager. This error message only occurs for MNCL or maintenance release upgrades (not for upgrades from SN03 to SN04).

**Mismatch error**




2 If a previous manager client has been installed, verify the client machine is still using the old version of the manager software by typing:

```
> /sdm/bin/sam21gui -version
```

The resulting version number indicates that we have not yet upgraded the client to match the server.

3 Access the directory where the Client Installer and Launcher (CIL) tool is to be located after the FTP operation by typing

```
> cd /tmp
```

and pressing the Enter key.

4 Connect to the CS 2000 Core Manager using file transfer protocol (FTP) by typing

```
> ftp <ipaddress>
```

and pressing the Enter key.

where

**ipaddress**
is the IP address of the CS 2000 Core Manager

5 Log on the CS 2000 Core Manager as an anonymous user by typing

```
Name:ftp
```

and pressing the Enter key.

6 When prompted for a password, ignore the prompt and press the Enter key to continue the procedure.

7 Get the Client Installer and Launcher tool (CIL) by typing

```
ftp> get cil
```

and pressing the Enter key.

8 Quit the connection to the CS 2000 Core Manager by typing

```
ftp> quit
```

and pressing the Enter key.

9 Make the CIL program executable by typing

```
> chmod 755 cil
```

and pressing the Enter key.

10 Execute CIL by typing

```
> ./cil
```

and pressing the Enter key.

Response:

```
    SDM CLIENT SOFTWARE INSTALLATION

Enter the IP address or hostname of the SDM that
you want to download the client software from.

SDM's Address:
```

11 At the CIL menu, connect to the CS 2000 Core Manager by typing

```
SDM's Address:<ipaddress>
```

and pressing the Enter key.

*where*

**ip_address**
is the IP address or the host name of the CS 2000 Core Manager.

**12** Select the CS 2000 Core Manager fileset to upgrade the client workstation to by typing

```
cil> select <#>
```

and pressing the Enter key.

*where*

#
is the number of the CS 2000 Core Manager fileset. An example of the fileset is snm_sam21_client_7.0.*xxx*.n.tar.Z where xxx represents the latest version and n represents the MNCL version.

**13** Install the selected fileset by typing

```
cil> apply
```

and pressing the Enter key.

**14** Enter the IP address of the server when prompted for it by typing the IP address at the prompt and pressing the Enter key.

**15** You have completed this procedure.

# Legacy peripherals

Please refer to the *Peripheral Module Release Document*, 297-9051-599 (intl) or 297-2663-599 (NA) in your DMS Helmsman collection.

# Upgrading an IW-SPM IP

## Perform an automated upgrade

Use at least two devices with this procedure. Use one device to perform the automated SPM upgrade. Use the second device as a trace device to monitor the progress of the automated SPM upgrade.

Some offices use a third device during the automated SPM upgrade. Use the third device as a MAP terminal. Post the SPMs and monitor SPM loading, patching, and service status.

Send the output of each device to a printer for record keeping.

SWUPGRADE PM will disable the Spectrum Patching After RTS (SPARTS) tool during the automated upgrade. When SWUPGRADE PM is completed or aborted, SPARTS is automatically re-enabled.

The SPM601 log generates when SPARTS is disabled and also enabled. No action is required when this log is generated.

**Table 1 Variable Abbreviations**

| Abbreviation | Definition |
|---|---|
| printer | the printer name |
| max_no | the UNLIMITED or the maximum number of SPMs the system upgrades concurrently |
| dev_name | the name of the new Patch Distribution volume |
| spm_no | the ID (number) of the SPM |
| step_name | the name of the step |

MAP displays in this procedure are provided as reference examples and may not represent the actual screen display. Load versions and resource modules (RMs) listed on the screen may vary depending on the office configuration.

Throughout the upgrade procedure, the request to type a command requires pressing the Enter key on the keyboard after the command has been typed.

### Procedure 1 Perform an automated upgrade

***At the CI level of the MAP display***

1 Send the terminal responses to a printer by typing

```
>RECORD START ONTO printer
```

2 Enter the SWUPGRADE PM increment for automated SPM upgrades by typing

```
>SWUPGRADE PM
```

3 Establish a second device as a trace device by typing

```
>SET TRACE_DEVICE dev_name
```

***Note:*** The second device records SWUPGRADE PM operations during the automated SPM upgrade.

4 The trace device must display a message indicating that the device is selected for TRACEing.

| If the device | Do |
|---|---|
| displays the message | step 5 |
| does not display the message | Confirm the correct device is selected as the trace device. If necessary, repeat step 3. |

5 Start the SPM upgrade shift by typing

```
>SET SHIFT STARTED
```

SWUPGRADE PM checks for the availability of a $XREF patch cross-reference file and processes patch cross-reference information.

6 Display the SWUPGRADE PM environment variables by typing

```
>DISPLAY VAR ALL
```

The variable name TRACE_DEVICE is the trace device established in step 3. SHIFT indicates the status of the current upgrade shift. CONCURRENCY indicates the maximum number of concurrent upgrades.

7 Display HELP for the CONCURRENCY variable by typing

```
>HELP VAR CONCURRENCY
```

8 Determine the maximum number of SPMs to upgrade concurrently. Note that a concurrency value set to UNLIMITED can exceed the maintenance window for the SPM upgrade shift in large scale offices. The maximum value cannot exceed eight.

The value defaults to eight if entering a value of UNLIMITED or greater than eight.

| If the value in CONCURENCY | Do |
|---|---|
| needs to be changed | step 9 |
| does not need to be changed | step 11 |

**9** Set the concurrency value by typing

```
>SET CONCURRENCY max_no
```

**10** Display the environment variables and confirm the change by typing

```
>DISPLAY VAR ALL
```

**11** Set prompting to on by typing

```
>PROMPTING ON
```

PROMPTING ON is the recommended method of operation. Set PROMPTING ON forces a pause after each automated step. This allows user intervention for the next required step. The remainder of this procedure assumes prompting is enabled.

**12** From a second terminal, post the nodes designated for an upgrade by typing

```
>MAPCI;MTC;PM;POST SPM spm_no
```

*Example*

```
>MAPCI;MTC;PM;POST SPM 23
```

**13** Display alarms on the RMs on the SPMs by typing

```
>QUERYPM FLT
```

**14** Display and note any alarms on the nodes by typing

```
>LISTALM
```

**15** Display and note the carrier statuses on the node by typing

```
>MAPCI;MTC;TRKS;CARRIER;POST SPM spm_no  1
```

**16** Determine the impact of the current alarm status on the upgrade.

| If there are | Do |
|---|---|
| alarms other than ISTB alarm | step 17 |
| no alarms or all alarms are ISTB alarms | step 18 |

**17** Perform the appropriate alarm clearing procedures. After completing the required procedures, go to step 18.

**18** From the SWUPGRADE device, begin the automated SPM upgrade by typing

```
>START
```

**19** Display and review the upgrade steps by typing

```
>DISPLAY STEPS
```

A step with an "_A_" identifies the step as an automated step. An "_M_" identifies the step as a manual step.

After an automated step has been completed the status changes from NEEDED to COMPLETED.

The columns marked as PERM, ACT, and PROC are used by other platforms and do not apply to the SPM upgrade.

Steps proceed automatically, however the option exists to manually select a step.

**20** Display HELP on the step you wish to execute by typing

```
>HELP STEP step_name
```

SWUPGRADE PM displays a brief description of the step including

- the nodes affected by the step
- the load(s) and PRSU(s) required by the step
- the steps required prior to the step

| If upgrading from | Do |
|---|---|
| an SN06 release to SN07 or higher | step 21 |
| an SN07 release or higher | step 22 |

**21** If upgrading to SN07 (or higher) from an SN06 release, Succession offices must only upgrade IW SPM IPs. To ensure this, choose only to upgrade steps identified by the presence of a GEM load (NTLZ20 resource module).

*IW SPM IP MAP Example*

```
PMUPGRADE task:       1
Node type:          SPM
Loaded from flash:  NO
Automated:          YES
Concurrency:      UNLIMITED
       Nodes:     SPM 0
                  SPM 1
       Loads:     GEM20CP
                  IWS20CQ
```

**22** Based on your office requirements, determine if you wish to upgrade or not upgrade (override) the step.

| If | Do |
|---|---|
| not upgrading a step | step 23 |
| upgrading a step | step 25 |

**23** Override the step by typing

```
>OVERRIDE step_name
```

**24** At the prompt, accept the override by typing

```
>Y
```

***Note:*** After overriding a step, the option to reinstate that step exists by typing **>RESET step_name** .

**25** Ensure that the HELP STEP command has been performed for every step_name.

| If all step_names have | Do |
|---|---|
| not been verified | step 20 |
| been verified | step 26 |

**26** Execute the upgrade process sequentially or out of sequence through one of the following commands:

| If executing the upgrade | Do |
|---|---|
| sequentially | Type<br>**>GO** |
| out of sequence | Type<br>**>RUNSTEP step_name**<br>**ATTENTION**<br>Do not choose to RUNSTEP a step_name that was selected for override. |

**27** Monitor the automated upgrade progress through the following:

- the trace device response
- the status of each node
- a log device

SWUPGRADE PM stops executing if:

- nodes are not ready for upgrading
- all nodes have been successfully upgraded
- An SPM upgrade failure occurs.
- The SWUPGRADE PM shift exceeds the 14 hour time limit.
- a SET SHIFT FINISHED or SET SHIFT ABORTED command has been entered

  ***Note:*** SET SHIFT FINISHED stops the step after the full upgrade for the nodes in the step has completed

  SET SHIFT ABORTED stops the step after the current maintenance action for node(s) has completed.

**28** After SWUPGRADE PM completes a step, the trace device displays an upgrade status report for each node.

| If | Do |
|---|---|
| every node in the step passed and you want to continue the SPM upgrade shift | step 19 |
| a node in the step failed | step 29 |
| every node in the step passed and you want to finish the SPM upgrade shift | step 30 |

***Note:*** Use the QUERYPM FILES command from the MAP display to confirm each node is correctly loaded and in-service.

**29** Possible reasons for a node failure are:

- The SPM status, or one of its units, changed due to a maintenance problem not related to the automated upgrade.
- The SPM load file or required PRSU files are not in the Destination Volume.
- The node encountered a hardware problem.

Review logs PM703, SPM650, SPM651,SPM300, SPM500,SPM335 and NODE500, plus the trace device output to determine why the node failed the automated upgrade.

| If you can | Do |
|---|---|
| determine why the node failed | Correct the problem and return to step 26 |

| If you can | Do |
|---|---|
| not determine why the node failed | Contact your next level of support.<br><br>If the problem is resolved, go to step 26<br><br>To continue the upgrade shift, go to step 19<br><br>To end the upgrade shift, go to step 30 |

**30** Finish the automated SPM upgrade shift by typing

```
>SET SHIFT FINISHED
```

*Result*

A Summary Report for PM Software Upgrade containing the following information:

- the step name
- the elapsed time between the previous and current step
- the time the step began
- the elapsed time to execute the step
- the final result status

A result status of STEP NOT COMPLETE indicates SWUPGRADE PM did not perform the step. This could indicate a step that was overridden and performed manually.

The SET SHIFT FINISHED command can generate a PM700 log that indicates the SPM upgrade shift has finished. No action is required for this log.

**31** Display the step of the automated SPM upgrade by typing

```
>DISPLAY STEPS
```

| If all steps | Do |
|---|---|
| except UPGRADE_COMPLETE are complete or overridden | step 32 |
| are not complete or overridden and you do not intend to continue[1] | step 35 |

1.If all steps are not complete and overridden the upgrade can be resumed at a later date by restarting this procedure at step 1.

**32** Execute the UPGRADE_COMPLETE step by typing

```
>GO
```

**33** Obtain the final record of all completed steps by typing

```
>DISPLAY STEPS
```

**34** Complete the UPGRADE_COMPLETE step by typing

```
>GO
```

**35** Quit the SWUPGRADE PM utility by typing

```
>QUIT
```

**36** Stop the terminal responses from printing by typing

```
>RECORD STOP ONTO printer
```

**37** You have completed this procedure.

Complete the automatic upgrade using the Completing the IW-SPM IP upgrade.

# Perform an IW SPM IP manual upgrade or downgrade

The following table defines the variables used in this procedure.

**Variable Abbreviations**

| Abbreviation | Definition |
|---|---|
| spm_no | the number of the SPM (0 to 85) |

Throughout the upgrade procedure, the request to type a command requires pressing the Enter key on the keyboard after the command has been typed.

## Perform a manual upgrade or downgrade

### *At the CI level of the MAP display*

**1** Ensure that the 'Prepare a manual upgrade or downgrade' section of this document has been completed.

**2** Post the SPM designated for an upgrade by typing

```
>MAPCI;MTC;PM;POST SPM spm_no
```

*Example*

```
>MAPCI;MTC;PM;POST SPM 23
```

**3** Check alarms on the SPM node and circuit packs by typing

| Alarm Source | Command |
|---|---|
| SPM node | **>LISTALM** |
| circuit pack | **>QUERYPM FLT** |

**4** Any alarms, other than ISTB alarms, must be cleared before continuing.

| If the alarm listings show | Do |
|---|---|
| alarms other than ISTB alarm | step 5 |
| no alarms or ISTB alarms only | step 6 |

5 Perform the appropriate alarm clearing procedure. After alarms other than ISTB have been cleared, continue to step 6.

| If performing | Do |
|---|---|
| an upgrade | step 6 |
| a downgrade | step 7 |

6 Upgrade circuit packs by protection groups for each IW SPM that requires an upgrade. The order for upgrading circuit packs, and the procedures are below.

***Note:*** The order for upgrading circuit packs is as follows: SRM -> GEM -> CEM.

| If | Do |
|---|---|
| SRM | Upgrading or Downgrading an SRM |
| GEM | Upgrade or Downgrade a GEM |
| CEM | Upgrading a CEM |
| After upgrading packs | step 10 |

7 The procedure for downgrading the CEM varies based on whether downgrading to a different release or within the same release.

***Note:*** The order for downgrading circuit packs is as follows: CEM -> GEM -> SRM.

| If downgrading to a | Do |
|---|---|
| different release (i.e. 16.0 -> 15.8) | step 8 |
| different version in the same release (i.e.15.4 ->15.3) | step 9 |

8 Downgrade circuit packs to an earlier release as follows:

| If | Do |
|---|---|
| CEM | "Downgrading a CEM to an earlier release" in *Upgrading the IW-SPM (IP)*, NN10056-461 |
| GEM | Upgrade or Downgrade a GEM |
| SRM | Upgrading or Downgrading an SRM |
| After downgrading packs | step 10 |

**9** Downgrade circuit packs to an earlier version within the same release as follows:

| If | Do |
|---|---|
| CEM | "Downgrading a CEM to an earlier release" in *Upgrading the IW-SPM (IP),* NN10056-461 |
| GEM | Upgrade or Downgrade a GEM |
| SRM | Upgrading or Downgrading an SRM |

**10** When all circuit packs protection groups have been upgraded or downgraded follow the Perform an IW SPM IP manual upgrade or downgrade procedure.

**ATTENTION**

Follow your company policy for soaking selected circuit packs before upgrading the rest of your office. See the appendix "Limited soak-in deployment" to soak a new load on a circuit pack without changing default loads in table PMLOADS and table MNCKTPAK.

# Upgrading or Downgrading an SRM

**CAUTION**

Complete the procedure Prepare an IW SPM IP manual upgrade or downgrade before upgrading or downgrading a component.

This procedure changes the software load for a Sync Resource Module (SRM) which provides the timing source for the switch.

Both IW SPMs with SRMs configured must be upgraded prior to upgrading the remaining IW SPMs. After upgrading the first SPM/SRM, immediately upgrade the second SPM/SRM. It is important to upgrade the SPM/SRMs one after the other, not simultaneously.

The following Variable Abbreviations table defines the variables used in this procedure.

**Variable Abbreviations**

| Abbreviation | Definition |
|---|---|
| spm_no | the number of the SPM (0 to 85) |
| rm_no | the Sync RM number |
| link_no | the BITS link number (0 to 2) |
| patch_id | the PRSU name |

***At the CI level of the MAP display***

1 Access and monitor the switch timing links at the clock level of the MS to determine the STANDBY SRM by typing

```
>MAPCI;MTC;MS;CLOCK
```

*Example of a MAP screen:*

```
  MS 0       .          Master         F                    . .
  MS 1       .          Slave          F                    . .

Shelf 0                 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2
Card  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
Chain           |     |
MS 0  . . . . . I - - I - - - - - - - - . - - . . . . . .
MS 1  . . . . . I - - I - - - - - - - - F - - . . . . . .

Card 02 Alm Stat %Adj Src | Car Stat Sp PM     RMTyp SSM
MS 0  .  .  Lkg +08.6 Lk0 | Lk0 Lck   - SPM 022 SRM  PRS
MS 1  .  .  Syn -00.8 Ms0 | Lk1 Smp   - SPM 023 SRM  PRS
Links Slipping:  NA   out of  NA
MTC:
MS:
SHELF:
CLOCK:
```

***Note:*** The active timing node is indicated by “Lck” in the “Stat” column. In this example, SPM 022 is the active SPM/SRM (the SRM that is providing the clocking reference to the MS). Therefore the upgrade would begin on SPM 023.

**2** From a second window, post the SPM with the STANDBY SRM by typing

**>MAPCI;MTC;PM;POST SPM spm_no**

*Example of a MAP screen:*

```
SPM 23  INSV     Class: IW
Shlf0 SL A Stat  Shlf0 SL A Stat  Shlf1 SL A Stat  Shlf1 SL A Stat
--- -  1 A Insv  CEM 1  8 I Insv  --- -  1 - ----  --- -  8 - ----
--- -  2 A Insv  GEM 0  9 A Insv  --- -  2 - ----  --- -  9 - ----
--- -  3 I Insv  GEM 1 10 I Insv  --- -  3 - ----  --- - 10 - ----
--- -  4 A Insv  --- - 11 A Insv  --- -  4 - ----  --- - 11 - ----
--- -  5 - ----  --- - 12 A Insv  --- -  5 - ----  --- - 12 - ----
SRM 0  6 A ISTb  --- - 13 I Insv  --- -  6 - ----  --- - 13 - ----
CEM 0  7 A Insv  --- - 14 A Insv  --- -  7 - ----  --- - 14 - ----
```

**3** Access the SRM card by typing

**>SELECT SRM 0**

*Example of a MAP screen:*

```
Interface:

Loc : Row D FrPos 1 ShPos 6 ShId 0 Slot 6  Prot Grp : 1
Default Load: SYN19EF                      Prot Role: Working
```

**4** Ensure that the SRM is in an ISTB condition with the new load listed as default, by typing.

**>QUERYMOD**

*Example of a MAP screen:*

```
SPM 23   SRM 0  Query: Request has been submitted.
SRM  0 ISTb Act    Loc: Row D  FrPos  1 ShPos  6 ShId 0  Slot  6

Default Load: SYN19EF             Actual Load: SYN17EDD
```

**5** Access the BITS link level by typing

**>BITS**

*Example of a MAP screen:*

```
SPM 23    SRM 0
   LinkNo   BitsName   Status  State   SSM   AlmSev
     0      BITSA       Act    InSv    PRS
     1      BITSB       InAct  InSv    PRS
.    2      BITSOUT            Uneq    NIL
BITS:
```

**6** Record the BITS link numbers associated with the SRM and the state of each link.

**7** Manual busy (ManB) the inactive BITS links by typing

**>BSY link_no**

*Example*

**>BSY 1**

*Response*

```
Busy:Request has been Submitted.
Busy:Command Completed.State Change has passed.
```

**8** Force the active BITS links to ManB by typing

**>BSY link_no FORCE**

*Example*

**>BSY 0 FORCE**

*Response*

```
WARNING: BITSB Link is a Timing Link.
Do you want to BUSY this Link.
Please confirm ("YES","Y","NO",or "N"):
```

**9** At the confirmation prompt, type:

**>Y**

*Response*

```
Busy:Request has been Submitted.
Busy:Command Completed.State Change has passed.
```

**10** Return to the SRM level by typing

**>QUIT**

**11** Force the SRM to ManB by typing

**>BSY FORCE**

*Response*

```
WARNING: This RM provides timing information.
Bsying out this RM might result in loss of
Synchronization.
A Bsy action may impact services on this node.
Do you wish to continue?
Please confirm ("YES","Y","NO",or "N"):
```

**12** At the confirmation prompt, type:

**>Y**

*Response*

SRM `Busy:Request has been Submitted.`

SRM `Busy:Command Completed.`

**13** Load the SRM with the new load by typing

**>LOADMOD**

| If the loadname is | Do |
|---|---|
| not in the SPMLDVAL table | step 14 |
| in the SPMLDVAL table | step 15 |

**14** At the confirmation prompt, continue by typing

**>Y**

### Example of MAP response

>y
*** WARNING: Table SPMLDVAL is not datafilled for this loadname. Contact your next level of support before proceeding with upgrade. Do you want to continue without datafilling the table?

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

| If choosing to | Do |
|---|---|
| continue | step 15[1] |
| update the SPMLDVAL table | stop the upgrade and contact the next level of support |

1.Continuing the upgrade when the loadname is not in the SPMLDVAL table prevents that load from being available in that table for future reference.

**15** At the confirmation prompt, type:

**>Y**

*Response*

```
SRM Load:Request has been submitted.
SRM Load: Command Completed. Command Passed
```

| If the SRM device is | Do |
|---|---|
| the first for the office | step 16 |
| the second for the office | step 23 |

**16** Open a third window and access the PRSM tool by typing

**>PRSM**

**17** Ensure that PRSM recognizes any pre-applied PRSUs and has found all applied PRSU files by typing

**>DBAUDIT SPM spm_no SRM rm_no**

*Example*

**>DBAUDIT SPM 23 SRM 0**

### Example of MAP response

Database audit submitted for 1 DESTs
Auditing destination SPM 23 SRM 0....
Database audit completed for 1 DEST
Database audit completed for 1 DEST
Database discrepancy found in 0 DESTs

**18** Identify if PRSM found all patch files built into the PPSL by typing

**>SELECT PRSUID CATEGORY STATUS BUILTIN FROM DESTSET SPM spm_no SRM rm_no**

### Example of MAP response

```
>select prsuid category status builtin from destset spm 23 srm 0
PRSUID     CAT     ST    BUILTIN
------------ -----     ---    ------------
TAB51S0P    GEN   A     Y
BUZ80S0P    GEN   A     Y
CTC51S0P    GEN   A     Y
DXH62S0P    GEN   A     Y
 DXH63S0P  GEN    A     Y
JXM65S0P    GEN   A      Y
KAA01S0P    GEN   A      Y
KRI62S0P    GEN   A      Y
LLH11S0P    GEN   A      Y
SBF80S0P    GEN   A      Y
SBF90S0P    GEN   A     Y
TAV54S0P    GEN  A     Y
```

***Note:*** An empty list appears for a non-PPSL load (the load is not pre-patched).

An unknown category displayed as question marks (???) appears if PRSM cannot locate PRSU files in a PPSL during the first dbaudit of a newly loaded SPM device. This situation does not occur if all PRSU files have been placed in a PADNDEV table defined volume as instructed in the Upgrade Preparation procedure.

If this situation should occur use the validate command in PRSM for each PRSU with a category of ??? in at least one applicable DEST. For example: **VALIDATE ABC30S0Q IN SPM 23 SRM 0**

Also before proceeding to the next device type, ensure that all patch files are placed in the PADNDEV table defined volume according to the Upgrade Preparation procedure.

**19** If required, patch the SRM device.

| If patches | Do |
|---|---|
| are required for the load file | step 20 |
| are not required for the load file | step 21 |

***Note:*** The required patches were printed in of the procedure entitled “Preparing a manual upgrade or downgrade”.

**20** Apply the patches by typing

```
>APPLY 'patch_id | patch_id | patch_id IN SPM
spm_no  SRM rm_no
```

*Example*

```
>APPLY 'ABC05513 | DEF10513 | GHI45513 IN SPM 23
SRM 0
```

***Note:*** Repeat the command as necessary to apply additional patches.

**21** Ensure that the SRM is correctly patched by typing

```
>REPORT DEST SPM spm_no SRM rm_no
```

*Example*

```
>REPORT DEST SPM 23 SRM 0
```

***Note 1:*** For the first SRM, the output should be the combination of the PSRUs applied in step 20 and the pre-applied PRSUs displayed in step 18.

***Note 2:*** For the second SRM, the list of patches should be identical to the list obtained in this step for the first SRM.

### Example of MAP response

```
REPORT DEST SPM 23 SRM 0
PRSUID          STATDATE STATT CAT ACT ST LOADNAME H DESTID
--------------- -------- ----- --- --- -- -------- - ----------------------
ABC05S13       20020915 23:29 GEN A SRM20BU N SPM 23 SRM 0
DEF10S13       20020915 23:33 GEN A SRM20BU N SPM 23 SRM 0
GHI45S13       20020915 23:36 GEN A SRM20BU N SPM 23 SRM 0
TAB51S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
CTC51S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
BUZ80S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
DXH63S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
DXH62S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
JXM65S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
KAA01S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
KRI62S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
LLH11S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
SBF80S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
SBF90S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
TAV54S0P      20020915 23:10 GEN A SRM20BU N SPM 23 SRM 0
```

**22** Exit the PRSM tool by typing

```
>QUIT
```

**23** From the second window opened in step 2, return the SRM to service by typing

```
>RTS
```

*Response*

```
SPM SRM RTS:Request has been submitted.
SPM SRM RTS: Command Completed.
```

**24** Access the BITS level by typing

```
>BITS
```

**25** Restore the BITS links to service by typing

```
>RTS  link_no
```

*Example*

```
>RTS   0
>RTS   1
```

*Result*

The links change from InAct ManB to Act InSv and InAct InSv.

**26** Return to the SPM level by typing

```
>QUIT
```

**27** Return to the posted node level by typing

```
>QUIT
```

**28** Display alarms on the SPM by typing

```
>QUERYPM FLT
```

Display alarms on the SPM by typing

```
>LISTALM
```

If new alarms were introduced during this procedure, clear the alarms using procedures in the Fault Management section.

| If the SRM device is | Do |
|---|---|
| the first for the office | step 29 |
| the second for the office | step 31 |

**29** From the original window in step 1, switch the SRM from ACTIVE to STANDBY by typing

```
>SWCARR
```

**30** Go to step 1 and repeat the procedure for the second SRM.

**31** The SRM circuit pack protection group upgrade or downgrade is completed.

| If | Do |
|---|---|
| upgrading | Upgrade or Downgrade a GEM on page 664 |
| downgrading | Completing the IW-SPM IP upgrade on page 1547 |

# Upgrade or Downgrade a GEM

The procedure requires:

- in-service loading the inactive GEM
- switching activity between the inactive and the active GEM
- loading the inactive GEM
- switching activity to return resources to original locations

The following table defines the variables used in this procedure.

**Variable Abbreviations**

| Abbreviation | Definition |
|---|---|
| spm_no | the number of the SPM (0 to 85) |
| inact_rm | the number of the inactive GEM |
| rm_no | the number of the GEM number |
| prsu_id | the PRSU name |
| act_rm | the number of an active GEM |
| shelf_no | the shelf number of the inactive GEM |

## Upgrading or downgrading a GEM

### *At the CI level of the MAP display*

**1** If not already posted, post the SPM by typing

```
>MAPCI;MTC;PM;POST SPM spm_no
```

**2** Record the unit number and shelf number of the inactive GEM in the circuit pack protection group. Also record the number of the inactive CEM.

**3** Select the inactive GEM by typing

```
>SELECT GEM inact_rm
```

*Example*

```
>SELECT GEM 1
```

*Result*

Both GEMs are in an ISTb status due to the load name change made in the MNCKTPAK table.

4 Ensure that the GEM is ISTB and inactive by typing.

```
>QUERYMOD
```

***Note:*** The default load is the new load and the actual load is the load scheduled for change.

### Example of MAP display

```
SPM  23  GEM  1 Query: Request has been submitted.
GEM  1 ISTb InAct  Loc: Row CC  FrPos 28 ShPos  0 ShId 0 Slot 10
Default Load: GEM198BI                Actual Load: GEM19BU
```

5 In-service load the inactive RM by typing

```
>LOADMOD INSVLD
```

During execution of the LOADMOD INSVLD command, the RM automatically goes to a SysB state and then returns to service.

| If the loadname is | Do |
|---|---|
| not in the SPMLDVAL table | step 6 |
| in the SPMLDVAL table | step 7 |

6 At the confirmation prompt, continue by typing

```
>Y
```

### Example of MAP response

```
>y
*** WARNING: Table SPMLDVAL is not datafilled for this loadname. Contact
your next level of support before proceeding with upgrade. Do you want to
continue without datafilling the table?

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

| If choosing to | Do |
|---|---|
| continue | step 7[1] |
| update the SPMLDVAL table | stop the upgrade and contact the next level of support |

1.Continuing the upgrade when the loadname is not in the SPMLDVAL table prevents that load from being available in that table for future reference.

7 At the confirmation prompt, continue by typing

```
>Y
```

### Example of MAP response

```
SPM 23  GEM  1   Load: Request has been submitted.
SPM 23 GEM  1  Load: Command completed. Command passed.
```

| If the GEM load is | Do |
|---|---|
| the first for this office | step 8 |
| not the first for this office | step 14 |

**8** Open a second window and access the PRSM tool by typing

```
>PRSM
```

**9** Ensure that PRSM recognizes any pre-applied PRSUs by typing

```
>DBAUDIT SPM spm_no GEM rm_no
```

*Example*

```
>DBAUDIT SPM 23 GEM 1
```

### Example of MAP response

```
Database audit submitted for 1 DESTs
Auditing destination SPM 23 GEM 1....
Database audit completed for 1 DEST
Database audit completed for 1 DEST
Database discrepancy found in 0 DESTs
```

**10** Identify if PRSM found all patch files built into the PPSL by typing

```
>SELECT PRSUID CATEGORY STATUS BUILTIN FROM
DESTSET SPM spm_no CEM cem_no
```

### Example of MAP response

```
>select prsuid category status builtin from destset spm 23 cem 0
PRSUID     CAT     ST    BUILTIN
---------- -----   ---   ----------
TAB51S0P    GEN   A     Y
BUZ80S0P    GEN   A     Y
CTC51S0P    GEN   A     Y
DXH62S0P    GEN   A     Y
DXH63S0P   GEN    A     Y
JXM65S0P    GEN   A      Y
KAA01S0P    GEN   A      Y
KRI62S0P    GEN   A      Y
LLH11S0P    GEN   A      Y
SBF80S0P    GEN   A      Y
SBF90S0P    GEN   A     Y
TAV54S0P    GEN  A     Y
```

***Note:*** An empty list appears for a non-PPSL load (the load is not pre-patched).

An unknown category displayed as question marks (???) appears if PRSM cannot locate PRSU files in a PPSL during

the first dbaudit of a newly loaded SPM device. This situation does not occur if all PRSU files have been placed in a PADNDEV table defined volume as instructed in the Upgrade Preparation procedure.

If this situation should occur use the validate command in PRSM for each PRSU with a category of??? in at least one applicable DEST. For example: **VALIDATE ABC30S0Q IN SPM 23 GEM 1**

Also before proceeding to the next device type, ensure that all patch files are placed in the PADNDEV table defined volume according to the Upgrade Preparation procedure.

**11** If required, patch the GEM load file.

| If patches | Do |
|---|---|
| are required for the load file | step 12 |
| are not required for the load file | step 13 |

**12** Apply the patches by typing

```
>APPLY 'patch_id | patch_id | patch_id IN SPM
spm_no  GEM inact_rm
```

*Example*

```
>APPLY 'ABC05513 | DEF10513 | GHI45513 IN SPM 23
GEM 1
```

***Note:*** Repeat the command as necessary to apply additional patches.

**13** Ensure that the inactive GEM has been patched correctly by typing

```
>REPORT DEST SPM spm_no GEM inact_rm
```

*Example*

```
>REPORT DEST SPM 23 GEM 1
```

***Note:*** The output should be the combination of the PSRUs applied in and the pre-applied PRSUs displayed in.

### Example of MAP response

```
REPORT DEST SPM 23 GEM 1
PRSUID          STATDATE STATT CAT ACT ST LOADNAME H DESTID
--------------- -------- ----- --- --- -- -------- - ----------------------
ABC05S13       20020915 23:29 GEN A GEM19BU N SPM 23 GEM 1
DEF10S13       20020915 23:33 GEN A GEM19BU N SPM 23 GEM 1
GHI45S13       20020915 23:36 GEN A GEM19BU N SPM 23 GEM 1
TAB51S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
CTC51S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
BUZ80S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
DXH63S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
DXH62S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
JXM65S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
KAA01S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
KRI62S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
LLH11S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
SBF80S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
SBF90S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
TAV54S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 1
```

**14** From the original window, access the protection level of the MAP by typing

**>PROT**

**15** Switch activities from the active GEM to the inactive GEM by typing

**>MANUAL act_rm inact_rm**

*Example*

**>MANUAL 0 1**

**16** Confirm the system prompt by typing

**>Y**

*Result*

The active GEM becomes the inactive GEM and the former inactive (upgraded) GEM becomes active.

**17** Exit the PROT level by typing

**>QUIT**

**18** Select the inactive GEM by typing

**>SELECT inact_rm**

*Example*

**>SELECT GEM 0**

**19** Ensure that the GEM is ISTb and inactive by typing

**>QUERYMOD**

**20** Mate load the inactive GEM from its mate by typing

```
>LOADMOD MATE act_rm
```

*Example*

```
>LOADMOD MATE 1
```

During execution of the command, the RM automatically goes to a SysB state and then returns to service.

**21** At the confirmation prompt, continue by typing

```
>Y
```

### Example of MAP response

```
SPM 23   GEM  0   Load: Request has been submitted.
SPM 23  GEM  0   Load: Command completed. Command passed.
```

**22** From the second window running the PRSM tool, ensure that SPARTS correctly patched the RM by typing

```
>REPORT DEST SPM spm_no GEM inact_rm
```

*Example*

```
>REPORT DEST SPM 23 GEM 0
```

***Note:*** The resulting list should match the list obtained in step 13.

### Example of MAP response

```
REPORT DEST SPM 23 GEM 0
PRSUID          STATDATE STATT CAT ACT ST LOADNAME H DESTID
---------------- -------- ----- --- --- -- -------- - ----------------------
ABC05S13       20020915 23:29 GEN A GEM19BU N SPM 23 GEM 0
DEF10S13       20020915 23:33 GEN A GEM19BU N SPM 23 GEM 0
GHI45S13       20020915 23:36 GEN A GEM19BU N SPM 23 GEM 0
TAB51S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
CTC51S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
BUZ80S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
DXH63S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
DXH62S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
JXM65S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
KAA01S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
KRI62S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
LLH11S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
SBF80S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
SBF90S0P     20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
TAV54S0P      20020915 23:10 GEN A GEM19BU N SPM 23 GEM 0
```

**23** Ensure that any patch failures are corrected by typing

```
>ISTBAUDIT SPM spm_no GEM inact_rm
```

*Example*

```
>ISTBAUDIT SPM 23 GEM 0
```

### Example of MAP response

```
This DEST set does not have any patch-related problems.
```

**24** Exit the PRSM tool by typing

```
>QUIT
```

**25** From the original window, access the protection level of the MAP by typing

```
>PROT
```

**26** Switch activities from the active GEM to the inactive GEM by typing

```
>MANUAL act_rm inact_rm
```

*Example*

```
>MANUAL 1 0
```

**27** Confirm the system prompt by typing

```
>Y
```

**28** The GEM circuit pack upgrade is completed.

| If | Do |
|---|---|
| upgrading | Upgrading a CEM |
| downgrading | Completing the IW-SPM IP upgrade |

In summary, this upgrade procedure requires:

- in-service loading the inactive CEM
- switching activity between the inactive and the active CEM
- in-service loading the inactive CEM
- switching activity to return resources to the original location

The Variable Abbreviations table defines the variables used in this procedure.

**Variable Abbreviations**

| Abbreviation | Definition |
|---|---|
| spm_no | the number of the SPM |
| rm_no | the CEM resource module (RM) number |
| inact_rm | the number of the inactive CEM RM |
| act_rm | the number of the active CEM RM |
| prsu_id | the PRSU name |

**Upgrade a CEM**

***At the CI level of the MAP display***

**1** If not already posted, post the node by typing

```
>MAPCI;MTC;PM;POST SPM spm_no
```

*Example*

```
>MAPCI;MTC;PM;POST SPM 23
```

**2** Record the unit number and shelf number of the inactive CEM.

**3** Select the inactive CEM, designated with an “I”, by typing

```
>SELECT CEM inact_rm
```

*Example*

```
>SELECT CEM 1
```

**4** In-service load the inactive CEM by typing

```
>LOADMOD INSVLD
```

During execution of the command, the CEM automatically goes to a SysB state and then returns to service.

| If the loadname is | Do |
|---|---|
| not in the SPMLDVAL table | step 5 |
| in the SPMLDVAL table | step 6 |

**5** At the confirmation prompt, continue by typing

```
>Y
```

### Example of MAP response

```
>y
*** WARNING: Table SPMLDVAL is not datafilled for this loadname. Contact
your next level of support before proceeding with upgrade. Do you want to
continue without datafilling the table?

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

| If choosing to | Do |
|---|---|
| continue | step 6[1] |
| update the SPMLDVAL table | stop the upgrade and contact the next level of support |

1.Continuing the upgrade when the loadname is not in the SPMLDVAL table prevents that load from being available in that table for future reference.

**6** At the confirmation prompt, continue by typing

```
>Y
```

| If the CEM device is | Do |
|---|---|
| the first for this office | step 7 |
| not the first for this office | step 13 |

**7** Open a second window and access the PRSM tool by typing

```
>PRSM
```

**8** Ensure that PRSM recognizes any pre-applied PRSUs and has found all applied PRSU files by typing

```
>DBAUDIT SPM spm_no CEM inact_rm
```

*Example*

```
>DBAUDIT SPM 23 CEM 1
```

### Example of MAP response

```
Database audit submitted for 1 DESTs
Auditing destination SPM 23  CEM 1....
Database audit completed for 1 DEST
Database audit completed for 1 DEST
Database discrepancy found in 0 DESTs
```

**9** Identify if PRSM found all patch files built into the PPSL by typing

```
>SELECT PRSUID CATEGORY STATUS BUILTIN FROM
DESTSET SPM spm_no CEM rm_no
```

### Example of MAP response

```
>select prsuid category status builtin from destset spm 23 cem 0
PRSUID     CAT     ST    BUILTIN
-------------  -----     ---   ------------
TAB51S0P    GEN   A     Y
BUZ80S0P    GEN   A     Y
CTC51S0P    GEN   A     Y
DXH62S0P    GEN   A     Y
 DXH63S0P  GEN    A     Y
JXM65S0P    GEN   A      Y
KAA01S0P    GEN   A      Y
KRI62S0P    GEN   A      Y
LLH11S0P    GEN   A      Y
SBF80S0P    GEN   A      Y
SBF90S0P    GEN   A     Y
TAV54S0P    GEN  A     Y
```

***Note:*** An empty list appears for a non-PPSL load (the load is not pre-patched).

An unknown category displayed as question marks (???) appears if PRSM cannot locate PRSU files in a PPSL during the first dbaudit of a newly loaded SPM device. This situation does not occur if all PRSU files have been placed in a PADNDEV table defined volume as instructed in the Upgrade Preparation procedure.

If this situation should occur use the validate command in PRSM for each PRSU with a category of ??? in at least one applicable DEST. For example: **VALIDATE ABC30S0Q IN SPM 23 CEM 1**

Also before proceeding to the next device type, ensure that all patch files are placed in the PADNDEV table defined volume according to the Upgrade Preparation procedure.

**10** If required, patch the CEM load file.

| If patches | Do |
|---|---|
| are required for the RM load file | step 11 |
| are not required for the RM load file | step 13 |

***Note:*** The required patches were printed in step 17 of the procedure entitled “Prepare a manual upgrade or downgrade”.

**11** Apply the patches by typing

```
>APPLY 'prsu_id | prsu_id | prsu_id IN SPM
spm_no  CEM inact_rm
```

*Example*

```
>APPLY 'ABC05S13 | DEF10S13 | GHI45S13 IN SPM 23
CEM 1
```

***Note:*** Repeat the command as necessary to apply additional patches.

**12** Ensure that the inactive CEM is correctly patched by typing

```
>REPORT DEST SPM spm_no CEM inact_rm
```

*Example*

```
>REPORT DEST SPM 23 CEM 1
```

***Note:*** The output should be the combination of the PSRUs applied in step 11 and the pre-applied PRSUs displayed in step 9.

### Example of MAP response

```
REPORT DEST SPM 23 CEM 1
PRSUID          STATDATE STATT CAT ACT ST LOADNAME H DESTID
--------------- -------- ----- --- --- -- -------- - ----------------------
ABC05S13      20020915 23:29 GEN A CEM17BU N SPM 23 CEM 1
DEF10S13      20020915 23:33 GEN A CEM17BU N SPM 23 CEM 1
GHI45S13      20020915 23:36 GEN A CEM17BU N SPM 23 CEM 1
TAB51S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
CTC51S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
BUZ80S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
DXH63S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
DXH62S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
JXM65S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
KAA01S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
KRI62S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
LLH11S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
SBF80S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
SBF90S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
TAV54S0P     20020915 23:10 GEN A CEM17BU N SPM 23 CEM 1
```

**13** From the original window, access the protection level of the MAP by typing

```
>PROT
```

**14** Switch activities from the active CEM to the inactive CEM by typing

```
>MANUAL
```

**15** Confirm the system prompt by typing

```
>Y
```

*Result*

The active CEM becomes the inactive CEM and the former inactive (upgraded) CEM becomes active.

**16** Exit the PROT level by typing

```
>QUIT
```

**17** Select the inactive CEM by typing

```
>SELECT inact_rm
```

*Example*

```
>SELECT CEM 0
```

**18** Ensure that the CEM is ISTb and inactive by typing

```
>QUERYMOD
```

**19** In-service load the inactive CEM by typing

```
>LOADMOD INSVLD
```

During execution of the command, the RM automatically goes to a SysB state and then returns to service.

**20** At the confirmation prompt, continue by typing

```
>Y
```

**21** From the second window running the PRSM tool, ensure that SPARTS correctly patched the RM by typing

```
>REPORT DEST SPM spm_no CEM inact_rm
```

*Example*

```
>REPORT DEST SPM 23 CEM 0
```

***Note:*** The resulting list should match the list obtained in step 12.

### Example of MAP response

```
REPORT DEST SPM 23 CEM 0
PRSUID          STATDATE STATT CAT ACT ST LOADNAME H DESTID
--------------- -------- ----- --- --- -- -------- - ----------------------
ABC05S13       20020915 23:29 GEN A CEM17BU N SPM 23 CEM 0
DEF10S13       20020915 23:33 GEN A CEM17BU N SPM 23 CEM 0
GHI45S13       20020915 23:36 GEN A CEM17BU N SPM 23 CEM 0
TAB51S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
CTC51S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
BUZ80S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
DXH63S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
DXH62S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
JXM65S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
KAA01S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
KRI62S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
LLH11S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
SBF80S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
SBF90S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
TAV54S0P      20020915 23:10 GEN A CEM17BU N SPM 23 CEM 0
```

**22** Ensure that any patch failures are corrected by typing

**>ISTBAUDIT SPM spm_no CEM inact_rm**

*Example*

**>ISTBAUDIT SPM 23 CEM 0**

### Example of MAP response

```
This DEST set does not have any patch-related problems.
```

**23** Exit the PRSM tool by typing

**>QUIT**

**24** From the original window, access the protection level of the MAP by typing

**>PROT**

**25** Switch activities from the active CEM to the inactive CEM by typing

**>MANUAL**

**26** Confirm the system prompt by typing

**>Y**

**27** Exit the protection level by typing

**>QUIT**

**28** Display any CEM alarms by typing

**>QUERYMOD**

**29** Exit the CEM level by typing

```
>QUIT
```

**30** Display any SPM alarms, with both CEMs in service, by typing

```
>LISTALM
```

**31** If new alarms were introduced during this procedure, clear the alarms using procedures in the Fault Management section.

**32** The CEM circuit pack upgrade procedure is complete.

Complete the upgrade using the Completing the IW-SPM IP upgrade procedure.

# Upgrading the CS 2000 Management Tools software

## Upgrade strategy

Upgrading CS 2000 Management Tools software occurs when a new load is delivered to the customer site. Upgrade loads are delivered on a CD-ROM.

**ATTENTION**
The core manager must be upgraded prior to upgrading the CS 2000 Management Tools. Once the core manager is upgraded, you cannot provision Gateway Controllers (GWCs) until the CS 2000 Management (CS2M) software package on the CS 2000 Management Tools server is upgraded to the same release.

**ATTENTION**
Once you begin an upgrade of the CS2000 Management Tools applications, continue until you have upgraded each application to (I)SN07. Failing to upgrade an application to the (I)SN07 release will result in operational difficulties.

**ATTENTION**
During an end-to-end upgrade, upgrading the SAM21 shelf controller is part of upgrading the CS 2000 Management Tools to facilitate migration of the CS 2000 SAM21 Manager. Therefore, use the procedures included with the CS 2000 Management Tools to upgrade the SAM21 shelf controller and not the procedures in the SAM21 documentation suite.

The supported upgrade paths to the (I)SN07 release are listed below. Follow the link associated with the release you are upgrading from.

- Upgrading from (I)SN05 to (I)SN07 on page 679
- Upgrading from (I)SN06 to (I)SN07 on page 683
- Upgrading from (I)SN06.2 to (I)SN07 on page 685
- Upgrading from (I)SN07 to (I)SN07 (maintenance release) on page 693

## Upgrading from (I)SN05 to (I)SN07

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

**ATTENTION**

If you are upgrading from (I)SN05 and you have the Audio Provisioning Server (APS) on a separate server from the CS 2000 Management Tools, you need to combine the servers prior to upgrading the office to the (I)SN07 release. This procedure assumes that APS is on the same server as the CS 2000 Management Tools for an (I)SN05 to an (I)SN07 upgrade.

**ATTENTION**

The SSPFS must be at the latest maintenance release (MNCL) for the release you are currently running, and be patch-current, prior to performing the upgrade procedures.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN05 to (I)SN07 Upgrade checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Upgrade the Succession Server Platform Foundation Software (SSPFS). | | Perform procedure Upgrading SSPFS software on page 698. |
| 2 | Install any SSPFS MNCLs.<br><br>***Note:*** Only perform this activity if you received a notification bulletin that an SSPFS MNCL is available for the release you just upgraded to. | | Refer to the instructions provided with the MNCL. |
| 3 | Apply any SSPFS patches. | | Perform procedure Applying patches using the NPM on page 1674. |
| 4 | Configure the CM CLLI. | | Perform procedure Setting the CS 2000 CLLI on an SSPFS-based server on page 911. |

## (I)SN05 to (I)SN07 Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 5 | Set up the BootP file.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Setting up the BootP file on SSPFS on page 702. |
| 6 | Install the CS 2000 Management Components (CS2M) software package. | | Perform procedure Installing or upgrading the CS2M software on page 711. |
| 7 | Apply all patches to the following devices on the CS 2000 Management Tools server: PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Applying patches using the NPM on page 1674 . |
| 8 | Start the SESM server application. | | Perform procedure Starting the SESM server application on page 719 . |
| 9 | Stop and start the Patching Server Element (PSE) on each of the Media Gateway 9000 (MG 9000) manager servers (t1400). That is on the MG 9000 manager server, MG 9000 manager midtier, and MG 9000 manager OMCollector.<br><br>***Note:*** Only perform this activity if you have MG 9000 network elements in your network. | | Perform procedure Stopping the PSE server application on a Sun server on page 774 . |
| | | | Perform procedure Starting the PSE server application on a Sun server on page 775 . |
| 10 | Upgrade the Audio Provisioning Server (APS) software. | | Perform procedure Upgrading APS software on page 725. |

## (I)SN05 to (I)SN07 Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 11 | Migrate the SAM21 Manager data from the core manager to the CS 2000 Management Tools server.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Migrating the CS 2000 SAM21 Manager data on page 742 . |
| 12 | Install the SAM21 platform fileset on the core manager.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Installing SAM21 Platform software on page 744 . |
| 13 | Start the SAM21EM server application. | | Perform procedure Starting the SAM21 Manager server application on page 722 . |
| 14 | Launch the CS 2000 SAM21 Manager client application that resides on the CS 2000 Management Tools server.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Launching CS 2000 Management Tools client applications on page 1651 .<br><br>***Note:*** Java™ 2 Runtime Environment (JRE) version 1.4.1_02 and Java™ Web Start (JWS) version 1.2.0_02 must be installed. The “Client Software Install Guide” link on the launch page, provides instructions on how to verify the version, and provides the installation packages and instructions, if required. The user who installs JWS and JRE must have administration privileges on the client workstation. |
| 15 | Upgrade the shelf controllers to (I)SN07 for all shelves using the CS 2000 SAM21 Manager client that resides on the core manager.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Upgrading software on the SAM21 Shelf Controller on page 752. |

## (I)SN05 to (I)SN07 Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 16 | Migrate all the SAM21 shelves to the CS 2000 SAM21 Manager that resides on the CS 2000 Management Tools server.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Migrating the SAM21 network elements to the CS 2000 SAM21 Manager on the CS 2000 Management Tools server on page 762. |
| 17 | Complete the SAM21Manager migration, which includes removing the SAM21 Manager fileset from the core manager.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Completing the CS 2000 SAM21 Manager migration on page 770. |
| 18 | Complete the CS 2000 Management Tools upgrade. | | Refer to Completing the CS 2000 Management Tools upgrade on page 1549. |

## Upgrading from (I)SN06 to (I)SN07

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

**ATTENTION**
The SSPFS must be at the latest maintenance release (MNCL) for the release you are currently running, and be patch-current, prior to performing the upgrade procedures.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN06 to (I)SN07 Upgrade checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Upgrade the Succession Server Platform Foundation Software (SSPFS). | | Perform procedure Upgrading SSPFS software on page 698. |
| 2 | Install any SSPFS MNCLs.<br><br>***Note:*** Only perform this activity if you received a notification bulletin that an SSPFS MNCL is available for the release you just upgraded to. | | Refer to the instructions provided with the MNCL. |
| 3 | Apply any SSPFS patches. | | Perform procedure Applying patches using the NPM on page 1674. |
| 4 | Configure the CM CLLI. | | Perform procedure Setting the CS 2000 CLLI on an SSPFS-based server on page 911. |
| 5 | Set up the BootP file.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Setting up the BootP file on SSPFS on page 702. |
| 6 | Install the CS 2000 Management Components (CS2M) software package. | | Perform procedure Installing or upgrading the CS2M software on page 711. |

## (I)SN06 to (I)SN07 Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 7 | Apply all patches to the following devices on the CS 2000 Management Tools server: PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Applying patches using the NPM on page 1674. |
| 8 | Start the SESM and SAM21EM server applications. | | Perform procedure Starting the SESM server application on page 719. |
| | | | Perform procedure Starting the SAM21 Manager server application on page 722. |
| 9 | Stop and start the Patching Server Element (PSE) on each of the Media Gateway 9000 (MG 9000) manager servers (t1400). That is on the MG 9000 manager server, MG 9000 manager midtier, and MG 9000 manager OMCollector.<br><br>***Note:*** Only perform this activity if you have MG 9000 network elements in your network. | | Perform procedure Stopping the PSE server application on a Sun server on page 774. |
| | | | Perform procedure Starting the PSE server application on a Sun server on page 775. |
| 10 | Upgrade the Audio Provisioning Server (APS) software. | | Perform procedure Upgrading APS software on page 725. |
| 11 | Install the SAM21 platform fileset on the core manager.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Installing SAM21 Platform software on page 744. |
| 12 | Complete the CS 2000 Management Tools upgrade. | | Refer to Completing the CS 2000 Management Tools upgrade on page 1549. |

## Upgrading from (I)SN06.2 to (I)SN07

The configurations that support an upgrade from (I)SN06.2 to (I)SN07 are listed below. Follow the link associated with your configuration.

- Sun Netra t1400 to Sun Netra t1400 on page 686
- Sun Netra 240 to Sun Netra 240 one-server configuration on page 688
- Sun Netra 240 to Sun Netra 240 two-server configuration on page 690

***Note 1:*** Migrating from a Sun Netra t1400 to a Sun Netra 240 one-server or two-server configuration is not supported as part of an upgrade to (I)SN07.

***Note 2:*** Migrating from a Sun Netra 240 one-server configuration to a Sun Netra 240 two-server configuration is not supported as part of an upgrade to (I)SN07.

**ATTENTION**

The SSPFS must be at the latest maintenance release (MNCL) for the release you are currently running, and be patch-current, prior to performing the upgrade procedures.

### Sun Netra t1400 to Sun Netra t1400

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN06.2 to (I)SN07 (Sun Netra t1400 to Sun Netra t1400) Upgrade checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Upgrade the Succession Server Platform Foundation Software (SSPFS). | | Perform procedure Upgrading SSPFS software on page 698. |
| 2 | Install any SSPFS MNCLs.<br><br>***Note:*** Only perform this activity if you received a notification bulletin that an SSPFS MNCL is available for the release you just upgraded to. | | Refer to the instructions provided with the MNCL. |
| 3 | Apply any SSPFS patches. | | Perform procedure Applying patches using the NPM on page 1674. |
| 4 | Configure the CM CLLI. | | Perform procedure Setting the CS 2000 CLLI on an SSPFS-based server on page 911. |
| 5 | Upgrade the CS 2000 Management Components (CS2M) software package. | | Perform procedure Installing or upgrading the CS2M software on page 711. |
| 6 | Apply all patches to the following devices on the CS 2000 Management Tools server: PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Applying patches using the NPM on page 1674. |
| 7 | Start the SESM and SAM21EM server applications. | | Perform procedure Starting the SESM server application on page 719. |
| | | | Perform procedure Starting the SAM21 Manager server application on page 722. |

## (I)SN06.2 to (I)SN07 (Sun Netra t1400 to Sun Netra t1400) Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 8 | Stop and start the Patching Server Element (PSE) on each of the Media Gateway 9000 (MG 9000) manager servers (t1400). That is on the MG 9000 manager server, MG 9000 manager midtier, and MG 9000 manager OMCollector.<br><br>***Note:*** Only perform this activity if you have MG 9000 network elements in your network. | | Perform procedure Stopping the PSE server application on a Sun server on page 774. |
| | | | Perform procedure Starting the PSE server application on a Sun server on page 775. |
| 9 | Upgrade the Audio Provisioning Server (APS) software. | | Perform procedure Upgrading APS software on page 725. |
| 10 | Install the SAM21 platform fileset on the core manager.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Installing SAM21 Platform software on page 744. |
| 11 | Complete the CS 2000 Management Tools upgrade. | | Refer to Completing the CS 2000 Management Tools upgrade on page 1549. |

**Sun Netra 240 to Sun Netra 240 one-server configuration**
Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN06.2 to (I)SN07 (Sun Netra 240 to Sun Netra 240 one-server) Upgrade checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Upgrade the Succession Server Platform Foundation Software (SSPFS). | | Perform procedure Upgrading SSPFS software on page 698. |
| 2 | Install any SSPFS MNCLs.<br><br>***Note:*** Only perform this activity if you received a notification bulletin that an SSPFS MNCL is available for the release you just upgraded to. | | Refer to the instructions provided with the MNCL. |
| 3 | Apply any SSPFS patches. | | Perform procedure Applying patches using the NPM on page 1674. |
| 4 | Configure the CM CLLI. | | Perform procedure Setting the CS 2000 CLLI on an SSPFS-based server on page 911. |
| 5 | Upgrade the CS 2000 Management Components (CS2M) software package. | | Perform procedure Installing or upgrading the CS2M software on page 711. |
| 6 | Apply all patches to the following devices on the CS 2000 Management Tools server: PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Applying patches using the NPM on page 1674. |
| 7 | Start the SESM and SAM21EM server applications. | | Perform procedure Starting the SESM server application on page 719. |
| | | | Perform procedure Starting the SAM21 Manager server application on page 722. |

## (I)SN06.2 to (I)SN07 (Sun Netra 240 to Sun Netra 240 one-server) Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 8 | Stop and start the Patching Server Element (PSE) on each of the Media Gateway 9000 (MG 9000) manager servers (t1400). That is on the MG 9000 manager server, MG 9000 manager midtier, and MG 9000 manager OMCollector.<br><br>***Note:*** Only perform this activity if you have MG 9000 network elements in your network. | | Perform procedure Stopping the PSE server application on a Sun server on page 774. |
| | | | Perform procedure Starting the PSE server application on a Sun server on page 775. |
| 9 | Upgrade the Audio Provisioning Server (APS) software. | | Perform procedure Upgrading APS software on page 725. |
| 10 | Install the SAM21 platform fileset on the core manager.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Installing SAM21 Platform software on page 744. |
| 11 | Complete the CS 2000 Management Tools upgrade. | | Refer to Completing the CS 2000 Management Tools upgrade on page 1549. |

**Sun Netra 240 to Sun Netra 240 two-server configuration**
Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN06.2 to (I)SN07 (Sun Netra 240 to Sun Netra 240 two-server) Upgrade checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| **On the ACTIVE node** | | | |
| 1 | Obtain all patches applicable to SSPFS, PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Transferring patches to the NPM database manually on page 1664. |
| **On the INACTIVE node** | | | |
| 2 | Upgrade the Succession Server Platform Foundation Software (SSPFS). | | Perform procedure Upgrading SSPFS software on page 698. |
| 3 | Install any SSPFS MNCLs.<br><br>***Note:*** Only perform this activity if you received a notification bulletin that an SSPFS MNCL is available for the release you just upgraded to. | | Refer to the instructions provided with the MNCL. |
| 4 | Apply any SSPFS patches. | | Perform procedure Patching the inactive node of a cluster during an upgrade on page 712. |
| 5 | Configure the CM CLLI. | | Perform procedure Setting the CS 2000 CLLI on an SSPFS-based server on page 911. |
| 6 | Upgrade the CS 2000 Management Components (CS2M) software package. | | Perform procedure Installing or upgrading the CS2M software on page 711. |
| 7 | Apply all patches to the following devices on the CS 2000 Management Tools server: PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Patching the inactive node of a cluster during an upgrade on page 712. |

## (I)SN06.2 to (I)SN07 (Sun Netra 240 to Sun Netra 240 two-server) Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 8 | Stop and start the Patching Server Element (PSE) on each of the Media Gateway 9000 (MG 9000) manager servers (t1400). That is on the MG 9000 manager server, MG 9000 manager midtier, and MG 9000 manager OMCollector.<br><br>***Note:*** Only perform this activity if you have MG 9000 network elements in your network. | | Perform procedure Stopping the PSE server application on a Sun server on page 774. |
| | | | Perform procedure Starting the PSE server application on a Sun server on page 775. |
| **On the ACTIVE node** | | | |
| 9 | Stop the cluster. | | Perform procedure Stopping a cluster on page 718. |

## (I)SN06.2 to (I)SN07 (Sun Netra 240 to Sun Netra 240 two-server) Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| **On the newly ACTIVE node with (I)SN07 software** | | | |
| 10 | Upgrade the Audio Provisioning Server (APS) software.<br><br>***Note:*** Only perform this activity if APS is in your network. | | Perform procedure Upgrading APS software on page 725. |
| 11 | Install the SAM21 platform fileset on the core manager.<br><br>***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network. | | Perform procedure Installing SAM21 Platform software on page 744. |
| ***Note:*** At this point, you can easily revert this upgraded node back 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. | | | |
| 12 | Clone the image of the upgraded node onto the other node. | | Perform procedure Cloning the image of one node in a cluster to the other node on page 734. |
| 13 | Complete the CS 2000 Management Tools upgrade. | | Refer to Completing the CS 2000 Management Tools upgrade on page 1549. |

# Upgrading from (I)SN07 to (I)SN07 (maintenance release)

The configurations that support an upgrade from (I)SN07 to (I)SN07 are listed below. Follow the link associated with your configuration.

- Sun Netra t1400 to Sun Netra t1400 on page 693
- Sun Netra 240 to Sun Netra 240 one-server configuration on page 695
- Sun Netra 240 to Sun Netra 240 two-server configuration on page 696

**ATTENTION**

The SSPFS must be at the latest maintenance release (MNCL) for the release you are currently running, and be patch-current, prior to performing the upgrade procedures.

## Sun Netra t1400 to Sun Netra t1400

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN07 to (I)SN07 (Sun Netra t1400 to Sun Netra t1400) Upgrade checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Stop the SESM and SAM21EM server applications. | | Perform procedure Stopping the SESM server application on page 1877. |
| | | | Perform procedure Stopping the SAM21 Manager server application on page 1879. |
| 2 | Upgrade the CS 2000 Management Components (CS2M) software package. | | Perform procedure Installing or upgrading the CS2M software on page 711. |

## (I)SN07 to (I)SN07 (Sun Netra t1400 to Sun Netra t1400) Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 3 | Apply all patches to the following devices on the CS 2000 Management Tools server: PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Applying patches using the NPM on page 1674. |
| 4 | Start the SESM and SAM21EM server applications. | | Perform procedure Starting the SESM server application on page 719. |
| | | | Perform procedure Starting the SAM21 Manager server application on page 722. |

**Sun Netra 240 to Sun Netra 240 one-server configuration**
Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN07 to (I)SN07 (Sun Netra 240 to Sun Netra 240 one-server) Upgrade checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Stop the SESM and SAM21EM server applications. | | Perform procedure Stopping the SESM server application on page 1877. |
| | | | Perform procedure Stopping the SAM21 Manager server application on page 1879. |
| 2 | Upgrade the CS 2000 Management Components (CS2M) software package. | | Perform procedure Installing or upgrading the CS2M software on page 711. |
| 3 | Apply all patches to the following devices on the CS 2000 Management Tools server: PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Applying patches using the NPM on page 1674. |
| 4 | Start the SESM and SAM21EM server applications. | | Perform procedure Starting the SESM server application on page 719. |
| | | | Perform procedure Starting the SAM21 Manager server application on page 722. |

**Sun Netra 240 to Sun Netra 240 two-server configuration**
Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN07 to (I)SN07 (Sun Netra 240 to Sun Netra 240 two-server) Upgrade checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| **On the ACTIVE node** | | | |
| 1 | Obtain all patches applicable to PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Transferring patches to the NPM database manually on page 1664. |
| **On the INACTIVE node** | | | |
| 2 | Remove the Inactive node from the cluster. | | Perform procedure Removing a node from a cluster on page 708. |
| 3 | Upgrade the CS 2000 Management Components (CS2M) software package. | | Perform procedure Installing or upgrading the CS2M software on page 711. |
| 4 | Apply all patches to the following devices on the CS 2000 Management Tools server: PSE, SESM, SAM21 Manager, QCA, and NPM. | | Perform procedure Patching the inactive node of a cluster during an upgrade on page 712. |
| 5 | Return the upgraded node to the cluster. | | Perform procedure Returning a node to a cluster on page 715. |

## (I)SN07 to (I)SN07 (Sun Netra 240 to Sun Netra 240 two-server) Upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| **On the ACTIVE node** | | | |
| 6 | Stop the cluster. | | Perform procedure Stopping a cluster on page 718. |
| **On the newly ACTIVE node with (I)SN07 maintenance release software** | | | |
| ***Note:*** At this point, you can easily revert this upgraded node back 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. | | | |
| 7 | Clone the image of the upgraded node onto the other node. | | Perform procedure Cloning the image of one node in a cluster to the other node on page 734. |

# Upgrading SSPFS software

## Application

Use this procedure to upgrade the SSPFS software on a Sun server to the (I)SN07 release. Depending on your system, your upgrade paths are as follows:

- Sun Netra t1400 from (I)SN05, (I)SN06, or (I)SN06.2 to (I)SN07
- Sun Netra 240 from (I)SN06 or (I)SN06.2 to (I)SN07

## Prerequisites

This procedure has the following prerequisites:

- Ensure you have SSPFS Disk 1 and SSPFS Disk 2 for the (I)SN07 release.
- Ensure that none of the user-defined group identifications (GIDs) and user identifications (UIDs) conflict with the GIDs and UIDs that the SSPFS requires during the upgrade. If required, refer to procedure Verifying group IDs and user IDs on an SSPFS-based server on page 259.
- Ensure the site spec book is available with IP addresses, hostnames, and non-system logins.

**ATTENTION**

SSPFS does not have a rollback command, therefore, ensure you have backed up your Oracle data and file systems before proceeding with this procedure (see Preparing to upgrade the CS 2000 Management Tools software on page 240 for procedures.) Returning to a previous version of your system, requires that you install the previous version of SSPFS software and restore the Oracle data and file systems using the backups (see Downgrading the CS 2000 Management Tools software on page 1842 for procedures).

## Action

Perform the following steps to complete this procedure.

***At the Sun server console***

**1** Log in to the Sun server through the console (port A) using the root user ID and password.

***At the Sun server***

**2** Insert “SSPFS Disk 1” into the CD ROM drive.

***At the Sun server console***

**3** Run the pre-upgrade script by typing

```
# /cdrom/cdrom0/s0/pre_upgrade
```

and pressing the Enter key.

The pre-upgrade script prepares the server for the upgrade, and begins the upgrade of the Sun Solaris operating system.

**4** When prompted, confirm you want to continue with the installation by typing

```
# yes
```

and pressing the Enter key.

***Note:*** Entering yes confirms that the disk will be mirrored from the new OS.

**5** At the ok prompt, boot the system in single-user mode by typing

```
OK> boot -s
```

and pressing the Enter key.

**6** When prompted, enter the root password. Do not press Ctrl-D.

**7** Mount the drive using the command that corresponds to your system

Sun Netra t1400

```
# mount -F hsfs /dev/dsk/c0t6d0s0 /cdrom
```

and pressing the Enter key

Sun Netra 240

```
# mount -F hsfs /dev/dsk/c0t0d0s0 /cdrom
```

and pressing the Enter key.

**8** Start the upgrade process by typing

```
# /cdrom/upgrade
```

and pressing the Enter key.

***Note 1:*** The execution of this step takes approximately 120 minutes to complete depending on the system configuration. However, during this time, the server is fully functional and applications can be used.

***Note 2:*** During the upgrade of SSPFS, the system will attempt to apply many operating system patches. However, the patch set used was developed for upgrading from many possible earlier SSPFS releases, therefore you may see some patch installation failures, which is an expected and normal behavior.

***Note 3:*** An exception error about stopping NTSocks may be generated. Should this exception error be generated, you can ignore it and safely continue with the upgrade.

Once the upgrade completes, the system will reboot in single-user mode, and prompt you for the root password.

**9** When prompted, enter the root password. Do not press Ctrl-D.

***At the Sun server***

**10** Remove “SSPFS Disk 1” from the cdrom drive and insert “SSPFS Disk 2” into the drive.

***At the Sun server console***

**11** Mount the drive using the command that corresponds to your system

Sun Netra t1400

```
# mount -F hsfs /dev/dsk/c0t6d0s0 /cdrom
```

and pressing the Enter key

Sun Netra 240

```
# mount -F hsfs /dev/dsk/c0t0d0s0 /cdrom
```

and pressing the Enter key.

**12** Start the upgrade process by typing

```
# /cdrom/upgrade
```

and pressing the Enter key.

***Note 1:*** The execution of this step takes approximately 90 minutes to complete depending on the system configuration.

***Note 2:*** You can ignore any “rpcbind” errors.

**13** Once the system has rebooted, log in, then eject “SSPFS Disk 2” by typing

```
# eject cdrom
```

and pressing the Enter key.

**14** Verify that your system is running the version of the SSPFS by typing

```
# echo $SSPFS_VERSION
```

and pressing the Enter key.

***Note:*** The command is case sensitive.

**15**



**CAUTION**

Do not reboot the system under any circumstance until disk mirroring is complete, which takes approximately 90 minutes. If you reboot prior to disk mirroring completing, the following error is displayed:

```
Boot device: disk0:b File and args:
Not a valid ELF file
The file just loaded does not appear to
be executable.
```

To resolve this error, at the “OK” prompt, enter the command “boot disk1:b”, then wait 90 minutes or until metastat d2 returns that the mirror is no longer synchronizing.

You have completed this procedure.

# Setting up the BootP file on SSPFS

## Application

Use this procedure to set up the Succession Server Platform Foundation Software (SSPFS) platform as the bootp master and migrate the bootp entries from the core manager to the SSPFS platform.

***Note:*** Only perform this procedure if the CS 2000 SAM21 Manager is in your network.

## Prerequisites

This procedure has the following prerequisites:

- the OpenSSH fileset on the core manager must be APPLIED

  ***Note:*** You can verify whether the OpenSSH fileset is APPLIED using command “sdmmtc details” at the core manager. If it is not applied, refer to procedure “Installing or upgrading OpenSSH” in document Upgrading the CS 2000 Core Manager, NN10060-461.

- you need the password for the root user on the core manager (SDM)
- you need the IP address of the core manager (SDM)

  ***Note:*** You can obtain the IP address of the core manager (SDM) using command “sdmmtc eth” at the core manager. Use the IP address associated with the host name of the core manager, which is the first one.

**ATTENTION**

Do not begin this procedure until the SSPFS software has been upgraded to the new release. If required, refer to procedure Upgrading SSPFS software on page 698 in this document.

## 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 hostname 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** 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** Configure the IP address of the core manager (SDM) as follows:

**a** Enter the number that corresponds 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 -
```

**b** Enter the number that corresponds to the “OAMP Application Configuration” option in the menu.

*Example response*

```
OAMP Application Configuration
 1 - sdm_conf (Configure SDM IP Address)
 2 - sdm_unconf (Unconfigure SDM IP Address)
 3 - cmClli_conf (Configure CM_CLLI Address)
 4 - cmClli_unconf (Unconfigure CM_CLLI IP
     Address)
 5 - cm_conf (Configure CM IP Address)
 6 - cm_unconf (Unconfigure CM IP Address)

 X - exit

select -
```

**c** Enter the number that corresponds to the “sdm_conf” option in the menu.

**d** When prompted, enter the IP address and root user ID for the core manager (SDM).

*Example response*

```
SDM IP: 47.152.34.56
SDM User Name: root

Enter “ok” to accept current settings
```

**e** When prompted, confirm the current settings by typing

**ok**

and pressing the Enter key.

**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** For the SAM21 Manager user, generate the ssh key pair needed for data transmission between the SAM21 Manager and the CS 2000 Core Manager by typing

```
# keygen.sh sam21em
```

and pressing the Enter key.

*Example response*

```
Generating public/private rsa key pair.
Enter file in which to save the key
(/export/home/sam21em/.ssh/id_rsa):
```

**9** When prompted, press the Enter key to accept the default location and filename “/export/home/sam21em/.ssh/id_rsa” for the key.

***Note 1:*** If the default location and filename is not provided, enter “/export/home/sam21em/.ssh/id_rsa”.

***Note 2:*** If the location and filename “/export/home/sam21em/.ssh/id_rsa” already exists and you wish to overwrite, type **y** and press the Enter key. Otherwise, type **n**.

*Example response*

```
Your identification has been saved in
/export/home/sam21em/.ssh/id_rsa.
Your public key has been saved in
/export/home/sam21em/.ssh/id_rsa.pub.
The key fingerprint is:
21:cb:c6:7f:df:05:f8:4a:2f:23:e9:09:c8:37
bc:le sam21em@znc0s0j6

The authenticity of host ‘47.142.128.16
(47.142.128.16)’ can’t be established. RSA key
fingerprint is
21:cb:c6:7f:df:05:f8:4a:2f:23:e9:09:c8:37
bc:le sam21em@znc0s0j6
Are you sure you want to continue connecting
(yes/no)?
```

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

```
# yes
```

and pressing the Enter key.

*Example response:*

```
Warning: Permanently added '47.142.128.16'
(RSA) to the list of known hosts.
root@47.142.128.16's password:
```

**11** When prompted, enter the password for the SDM root user.

**12** When prompted, enter the password for the SDM root user again.

*Example response:*

```
Successfully performed bootptab manipulation
Synchronizing files IF clustered node
```

Once complete, the SAM21 Manager application will have access to the needed directories and files on the core manager.

**13** You have completed this procedure.

# Removing a node from a cluster

## Application

Use this procedure to remove a node from a cluster.

**ATTENTION**
Only perform this procedure when directed to do so.

## Prerequisites

You need the root user ID and password.

## Action

Perform the following steps to complete this procedure.

***At your workstation***

1. Telnet to the Inactive server in the cluster by typing

   ```
   > telnet <server>
   ```

   and pressing the Enter key.

   where

   **server**
   is the IP address or host name of the Inactive server 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** 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 “Cluster Configuration” option in the menu.

*Example response*

```
Cluster Configuration
 1 - join_cluster (Enable Failover - Join
     Cluster)
 2 - evict_cluster (Disable Failover - Evict
     Cluster)
 3 - failover_cluster (Invoke Cluster Failover)


 X - exit

select -
```

**8** Enter the number next to the “evict_cluster” option in the menu.

**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** You have completed this procedure.

# Installing or upgrading the CS2M software

## Application

Use this procedure to install or upgrade the CS 2000 Management Components (CS2M) software on the CS 2000 Management Tools server.

## Prerequisites

Ensure you have the CD that contains the CS2M software for the release you are installing or upgrading to.

## Action

Perform the following steps to complete this procedure.

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

**1** Insert the CD that contains the CS2M software into the CD-ROM drive of the CS 2000 Management Tools server.

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

**2** Log in to the CS 2000 Management Tools server through the console (port A) using the root user ID and password.

**3** Upgrade or install the CS2M software by typing

```
# /cdrom/cdrom0/bin/appl_mgr.ksh
```

and pressing the Enter key.

**4** When prompted, confirm you want to upgrade or install by typing

```
# y
```

***Note 1:*** The upgrade or installation takes approximately 10 minutes to complete.

***Note 2:*** During a (I)SN06.2 to (I)SN07 upgrade in a two-server configuration, if the system output indicates “ERROR executing pkgrm on NTsesm”, you can ignore the error.

**5** Eject the CD from the drive by typing

```
# eject cdrom
```

and pressing the Enter key.

**6** You have completed this procedure.

# Patching the inactive node of a cluster during an upgrade

## Application

Use this procedure to patch the inactive node of a cluster during an upgrade. A cluster refers to a Sun Netra 240 server pair.

**ATTENTION**
Only use this procedure when directed to do so.

## Prerequisites

This procedure has the following prerequisites:

- The patches have already been transferred to the NPM database. Either contact your network administrator to determine if this has already been done, or transfer them now on the Active node. If required, refer to procedure Transferring patches to the NPM database manually on page 1664 to transfer the patches to the NPM database.
- You have a valid user ID and password for the NPM host.

## Action

Perform the following steps to complete this procedure.

***At your workstation***

**1** Telnet to the inactive node of the cluster by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**
is the IP address or host name of the inactive node

**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** Patch the inactive node by typing

```
$ patchUpToDate
```

and pressing the Enter key.

*Example response:*

```
According to the current PSE configuration,
<hostname> is the NPM host.
   Is this correct? [yes]
```

**6** Press the Enter key to confirm the hostname that is displayed.

*Example response:*

```
Please enter a userid for a user on the NPM host
<hostname>. This must be a userid for which you
know the password.
```

**7** When prompted, enter the user ID for a user on the NPM host <hostname>.

*Example response:*

```
Please enter the password for <userid> on
<hostname>:
```

**8** When prompted, enter the password associated with the user ID.

*Example response:*

```
Obtaining the list of devices that can be
patched.

Obtaining patches from <hostname>. This may take
several minutes.

The following patches are about to be applied:
 PSE:
   KAA00O07
   KAA01O07
   KAA02O07

Do you wish to have these patches applied? [yes]
```

***Note:*** Only non-obsolete patches with all prerequisites available will be applied. Any patches that have already been applied or applied and removed, will not be applied again.

**9** Press the Enter key to confirm you want the patches applied.

***Note:*** Entering “no” causes processing to stop.

*Example response:*

```
PSE [1 of 1]: There are 3 patches to be applied.
    Applying KAA00O07 [1 of 3] to PSE.
    Applying KAA01O07 [2 of 3] to PSE.
    Applying KAA02O07 [3 of 3] to PSE.

The report, patchUpToDate.report, has been
produced.

Determining whether any devices need to be
restarted
```

***Note:*** The report that is produced, contains a summary of the patching actions that occurred, and any errors. This summary includes patches applied, any patches that were already applied when the patchUpToDate utility started, any patches that had been applied and removed when the patchUpToDate utility started, and any patches that were not applied because their prerequisite patches were not available.

**10** If prompted, confirm you want a restart to occur on each of the listed devices.

***Note:*** A restart enables the patches on the device. Entering “no” causes processing to continue without doing the restart.

**11** If prompted, confirm you want a system reboot to occur.

***Note:*** Entering “no” causes processing to continue without doing the system reboot.

**12** You have completed this procedure.

# Returning a node to a cluster

## Application

Use this procedure to return a node to a cluster.

**ATTENTION**
Only perform this procedure when directed to do so.

## Prerequisites

None

## Action

Perform the following steps to complete this procedure.

***At your workstation***

1 Telnet to the Inactive server in the cluster by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**
is the IP address or host name of the Inactive server 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** 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 “Cluster Configuration” option in the menu.

*Example response*

```
NTP Configuration
 1 - join_cluster (Enable Failover - Join
     Cluster)
 2 - evict_cluster (Disable Failover - Evict
     Cluster)
 3 - failover_cluster (Invoke Cluster Failover)


 X - exit

select -
```

**8** Enter the number next to the “join_cluster” option in the menu.

**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** You have completed this procedure.

# Stopping a cluster

## Application

Use this procedure to stop a cluster. A cluster refers to a Sun Netra 240 server pair.

**ATTENTION**
Only use this procedure when directed to do so from another procedure.

## Prerequisites

You must perform this procedure on the active node.

## Action

Perform the following steps to complete this procedure.

***At the active node console***

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

2 Stop the cluster by typing

```
# StopCluster
```

and pressing the Enter key.

Stopping a cluster causes the standby (inactive) server to take over and start providing OAM&P services as the new active server.

***Note:*** The high-availability (HA) cluster takes approximately 5 minutes to failover and bring up the standby node to Active state.

3 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.

# Upgrading APS software

## Application

Use this procedure to upgrade the APS software from release APS07 ((I)SN05), APS08 ((I)SN06), or APS08_2 ((I)SN06.2) to release APS09 ((I)SN07) on the CS 2000 Management Tools server.

**ATTENTION**
Only perform this procedure if you are upgrading from (I)SN05, (I)SN06, or (I)SN06.2 to (I)SN07 where APS is on the same server as the CS 2000 Management Tools.

## Prerequisites

This procedure has the following prerequisites:

- Ensure you performed a backup of APS audio files and APS oracle data using the applicable procedures listed below.
  - — Performing a backup of APS audio files to tape - Sun t1400 on page 289 , which applies to a Sun t1400 server with a DAT drive.
  - — Performing a backup of APS audio files to CD/DVD - Sun Netra 240 on page 291, which applies to a Sun Netra 240 server with a CD/DVD drive
  - — Performing a backup of APS oracle data to tape on page 293, which applies to a Sun t1400 server with a DAT drive.
  - — Performing a backup of APS oracle data to CD or DVD on page 295, which applies to a Sun Netra 240 server with a CD/DVD drive
- Ensure you have the CD that contains the APS and IPS database software required for an upgrade to release APS09 ((I)SN07).

## Action

***At the server console***

**1** Log in to the server through the console (port A) using the root user ID and password.

***Note:*** In a two-server configuration, you must upgrade APS software on the active node.

**2** Uninstall the current APS software as follows:

**a** List the APS software package and any patches that have been applied by typing

```
# pkginfo | grep aps
```

and pressing the Enter key.

| If | Do |
|---|---|
| patches display and you are running APS07 ((I)SN05) | step b |
| patches display and you are running APS08 ((I)SN06) or APS08.2 ((I)SN06.2) | step c |
| no patches display | step d |

**b** Prepare to remove the patches that were displayed by typing

```
# touch /etc/rc3.d/S80aps
```

and pressing the Enter key.

**c** Remove the patches that were displayed by typing

***Note:*** Remove the APS patches in the reverse order of their installation. For example, if patches were installed in the order of A, B, C, remove them in the order of C, B, A.

```
# pkgrm NTaps<aps_release>P<#>
```

and pressing the Enter key.

where

**aps_release**
is 07, 08, or 08.2.

**#**
is an APS patch number.

Repeat this command for each patch listed in the previous step.

**d** Remove the APS software as follows:

**i** Remove the NORTips package by typing

```
# pkgrm NORTips
```

and pressing the Enter key.

*Example response*

```
The following package is currently
installed:
NORTips    IPS08_2-25.0 DB Package which
           goes into /usr/ntdb/aps08_2.
             (sparc) 1.0

Do you want to remove this package?
```

When prompted, indicate you want to remove the NORTips package by typing

**y**

and pressing the Enter key.

*Example response*

```
## Removing installed package instance
<NORTips>

This package contains scripts which will be
executed with super-user permission during
the process of removing this package.

Do you want to continue with the removal of
this package [y, n,?, q]
```

When prompted, indicate you want to continue with the removal of the package by typing

**y**

and pressing the Enter key.

ii Remove the NTaps package by typing

```
# pkgrm NTaps<aps_release>
```

and pressing the Enter key.

where

**aps_release**
is 07, 08 or 8.2

*Example response*

```
The following package is currently
installed:
NTaps082   APS08_2-25.0 Package -
            /opt/uas/aps. April 16, 2004.
             (sparc) 1.0

Do you want to remove this package?
```

When prompted, indicate you want to remove the NTaps package by typing

**y**

and pressing the Enter key.

*Example response*

```
## Removing installed package instance
<NTaps082>

This package contains scripts which will be
executed with super-user permission during
the process of removing this package.

Do you want to continue with the removal of
this package [y, n,?, q]
```

When prompted, indicate you want to continue with the removal of the package by typing

**y**

and pressing the Enter key.

**e** Ensure the APS software package and any patches have been removed by typing

```
# pkginfo | grep aps
```

and pressing the Enter key.

There should be no output for this command.

**3** Install the APS09 software as follows:

**a** Insert the APS09 CD into the CD-ROM drive.

**b** Wait approximately 30 seconds for the server to auto mount the CD drive.

**c** Verify you can see the CD-ROM drive listed in the mounted drive list by typing

```
# df
```

and pressing the Enter key.

**d** Copy the contents on the CD to the root directory by typing

```
# cp /cdrom/cdrom0/* /
```

and pressing the Enter key.

**e** Verify the loads got copied by typing

```
# ls -l /NTaps09* NORTips*
```

and pressing the Enter key.

You should see two loads listed.

**f** Install the APS09 software package by typing

```
# pkgadd -d NTaps09-<xx>.pkg
```

and pressing the Enter key.

where

**xx**
is the APS loadbuild number

*Example response*

```
The following packages are available:

1 NTaps09   APS09-20.0 Package -
  /opt/uas/aps. June 2, 2004
  (sparc) 1.0
Select package(s) you wish to process (or
'all' to process all packages). (default:all)
[?,??,q]:
```

When prompted, indicate you want to install all packages by typing

**all**

and pressing the Enter key.

*Example response:*

```
Processing package instance <NTaps09> from
</NTaps09-20.0.pkg> (sparc) 1.0
## Processing package information.
## Processing system information.
   8 package pathnames are already properly
   installed.
## Verifying disk space requirements.
## Checking for conflicts with packages
   already installed.
The following files are already installed on
the system and are being used by another
package:
* /opt/uas/uas_conf_backup
* - conflict with a file which does not belong
to any package.
Do you want to install these conflicting
files [y,n,?,q]
```

| If the system | Do |
|---|---|
| prompts you about installing conflicting files | substep g |
| does not prompt you about installing conflicting files | substep i |

**g** Indicate you do not want to install these conflicting files by typing

**n**

and pressing the Enter key.

*Example response:*

```
Do you want to continue with the installation
of <NTaps09> [y, n,?, q]
```

**h** When prompted, indicate you want to continue with the installation by typing

**y**

and pressing the Enter key.

```
Installing APS10-20.0 Package - /opt/uas/aps.
June 2, 2004 as <NTaps09>
```

**i** Install the IPS software package by typing:

**# pkgadd -d NORTips09-<xx>.pkg**

and pressing the Enter key.

where

**xx**
is the APS loadbuild number

**j** When prompted, indicate you want to install all packages by typing

**all**

and pressing the Enter key.

| If the system | Do |
|---|---|
| prompts you about installing conflicting files | substep k |
| does not prompt you about installing conflicting files | substep m |

**k** Indicate you do not want to install these conflicting files by typing

**n**

and pressing the Enter key.

**l** When prompted, confirm you want to continue with the installation by typing

**y**

and pressing the Enter key.

**m** When prompted, confirm you want to continue with the installation by typing

**y**

and pressing the Enter key.

**n** Run the installation script by typing

```
# ./start.sh 2>&1 | tee /startinstall.log
```

and pressing the Enter key.

***Note:*** The installation can take approximately 60 minutes to complete. This is a safe stopping point in the procedure.

**o** Check the /apsinst.log for application install errors by typing

```
# cat /apsinst.log |more
```

and pressing the Enter key.

**p** Re-source your login shell as follows:

```
# cd /
```

and pressing the Enter key.

```
# ./etc/profile
```

and pressing the Enter key.

```
# . ./.profile
```

and pressing the Enter key.

***Note:*** Ensure there is a space between the two first periods (.) in the last command.

**4** Eject the APS09 CD from the CD-ROM drive as follows:

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

```
# cd /
```

and pressing the Enter key.

**b** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

**5** Delete the previous NTaps and NORTips packages if they are still present under the root (/) directory.

6 Verify the database, web server, web services, and the APS are up and running by typing

```
# servman query -status all
```

and pressing the Enter key.

*Example response:*

```
APP NAME                STATUS
=========               ======
OMPUSH                  RUNNING
DATABASE                RUNNING
CINOTIFIER              RUNNING
SESMService             RUNNING
WEBSERVICES             RUNNING
APS                     RUNNING
ORA_AUTO_BACKUP         RUNNING
DELEGATE                RUNNING
BOOTP                   RUNNING
ORA_ARCHIVE_ROTATOR     RUNNING
WEBSERVER               RUNNING
```

7 Configure the SNMP agent. If required, refer to procedure Configuring the SNMP agent on page 1591.

***Note:*** The APS SNMP is not running at the end of the APS upgrade.

8 At this point, only the admin user is active. Add other users to the security server and back into the APS database as follows:

**a** Access the APS login page and login as ‘admin’, ‘admin’. If required, refer to procedure “Logging in to the APS GUI” in the Media Server 2000 Security and Administration document, NN10337-611.

**b** Perform procedure “Listing users” in the Media Server 2000 Configuration Management document, NN10340-511, to list the users who can be added.

**c** Perform procedure “Creating users” in the Media Server 2000 Configuration Management document, NN10340-511, to add the users back into the APS GUI using remote security authentication.

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.

# Migrating the CS 2000 SAM21 Manager data

## Application

Use this procedure to migrate the CS 2000 SAM21 Manager data from the core manager to the CS 2000 Management Tools server.

**ATTENTION**
Rollback after this point requires that you perform procedure Performing a rollback of the CS 2000 SAM21 Manager on page 1856 in this document.

## Prerequisites

Procedure Preparing for the CS 2000 SAM21 Manager data migration on page 297 was completed prior to the upgrade.

## 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 hostname 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 Migrate the SAM21 Manager data from the core manager to the CS 2000 Management Tools server by typing

```
# /opt/nortel/sam21em/bin/migration/sam21emMigration.sh
```

and pressing the Enter key.

This script imports backup data from the core manager using scp, and populates the SAM21EM database.

*Example response*

```
SAM21 Element Manager Server Persistent Data Migration
================================================
Transferring data from 47.142.128.16 (SDM IP configured or
SSPFS).
Checking if persistent data already exists...
Secure copying sam21emMigration.tar from SDM
sam21emMigration.tar 100%
|**************************************************
10240                00:00
Retrieving Oracle SAM21 EM Password...
Extracting persistence.
Processing file: /tmp/scusql1.txt
Log file for /tmp/scusql1.txt available at:
/tmp/scusql1.txt.log
Attempting to reserve physical and logical IPs
based on SAM21 EM provisioned card data.
Successfully reserved IP addresses from provisioned card
data.
SAM21 Element Manager persistent data successfully migrate
```

**6** You have completed this procedure.

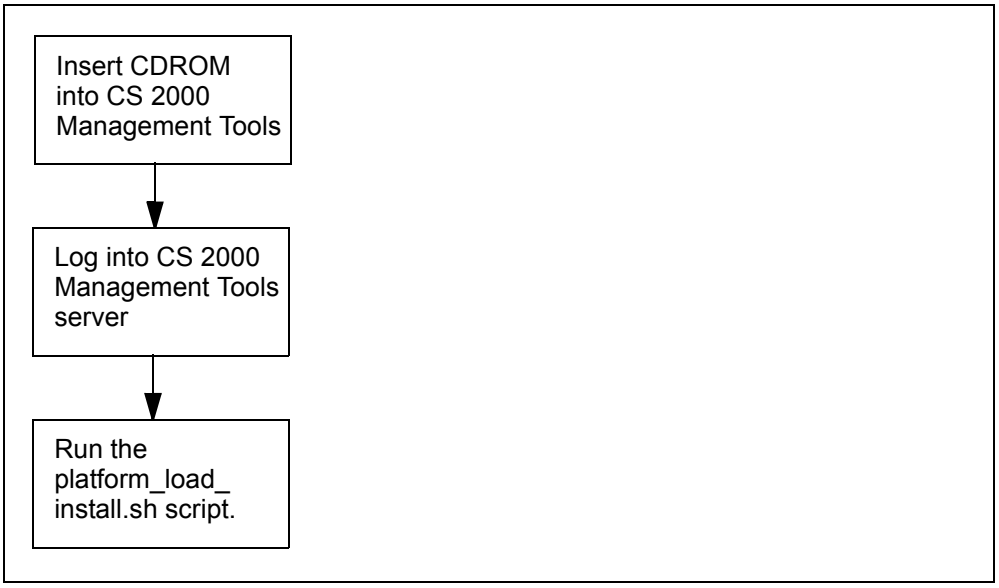
# Installing SAM21 Platform software

This procedure installs the SAM21 Shelf Controller software on the CS 2000 Core Manager or Core and Billing Manager 850 (CBM) so that the CS 2000 Core Manager or CBM can serve the software to a BOOTP request from a SAM21 Shelf Controller.

If this is an SN05 to SN07 upgrade, before performing this procedure, upgrade the CS 2000 SAM21 Manager server software on the CS 2000 Core Manager and install the CS 2000 SAM21 Manager package on the CS 2000 Management Tools server. These procedures are described in *IP Solutions Upgrade*, NN10344-450 or *ATM Solutions Upgrade*, NN10261-450.

Do not remove old SAM21 Shelf Controller filesets (NCL and MNCL filesets of the same release) from the CS 2000 Core Manager unless there is not enough disk space in the `/swd/sam21` volume on the CS 2000 Core Manager to apply new releases. If required, follow the procedure listed in section Old fileset removal on CS 2000 Core Manager on page 748. Use procedure Old fileset removal on CBM on page 750 for removing old .rpm packages.

The following figure summarizes the procedure.



***At the CS 2000 Management Tools frame (Sun Microsystems t1400 or Netra 240)***

**1** Insert the CDROM into the CDROM tray. If the unit is a Netra 240 in a cluster configuration, use the active Netra 240 unit. The active unit is identified by a lit USER LED on the front of the unit.

The CDROM label for the SAM21 Shelf Controller software includes the product code, SAM20007, on the lower half of the label.

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

**2** Log in and then use the su command to gain root privilege.

```
Trying <hostname>...
Connected to <hostname>.
Escape character is '^]'.

Authorized use only, activities logged.
login: username
Password: <password>
Last login: Fri Jan 30 12:48:10 from <otherhost>
prompt:>
prompt:> su - root
Password: <root_password>
#
```

**3** Execute the platform_load_install.sh script.

```
# /opt/nortel/sspfs/Scripts/platform_load_install.sh
```

*The screen clears and a menu is displayed.*

```
      Welcome to the Platform Installation Tool Version 3.2
   ========================================================================
      RPM INSTALLATION/REMOVAL
     ============================
     1) Install RPM from CDROM       2) Install RPM from Disk
     3) Uninstall RPM                4) Query all RPMs

      OTHER
     =========
    C) Change Rotation Parameters          P) View Rotation Parameters
     V) SAM21 Platform Version Installed     X) Exit

      Please choose one of the following: 1
```

***Note:*** *Options C and P are not available for offices configured with a CS 2000 Core Manager or a CBM.*

**4** Enter **1** and press the Return key to install the software.

*The screen clears and the contents of the .rpm package are displayed.*

```
                Verifying CDROM is mounted
/cdrom/cdrom on /vol/dev/dsk/c0t0d0/cdrom read only/nosuid/mapl-
case/noglobal/rr/traildot/dev=16c0001 on Sat Mar 27 16:34:13 2004
                CDROM is mounted.
                Listing file names in the rpm on the cd.

/swd/sam21/10.0.0.0401211453
/swd/sam21/10.0.0.0401211453.cksum
/swd/sam21/F695_flash.10.0.0.0401211453
/swd/sam21/F695_flash.10.0.0.0401211453.chksum
/swd/sam21/N765.flash.10.0.0.0401211453
/swd/sam21/N765a.flash.10.0.0.0401211453
/swd/sam21/Sitka.flash.10.0.0.0401211453
/swd/sam21/checkLoad
/swd/sam21/hostsmodify
/swd/sam21/hostsmodify.sh
/swd/sam21/hostsmodify.sspfs
/swd/sam21/logs/logfile
/swd/sam21/logs/slgcleansam
/swd/sam21/sc-atm-tools.rpm
/swd/sam21/sc-ip-tools.rpm
/swd/sam21/sc-mtc-tools.rpm

                Do you want to continue (y/n)? Y
```

***Note:*** *If the message* `There is no cd in the CDROM drive, please check drive` *is displayed, ensure that the CDROM is inserted in the tray for this unit.*

**5** Enter **Y** to proceed with the software installation.

*The software is extracted from the .rpm package. The .rpm package is transferred to the CS 2000 Core Manager or CBM.*

```
              Extracting files from the rpm archive on the cd.

Installing RPM package SAM21_PLAT-10.0-223.0
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
sam21_plat_10_0_223_0.rpm                   100%   11MB 750.4KB/s   00:14
root@47.135.214.127's password: <enter root password>
```

**6** Enter the root password for the CS 2000 Core Manager or the CBM.

*The software is installed on the CS 2000 Core Manager or CBM. If a CBM is used, the .rpm package is then copied to the inactive CBM unit and another prompt for the root password appears. If this happens enter the root password and press Return. After the load file is installed on the CS 2000 Core Manager or CBM, the transferred .rpm package is deleted from the CS 2000 Core Manager or CBM.*

```
              Extracting files from the rpm archive on the cd.

Installing RPM package SAM21_PLAT-10.0-223.0
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
sam21_plat_10_0_223_0.rpm                   100%   11MB 750.4KB/s   00:14
root@47.135.214.127's password: <enter root password>
Mate IP is 47.135.214.129
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
root@47.135.214.129's password: <enter root password>

     Configuring syslog to add designlog, statlog and customerlog files.
      Log files already added to syslog.

      Adding log rotation for designlog/statlog/customerlog files.
      Installation of Platform Load Complete.

      ******* Please hit ENTER key to continue ***********
```

***Note:*** *After the first installation, syslog and log rotation will not be reconfigured.*

**7** Enter **X** to exit.

**8** Enter the eject command:

```
# eject
```

9 Log out of the CS 2000 Management Tools server.

***At the CS 2000 Management Tools frame***

10 Remove the CDROM.

11 This procedure is complete.

***Note:*** For customers experienced with upgrading the SAM21 Shelf Controllers in earlier releases, no action is required at the CS 2000 Core Manager for software installation.

## Additional information

Do not use file links (hard or soft symbolic links) in the filesystem for bootloads. Links are not supported, they defeat the caching mechanism, and increase the time required to boot a SAM21 Shelf Controller.

## Old fileset removal on CS 2000 Core Manager

Do not remove old SAM21 Shelf Controller fileset (NCL and MNCL filesets of the same release) unless there is not enough disk space in the `/swd/sam21` volume to apply new releases.

To remove old SAM21 Shelf Controller filesets, perform the following procedure.

***At the Core Manager console or terminal window***

1 Change directory to `/var/adm/sam21`:

```
# cd /var/adm/sam21
```

2 Copy the custlog, designlog, and statlog configuration files to a backup version in the `/var/adm` directory:

```
# cp custlog ../custlog.bak
# cp designlog ../designlog.bak
# cp statlog ../statlog.bak
```

3 List the existing filesets:

```
# sdmmtc details
```

4 Find the SAM21 Shelf Controller fileset to be removed by using the filter command:

```
> filter sam21
```

### Filter command example

```
    SDM        CON      NET      APPL     SYS            CLLI: clliname
     .          .        .        .        .             Host: hostname

Details
 0 Quit      Filter: SAM21 (Description View)
 2             # Fileset Description                Version         Status
 3             1 SAM21 Platform v10                10.0.117.0      APPLIED
 4             2 SAM21 Platform v7                 7.0.558.4       APPLIED
 5             3                                >> 7.0.558.0       ARCHIVED
 6             4 SAM21 Platform v8                 8.0.24.9        APPLIED
 7 Select      5                                >> 8.0.24.0        ARCHIVED
 8 Remove      6 SAM21 Platform v9                 9.0.66.5        APPLIED
 9             7                                >> 9.0.66.0        ARCHIVED
10             8 Succession SAM21 Manager          8.0.24.2        APPLIED
11                                        Filesets: 1 to 8 of 8
```

**5** Remove the old SAM21 Shelf Controller fileset:

**> remove <#>**

**#**
is the number for the “SAM21 Platform” fileset to remove. For example, **remove 3** to remove version 7.0.558.0.

**6** Make the `/var/adm/sam21` directory:

```
# mkdir -p /var/adm/sam21
```

**7** Change directory to `/var/adm`, the location of the backup configuration files:

```
# cd /var/adm
```

**8** Move the backup configuration files into the `/var/adm/sam21` directory, and remove the backup suffix:

```
# mv custlog.bak sam21/custlog
# mv designlog.bak sam21/designlog
# mv statlog.bak sam21/statlog
```

**9** The current SAM21 Shelf Controller NCL and MNCL filesets need to be reapplied.

To reapply the filesets, use Installing SAM21 Platform software on page 744 in this document.

## Old fileset removal on CBM

Do not remove old SAM21 Shelf Controller fileset (NCL and MNCL filesets of the same release) unless there is not enough disk space in the `/swd/sam21` volume to apply new releases.

***At the CS 2000 Management Tools terminal***

**1** Log in as root and then run the platform_load_install.sh script.

*The screen clears and a menu is displayed.*

```
      Welcome to the Platform Installation Tool Version 3.2
=====================================================================
      RPM INSTALLATION/REMOVAL
     ============================
     1) Install RPM from CDROM       2) Install RPM from Disk
     3) Uninstall RPM                4) Query all RPMs

      OTHER
     =========
    C) Change Rotation Parameters          P) View Rotation Parameters
     V) SAM21 Platform Version Installed     X) Exit

      Please choose one of the following: 3
```

**2** Select **3** and press the Return key.

*The application connects to the CS 2000 Core Manager or CBM and displays the installed .rpm packages.*

```
           Uninstalling RPM Software.

           The Following RPM files are installed

3PC_MC_SSPFS-7.09-1.0
SAM21_PLAT-10.0-223.0
         Please enter rpm file you would like to uninstall or q to exit>
```

**3** Enter the name of the .rpm package to remove. For example, SAM21_PLAT-10.0-223.0.

***Note:*** The .rpm package name is case sensitive.

*A confirmation prompt is provided.*

```
      Please enter rpm file you would like to uninstall or q to exit>
SAM21_PLAT-10.0-223.0
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
     Are you sure you want to uninstall SAM21_PLAT-10.0-223.0 (y,n)>? Y
```

**4** Enter **Y** to confirm the uninstall prompt.

*The uninstall begins, and stops to prompt for the root password on the CS 2000 Core Manager or CBM. If the office uses a CBM, a second root password prompt is provided for the mate CBM unit.*

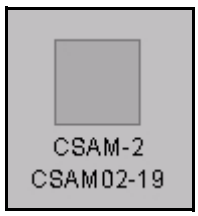
```
      Uninstalling RPM on SDM/CBM, you will be prompted for the sdm/cbm
root passwd.
root@47.135.214.127's password: <enter root password>
Mate IP is 47.135.214.129
root@47.135.214.129's password: <enter root password>
       SAM21_PLAT-10.0-223.0 RPM has been uninstalled


               ******* Please hit ENTER key to continue ***********
```

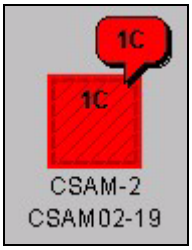
**5** This procedure is complete.

# Upgrading software on the SAM21 Shelf Controller

If this is an SN05 software upgrade to SN07, the shelf icon will appear isolated.




Not isolated




Isolated

**ATTENTION**

*The information in this attention box only applies to an SN05 to SN07 software upgrade.*

Ensure that the IP address provisioned in the SAM21 EM Server field of the Reprovision window is the call processing LAN interface on the CS 2000 Core Manager before beginning this procedure. This change must be made on the CS 2000 SAM21 Manager client hosted by the CS 2000 Core Manager and the CS 2000 SAM21 Manager client on the CS 2000 Management Tools server. If this IP address is not set to the call processing LAN interface prior to loading and Swact of the SAM21 Shelf Controllers to the new SN07 load, the CS 2000 SAM21 Manager server looses communication with the shelf after the first Swact. Therefore, the shelf becomes isolated. Contact Nortel Networks support personnel if the shelf becomes isolated.

Monitor the progress text at the States tab as each SAM21 Shelf Controller is locked in step 5. The SAM21 Shelf Controller that is upgraded first configures the second SAM21 Shelf Controller. In order to configure the first SAM21 Shelf Controller, it must be locked and unlocked so that the second SAM21 Shelf Controller can configure it. This additional step is only performed once for each SAM21 shelf.

Before the firmware parameters for a SAM21 Shelf Controller are configured, the progress text at the States tab during a lock includes the following lines:

```
Lock started
Locking in progress
Checking if SC firmware parameters are up to date
SC firmware parameters are not up to date
Configuring SC firmware parameters
Configuring netboot parameters
Configuring environment parameters
Saving configuration
SC firmware parameters configuration completed
Lock completed successfully
```

After the firmware parameters for a SAM21 Shelf Controller are configured, the progress text at the States tab includes the following lines:

```
Lock started
Locking in progress
Checking if SC firmware parameters are up to date
SC firmware parameters are up to date
Lock completed successfully
```

Ensure that the progress text for both SAM21 Shelf Controllers includes `SC firmware parameters are up to date.`

## Client interfaces

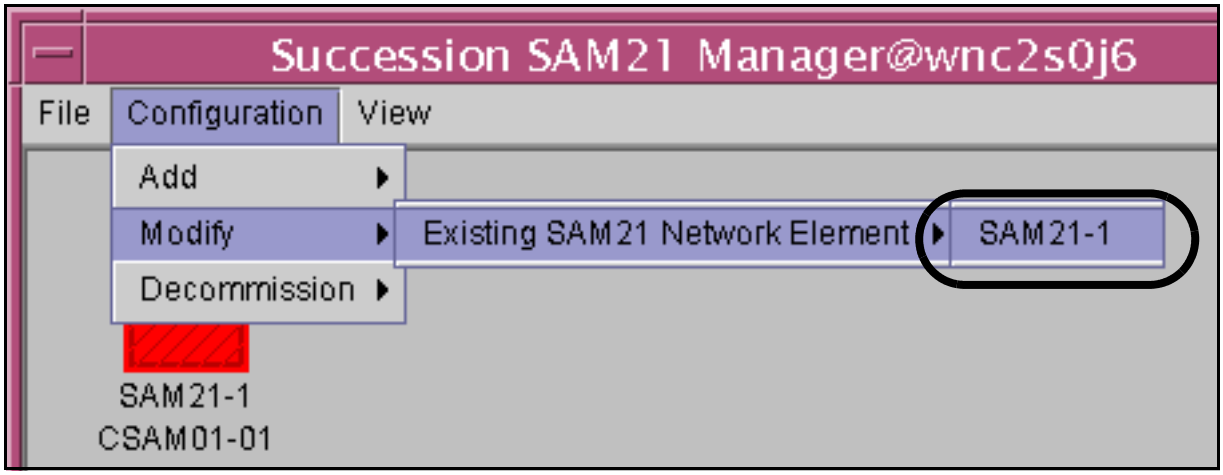
For the upgrade from SN05 to SN07, two versions of the CS 2000 SAM21 Manager client are used. Use the Java Web Start client hosted by the CS 2000 Management Tools server to reprovision the software load in steps 1, 2, and 3. Use the client hosted by the CS 2000 Core Manager and started with the **/sdm/bin/sam21gui** to lock and unlock the SAM21 Shelf Controllers as well as for SWACT in steps 5 through 11.

## Detailed procedure

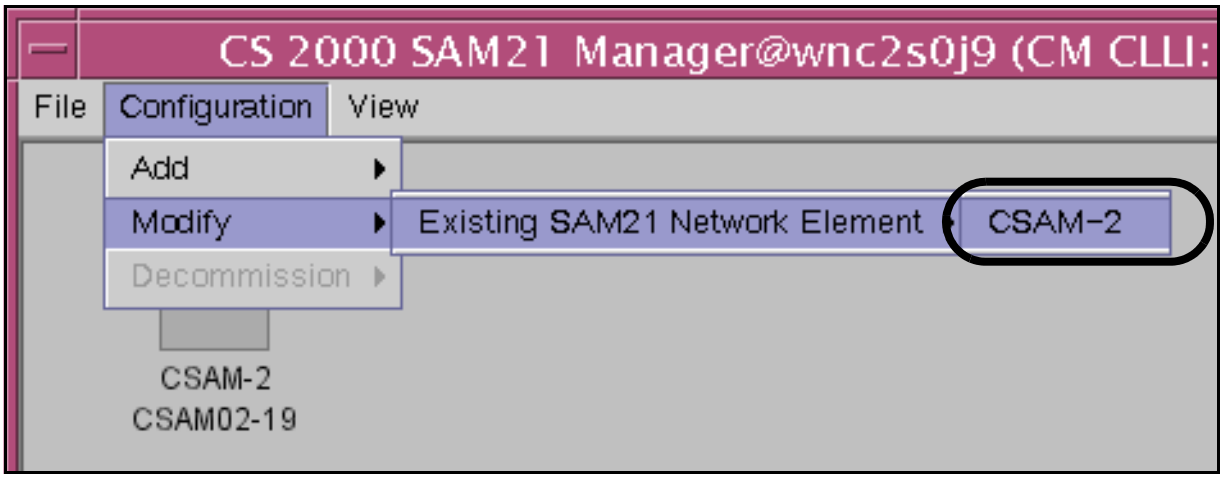
***At the CS 2000 SAM21 Manager client (Java Web Start client)***

**1** From the Subnet View, select Configuration, Modify and then the SAM21 shelf with the SAM21 Shelf Controllers to upgrade.

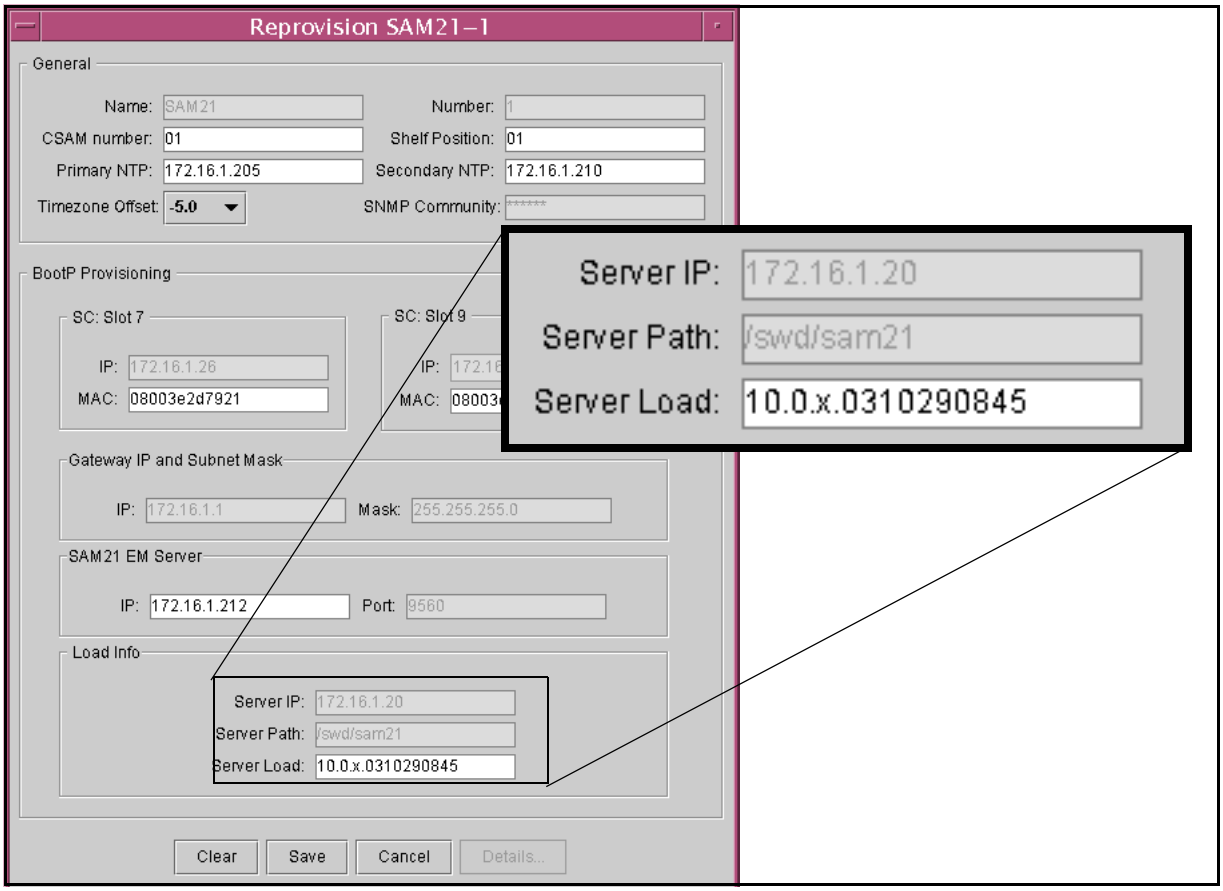
**Upgrade from SN05 to SN07**




**Upgrade from SN06 to SN07 or newer**



2 Enter the new software load name in the Server Load field on the Reprovision window. This action updates /etc/bootptab on the CS 2000 Core Manager. A warning is generated if the provisioning fails.



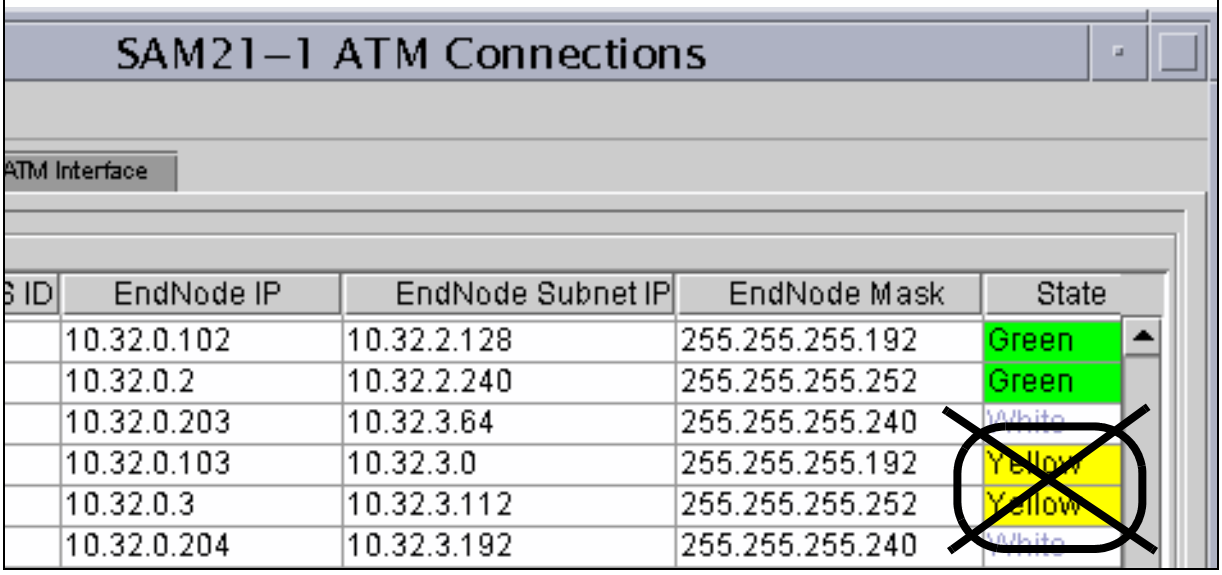

***Note 1:*** ‘ x’ is greater than or equal to zero. Refer to page 1-1 of the *SAM21 Platform Base Release Notes* for the correct value.

***Note 2:*** This graphic shows the SN06 to SN07 upgrade. For SN05 to SN07 upgrades, the Primary NTP, Secondary NTP, and Timezone Offset fields are not available. During these same upgrades, the IP address, MAC addresses, Gateway IP address, SAM21 EM Server IP, Server IP, and Server Path fields are available.

3 Click Save on the Reprovisioning window to save the data. Close the Reprovisioning window.

4 If the SAM21 Shelf Controllers are provisioned with ATM interfaces, verify that the inactive SAM21 Shelf Controller does not carry the active ATM link. Select Configuration and then IPOA Services from the Subnet View to open the ATM Connections window.

Green - active ATM link is on active SAM21 Shelf Controller
Yellow - active ATM link is on inactive SAM21 Shelf Controller
Red - connection between SAM21 Shelf Controller and end node existed but is currently broken
White - connection between SAM21 Shelf Controller and end node is provisioned, but never connected




If all the connections are yellow, then SWACT the SAM21 Shelf Controller at a period of low activity before proceeding. If some connections are green and some are yellow, as in the example, then check for alarms at the ATM equipment between the SAM21 Shelf Controller and the end node with the yellow connection. Correct the condition, check again that all connections are green, and then proceed.

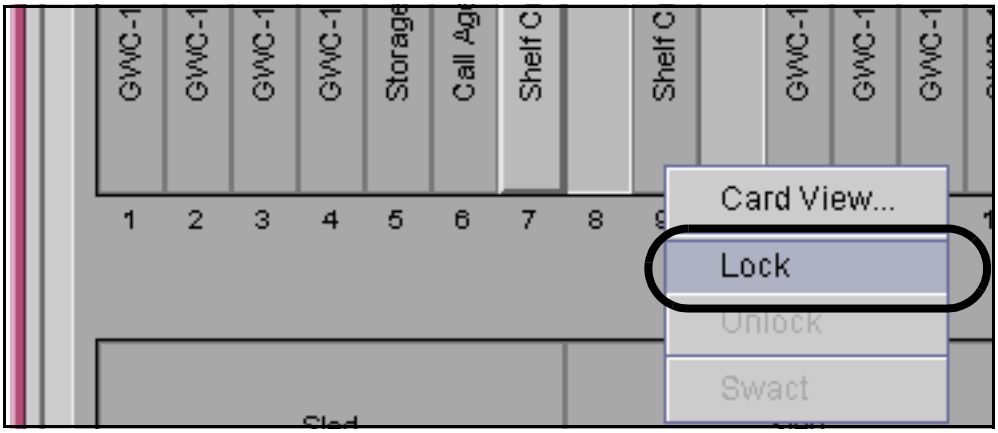
**5**

**ATTENTION**

If this is an SN05 to SN07 upgrade, perform steps 5 through 11 from the client that is hosted by the CS 2000 Core Manager and is started with the `/sdm/bin/sam21gui` command.

From the Shelf View window, right click on the card icon for the inactive SAM21 Shelf Controller and select Lock from the context menu.

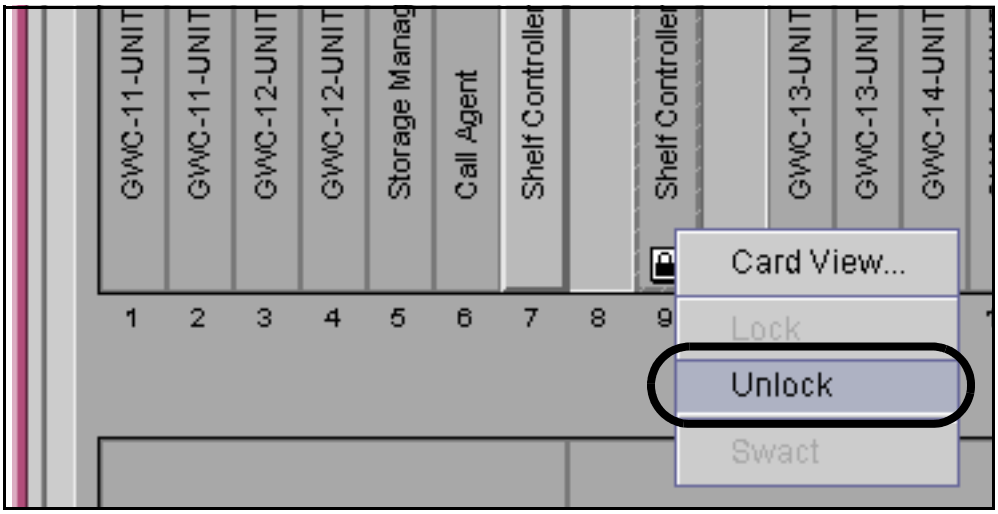
***Note:*** The Lock menu option is only available for the inactive SAM21 Shelf Controller.




**6** Wait for the Lock icon to appear on the SAM21 Shelf Controller icon and the other SAM21 Shelf Controller to indicate that it is in simplex (alarm 2C on the other SAM21 Shelf Controller).

***Note:*** If the CS LAN is provided by Nortel Networks Passport 8000 series router switches, reprovision the port on the Passport to auto-negotiate. Refer to Reprovision Passport port to auto-negotiate on page 760. This only needs to be done once. If this procedure was completed during the upgrade to SN06, do not reconfigure the port.

7 Right click on the same SAM21 Shelf Controller and select Unlock from the context menu and optionally verify that calls can originate and complete. The unlock request can require up to 10 minutes.




***Note:*** Optionally monitor the download and boot of the card from the States tab of the Card View window. If the card does not boot or if the *SAM21 Base Platform Release Notes* indicates that upgraded firmware is included in the load, refer to procedure SAM21 Shelf Controller does not unlock on page 1895 for information about configuring firmware parameters.

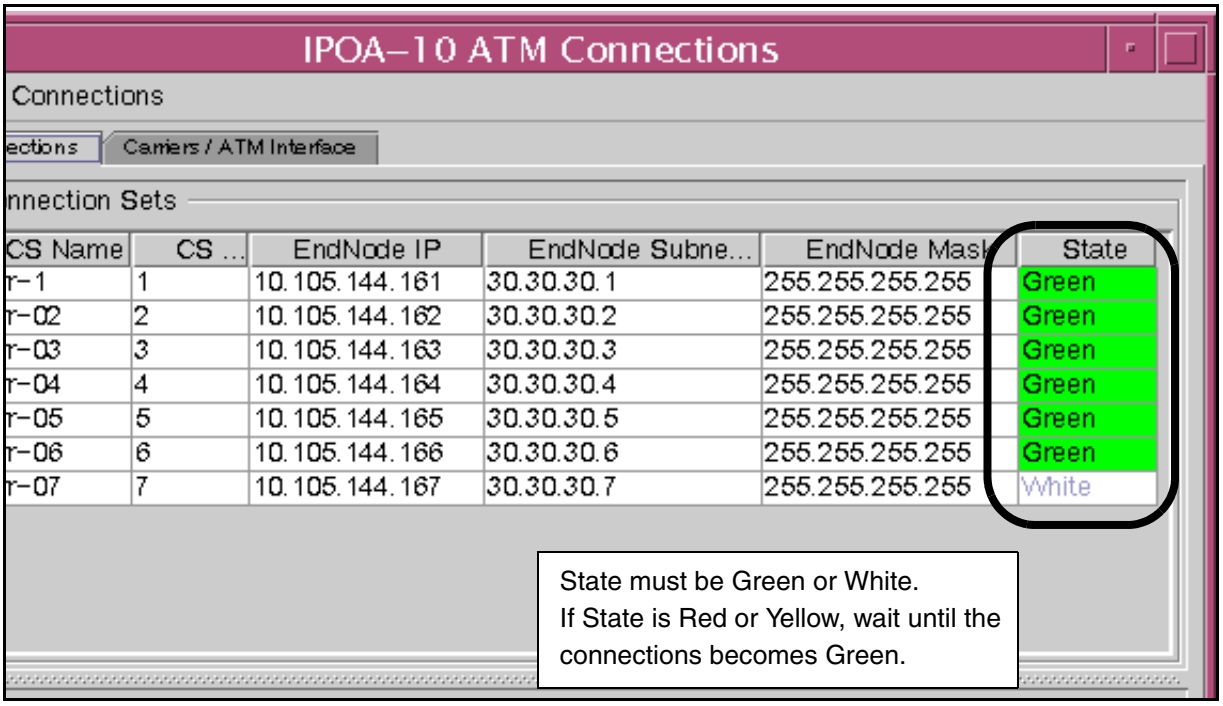
A successful boot reports the following message at the States tab of the Card View window:

```
Unlock started
Establishing control
Waiting for board to initialize
Unlock in progress
Waiting for SC to boot
SC is booting...
Unlock completed successfully
```

8 If required by operating company personnel, soak the new software load. If rollback to the previous release is required, refer to Rollback software on the SAM21 Shelf Controller on page 1853.

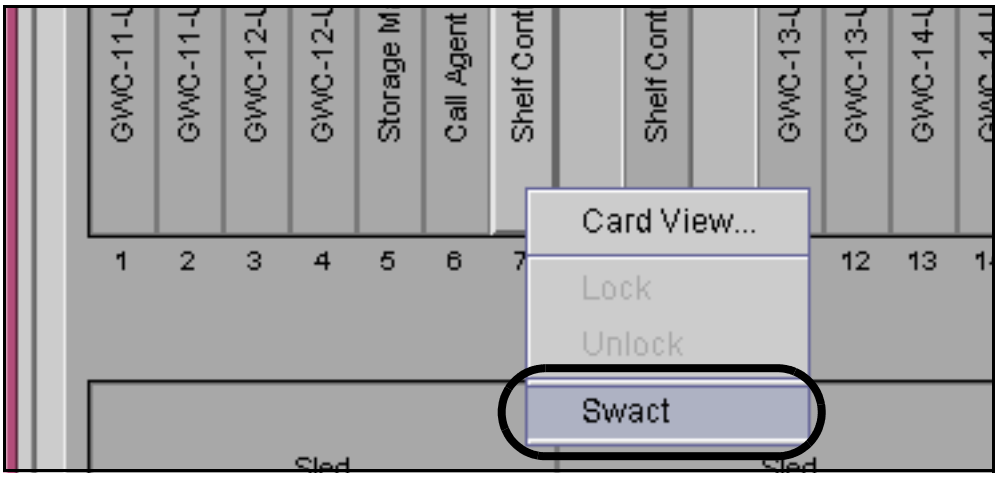
**9** If the SAM21 Shelf Controller is configured with an ATM interface, verify that all ATM connections are green at the ATM Connections window before proceeding.

**Check for Green state**




**10** After the hashed outline disappears from the Inactive SAM21 Shelf Controller, right click on the icon for the Active SAM21 Shelf Controller and select Swact from the context menu.

If required by telephone operating company personnel, soak the new software and firmware after the Swact.



**11**

**ATTENTION**
Rollback is not supported after this step is completed.

Lock and unlock the newly Inactive card as in steps 5 and 7. If firmware configuration was required with the first card, perform the firmware configuration on the newly inactive card.

**12** If this is an SN05 to SN07 upgrade, Swact the SAM21 Shelf Controllers again, and then Lock and Unlock the SAM21 Shelf Controller that was upgraded first. This step ensures that the firmware parameters are configured correctly. Monitor the progress text at the States tab as the SAM21 Shelf Controller boots.

**13** This procedure is complete.

## Reprovision Passport port to auto-negotiate

To enable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Passport router switch. Read, write, and administrative privileges are required for this procedure.

### *At the CLI for the Passport*

**1** Determine the slot and port on the Passport that connects to the device:

```
> show ip arp info <ip_address>
```

**ip_address**
is the physical IP address of the SAM21 Shelf Controller, the Gateway Controller, or USP

*The slot and port are reported.*

```
prompt:cpu> show ip arp info 172.30.242.25
================================================================================
                                      Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL
--------------------------------------------------------------------------------
172.30.242.25    00:90:69:1a:d4:fc   200   1/2   DYNAMIC 272
```

***Note:*** *If the response indicates MLT instead of the slot and port, perform this operation from the mate Passport unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.*

**2** Set the slot and port to auto-negotiate:

**`> config ethernet <slot>/<port> auto-negotiate enable`**

*The slot and port are reconfigured to auto-negotiate and the prompt returns.*

```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

**3** Verify the port configuration:

**`> show ports info config <slot>/<port>`**

*The slot and port configuration is displayed.*

```
prompt:cpu> show ports config info 1/2

================================================================================
                                      Port Config
================================================================================

PORT              AUTO  SFFD  ADMIN       OPERATE     DIFF-SERV  QOS MLT
NUM   TYPE        NEG.        DUPLX SPD   DUPLX SPD   EN   TYPE  LVL ID
--------------------------------------------------------------------------------
1/2   100BaseTX   true  false  half  100   full  100   fals  core  1   0
```

**4** Commit the change:

**`> save config`**

# Migrating the SAM21 network elements to the CS 2000 SAM21 Manager on the CS 2000 Management Tools server

## Application

Use this procedure to migrate each provisioned SAM21network element (NE) from the CS 2000 SAM21 Manager on the core manager, to the CS 2000 SAM21 Manager on the CS 2000 Management Tools server.

**ATTENTION**
This procedure requests that you reprovision each SAM21 NE using the CS 2000 SAM21 Manager client on the CS 2000 Management Tools server and the CS 2000 SAM21 Manager client on the core manager. It is important that you reprovision each SAM21 NE from both clients.

**ATTENTION**
It is important that you reprovision the SAM21 NEs from the CS 2000 SAM21 Manager on the CS 2000 Management Tools server first to avoid isolating the SAM21 NEs.

## Prerequisites

None

## Action

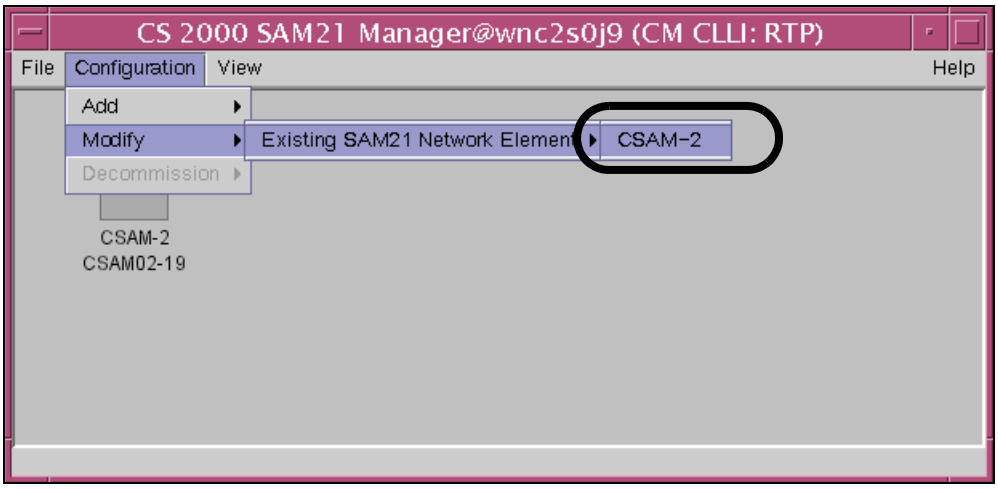
**Launch the CS 2000 SAM21 Manager client on the CS 2000 Management Tools server**

***At your workstation***

1 Launch the SAM21 Manager client application that resides on the CS 2000 Management Tools server. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

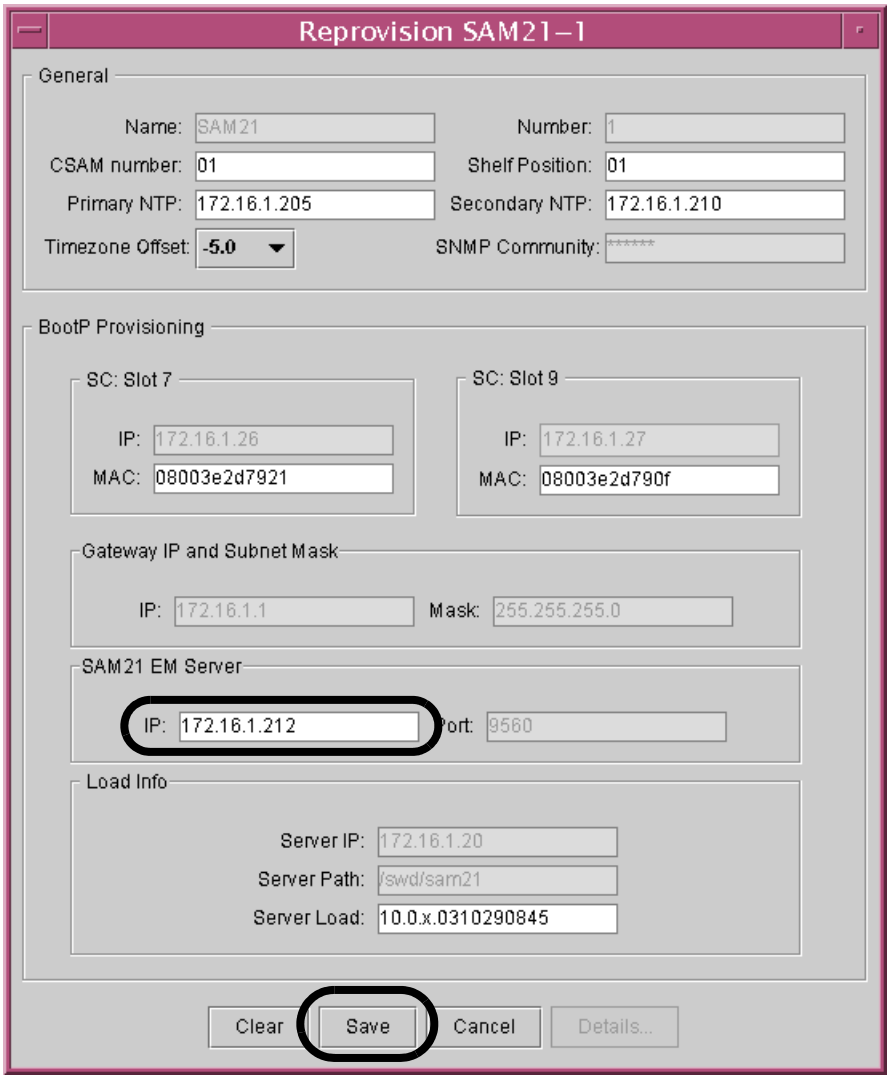
**2** Reprovision each SAM21 network element (NE) as follows:

**a** Use the Configuration menu to modify a SAM21 NE.




The Reprovision window for the SAM21 NE you selected, opens.

**b** Replace the existing IP address with the IP address of the CS 2000 Management Tools server, and click Save.




At this point, the CS 2000 Management Tools server bootp has updated the core manager bootp with the SAM21 Manager server IP address change. However, the CS 2000 SAM21 NEs are still communicating with the CS 2000 SAM21 Manager on the core manager.

## Launch the CS 2000 SAM21 Manager client on the core manager

***At the client workstation***

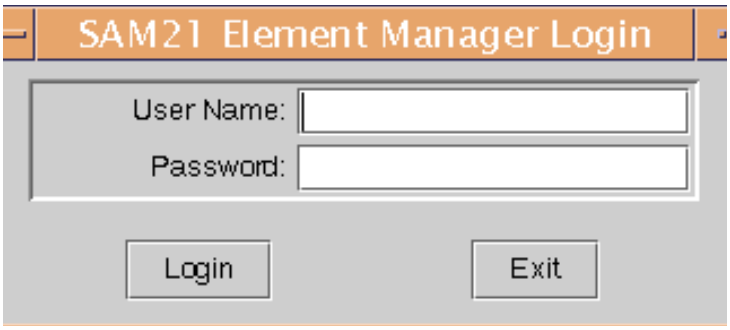
**3** Log on to the client workstation using the correct user ID and password. Do not log on as the root user.

**4** Launch the SAM21 Manager client application that resides on the core manager by typing

```
# /sdm/bin/sam21gui
```

and pressing the Enter key.

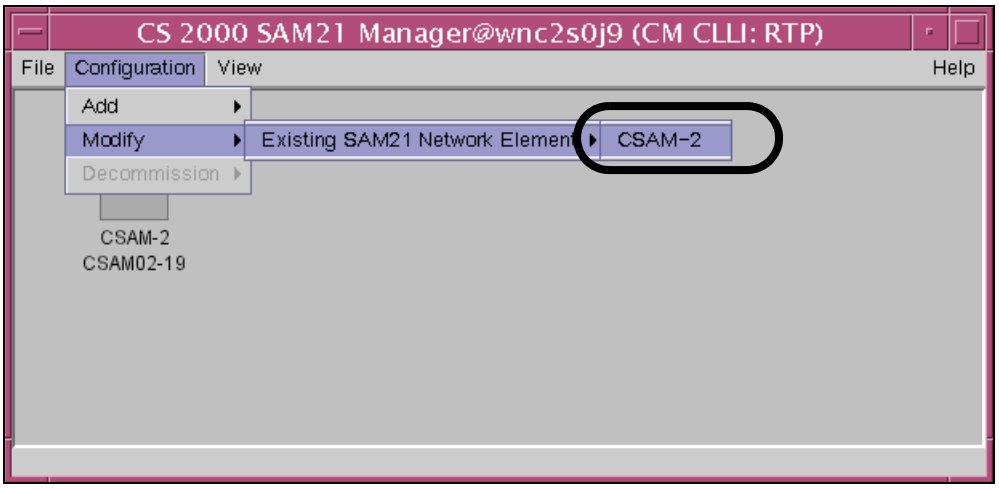
The user authentication window appears.




**5** Enter a valid user name and password, and click **Login**.

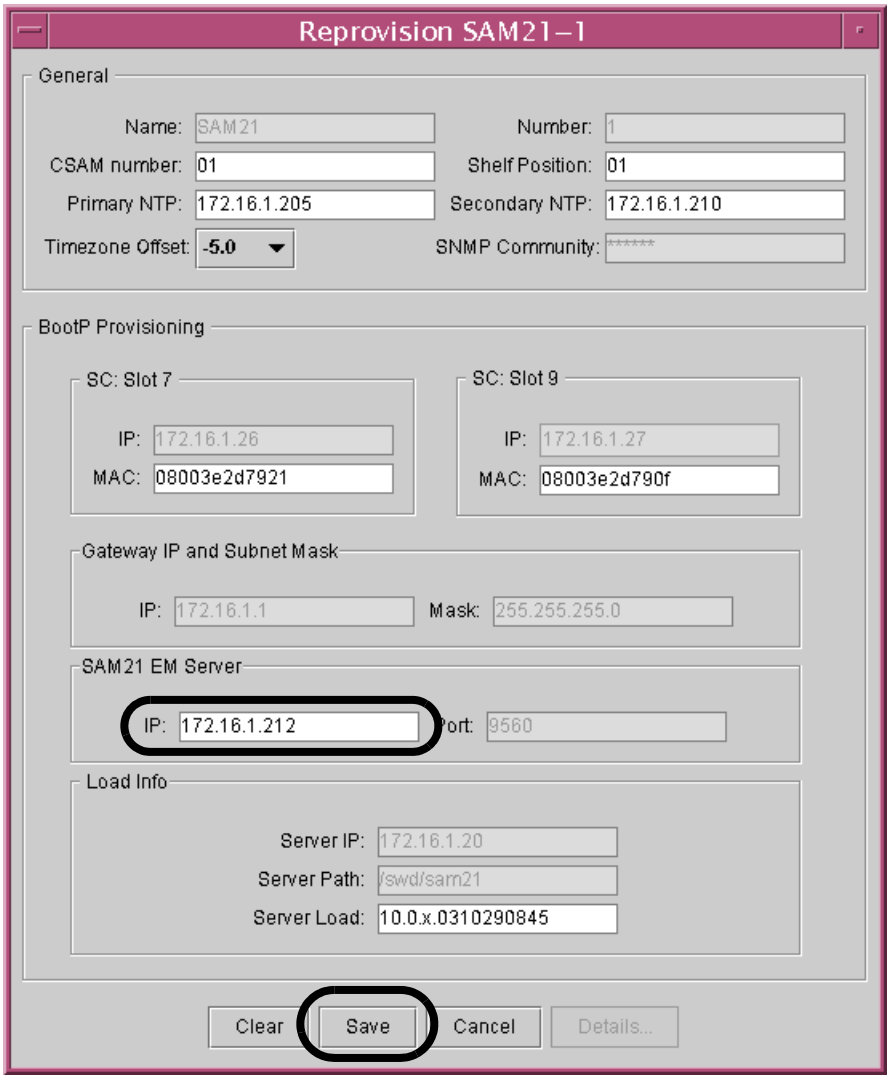
**6** Reprovision each SAM21 network element (NE) as follows:

**a** Use the Configuration menu to modify a SAM21 NE.




The Reprovision window for the SAM21NE you selected, opens.

**b** Replace the existing IP address with the IP address of the CS 2000 Management Tools server, and click Save.




An SNMP message is sent to both SAM21 NEs with the IP and port of the CS 2000 Management Tools server. Within approximately 1 minute, the node recovers from isolation on the CS 2000 SAM21 Manager that resides on the CS 2000 Management Tools server. Within approximately 2 minutes, the node will be isolated on the CS 2000 SAM21 Manager that resides on the core manager.

7 Decommission the isolated shelf. Refer to procedure “Deprovision a SAM21 shelf” in the SAM21 Shelf Controller Configuration Management document, NN10111-511, if required.

Persistent storage for the shelf is removed.

***Note:*** The bootp entries on the core manager are not removed by the CS 2000 SAM21 Manager.

8 Remove the CS 2000 SAM21 Manager from the client workstation as follows:

**a** Log on to the client workstation using the root user ID and password.

**b** Remove the contents of the “/sdm” directory by typing

```
# rm -r /sdm/snm
```

and pressing the Enter key.

```
# rm -r /sdm/bin
```

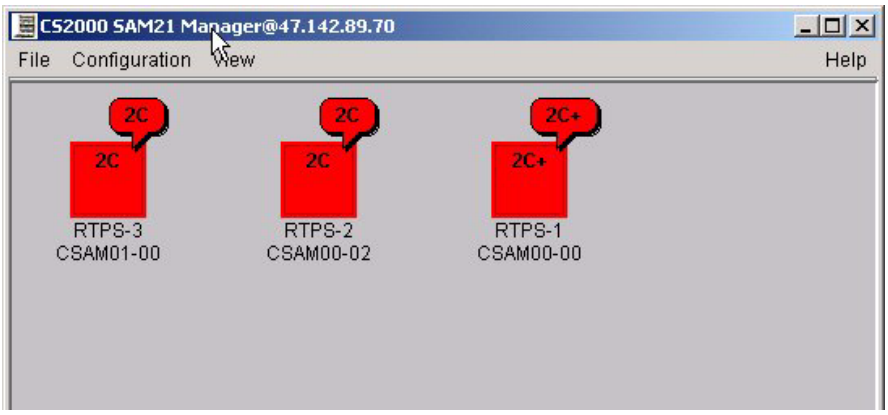
and pressing the Enter key.

***At the CS 2000 SAM21 Manager client on the CS 2000 Management Tools server***

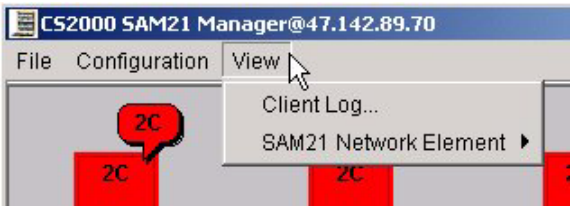
9 Verify that all SAM21 network elements are communicating with the CS 2000 SAM21 Manager on the CS 2000 Management Tools server as follows:

**a** Launch the SAM21 Manager client application that resides on the CS 2000 Management Tools server if not already available. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

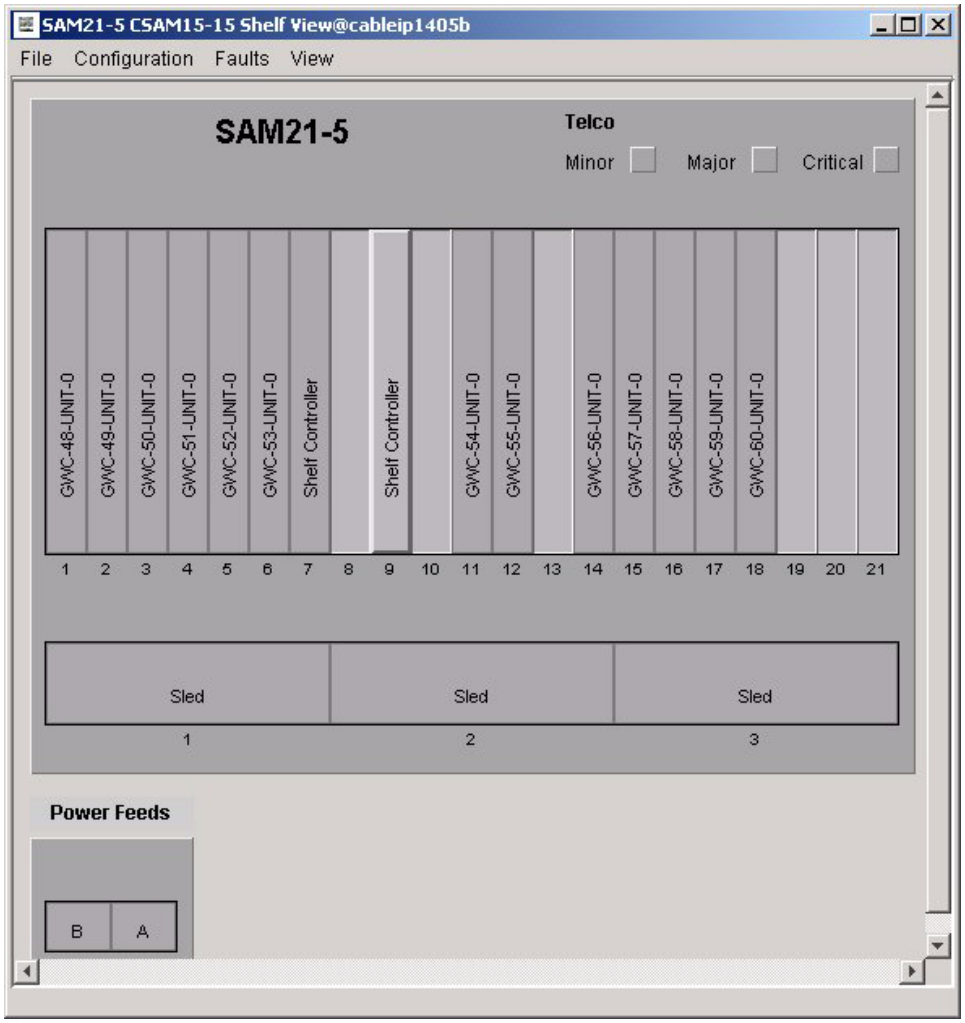
When you launch the CS2000 SAM21 Manager, the subnet view, similar to the following, is displayed.




**b** On the **View** menu, select **SAM21 Network Element**, and then select the first SAM21 network element in the list, or double click on the icon of the first SAM21 network element in the subnet display.




The shelf view of the SAM21 network element, similar to the following, is displayed.




**c** Repeat substep b to display the shelf view of each SAM21 network element.

| If you | Do |
|---|---|
| cannot display the shelf view of the SAM21 network elements | substep d |
| can display the shelf view of the SAM21 network elements | you have completed this procedure |

**d** Ensure you performed each step in this procedure. Contact support if necessary.

**10** You have completed this procedure.

# Completing the CS 2000 SAM21 Manager migration

## Application

Use this procedure to run the SAM21 EM post-migration script and remove the Succession SAM21 Manager fileset from the core manager.

**ATTENTION**
Rollback after this point requires that you boot the core manager from the backup tape to rollback to the CS 2000 SAM21 Manager on the core manager.

## Prerequisites

**ATTENTION**
Ensure you completed all the steps in procedure Migrating the SAM21 network elements to the CS 2000 SAM21 Manager on the CS 2000 Management Tools server on page 762 in this document.

You need the root user ID and password for the core manager.

## Action

***At the core manager console***

1 Log on to the core manager using the root user ID and password.

2 Busy the CS 2000 SAM21 Manager as follows:

**a** Access the application level of the maintenance interface by typing

```
# sdmmtc appl
```

and pressing the Enter key.

**b** Busy the CS 2000 SAM21 Manager by typing

> **bsy <#>**

and pressing the Enter key.

*Where:*

**<#>**
is the number next to the Succession SAM21 Manager fileset

**c** Confirm the busy command by typing

> **y**

and pressing the Enter key.

The CS 2000 SAM21 Manager client application on the core manager shuts down after the busy command.

**d** Exit the maintenance interface by typing

> **quit all**

and pressing the Enter key.

**3**

**ATTENTION**

This step deletes all persistent data for the CS 2000 SAM21 Manager in sdm/configdata/snm/persistence. Ensure you successfully migrated the data to the CS 2000 Management Tools server and reprovisioned all the SAM21 network elements to communicate with the CS 2000 Management Tools server before you proceed.

Run the SAM21 Manager post-migration script by typing

```
# /sdm/snm/bin/sam21emPostMigration.sh
```

and pressing the Enter key.

*Example response:*

```
SAM21 Element Manager Post Migration

====================================

WARNING: This action will DELETE all persistent
data for the SAM21 Element Manager from
sdm/configdata/snm/persistence.
Please ensure you have successfully migrated the
data to the SSPFS platform and decommissioned
all nodes via the Element Manager before
proceeding.
```

***Note:*** This step applies only for upgrades from (I)SN05 to (I)SN07.

**4** Confirm the command by typing

```
# yes
```

and pressing the Enter key.

*Example response:*

```
SAM21EM post migration successful
```

**5** Remove the Succession SAM21 Manager fileset as follows:

**a** Access the SWIM level by typing

```
# sdmmtc swim
```

and pressing the Enter key.

**b** Access the Details level by typing

```
> details
```

and pressing the Enter key.

**c** Select the Succession SAM21 Manager application by typing

> **select <#>**

and pressing the Enter key.

*where*

**#**
is the number next to the Succession SAM21 Manager fileset

**d** Remove the Succession SAM21 Manager application by typing

> **remove**

and pressing the Enter key.

**e** Confirm the removal by typing

> **y**

and pressing the Enter key.

***Note:*** The remove command also removes the older version of the SAM21 platform fileset.

**f** Exit the maintenance interface by typing

> **quit all**

and pressing the Enter key.

**6** You have completed this procedure.

# Stopping the PSE server application on a Sun server

## Application

Use this procedure to stop the Patching Server Element (PSE) server application on a Sun server.

## Prerequisites

None

## 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 PSE 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** Stop the PSE server application by typing

```
# pse stop
```

and pressing the Enter key.

**6** Verify the PSE server application stopped by typing

```
# pse status
```

and pressing the Enter key.

**7** You have completed this procedure.

# Starting the PSE server application on a Sun server

## Application

Use this procedure to start the Patching Server Element (PSE) server application on a Sun server.

## Prerequisites

None

## 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 PSE 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** Start the PSE server application by typing

```
# pse start
```

and pressing the Enter key.

**6** Verify the PSE server application started by typing

```
# pse status
```

and pressing the Enter key.

**7** You have completed this procedure.

# Upgrading MG 9000 components

An MG 9000 upgrade adheres to the following order:

- Upgrading the MG 9000 Manager on page 803
- Upgrading the Gateway Controller on page 834
- Upgrading the MG 9000 on page 908

## SN06.x to SN07 t1400/N240 one-server (simplex) upgrade checklist

Use the following table as a checklist for upgrading the MG 9000 Manager and MG 9000 from SN06.x to SN07 in a t1400/N240

single-server (simplex) configuration. Enter a check mark (√) in the √ column as each step or procedure is completed.

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **1** | Upgrade the MG 9000 Manager to SN07. | 1. The following steps are part of the procedure Upgrading MG 9000 Manager software from SN06.x to SN07 on page 805. Refer to that procedure and those referenced in the following steps to complete the MG 9000 Manager upgrade.<br>a. Configure the MG 9000 Manager master server by performing procedure Configuring the MG 9000 Manager master server software on page 818.<br>b. Configure the MG 9000 Manager mid-tier server by performing procedure Configuring the MG 9000 Manager mid-tier server software on page 823.<br>c. Install the MG 9000 Manager client software<br>• For Windows PC client installation, refer to Installing the MG 9000 Manager Windows PC client software on page 825<br>• For Sun workstation client installation, refer to Installing the MG 9000 Sun client software on page 827<br>d. Provision any new users, if required. Refer to *MG 9000 Security and Administration*, NN10162-611.<br>***Note:*** Previous SN06.x users are maintained through the upgrade. | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| 1 | Upgrade the MG 9000 Manager to SN07. (continued) | e. Start the SN06.x MG 9000 Manager client. Refer to *MG 9000 MG 9000 Security and Administration*, NN10162-611.<br>f. Start the SN07 MG 9000 Manager client. Refer to *MG 9000 MG 9000 Security and Administration*, NN10162-611<br><br>***Note 1:*** During the upgrade process, when the user clicks on the SN07 link in the Application Launch Point, the SN07 application launches. At that point, the user must login. This allows the user into the SN07 application. However, when the SN06.x link is selected, a second and different login box appears, meaning the user must log in again to access the SN06.x application. This only occurs during this upgrade session.<br><br>***Note 2:*** SN06.x and SN07 can run simultaneously. | |
| | ***Note 1:*** This is a safe stopping point<br><br>***Note 2:*** This completes the Manager upgrade. Before proceeding to upgrade the MG 9000 element, complete Preparing to upgrade the Gateway Controller on page 344 and Upgrading the Gateway Controller on page 834. | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **For each network element in SN06.x** | | | |
| **2** | Ensure all MG 9000 Patch Image (9PI) load files have been copied to the CS2000 Core Manager (SDM) to support upgrade / downgrade activity from DAT tape or CD-ROM. | Refer to "*Upgrading the CS S2000 Core Manager*, NN10060-461."<br>Refer to Installing MG 9000 loads into the CS 2000 Core Manager from DAT tape on page 909 or Installing MG 9000 loads into the CS 2000 Management Tools Manager from CDROM on page 916. | |
| **3** | Provisioning a floating IP address. | Refer to Provisioning a floating IP address on page 918. | |
| **4** | Upgrade the MTA card, if equipped. | Perform the procedure Downloading software into the MTA card on page 926. | |
| **5** | Upgrade the xDSL cards, if equipped | Perform the procedure Downloading software into the xDSL card on page 928. | |
| **6** | Determine if the sync reference/ timing signal source is correct. This must be correct to prevent alarms on the DCC and ITP cards when the upgrade is complete. | If the BITS cable was connected to the DCC card BITS connector during the hardware installation, using the Local Craft Interface (LCI) access the master shelf in the network element being upgraded, and select the active ITP card. From the menu, select Clock Sync->Provisioning. Ensure the MG 9000 is synched to the correct timing source, BITS or network:<br>• ITXBITS - if syncing to the ITX card<br>• DCCBITS - if syncing to the DCC cards and the cable is connected to the DCC card BITS connector<br>• Network - if syncing to the upstream network connection<br>Refer to *MG 9000 Configuration Management*, NN10096-511. | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **7** | Perform a card upgrade in the SN06.x subnet on the following cards on the NE: all DS1s, ABIs, ITPs, ITXs, and DCCs. | Perform the procedure Upgrading the MG 9000 from SN06.x to SN07 on page 923. | |
| **8** | Determine if the DCC cards software version is at 7. | From the Frame view, click on Actions->Software Upgrades in the menu bar. From the Software Upgrades view, click on Version List. Check the version of the DCC cards or click on the frame, shelf, card to view each DCC and make sure the software version indicates 7. Both DCC cards must be at the SN07 software version.<br><br>***Note 1:*** Upgrade should not progress until both DCC card versions are SN07.<br><br>***Note 2:*** Once the MG 9000 has been upgraded to SN07, no further provisioning should occur. | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **9** | Export data to XML file.<br><br>Wait for the Export To XML File window to indicate that the export is complete. | In the SN06.x Subnet View, select the MG9000 menu and click on Export NE. From the ExportNE Contents to XML File window, select an NE and click on Export. Refer to Performing an Export NE on page 832.<br><br>Look for: Completed XML Export of NE: <ne number><br><br>***Note 1:*** After the exports are complete, tar the entire persistdata directory, located on the MG 9000 master server, and place the exported data onto another machine for vaulting purposes. The following files and directories may be present in the persistdata directory:<br>• LoadFilesPersistData.dat<br>• xml<br>• ESA_SYSTEM_SD_V1.0.DTD<br><br>***Note:*** ESA_SYSTEM_SD_V1.0.DTD is generated only for SN06.2 MG 9000 Manager data, not for the SN06 MG 9000 Manager data.<br><br>• SubnetPersistData06_2.dat<br><br>Use the following information to tar the persistdata files and directories<br><br>tar cvf <filename>.tar /data/mg9kem/persistdata<br><br>It is recommended that the filename use the following format:<br><br><date.hostname_filename>.tar<br><br>for example,<br><br>OCT23.rtpd_persistdatabackup.tar<br><br>***Note 2:*** Keep a backup copy of the SN06.x XML file in case a downgrade is required. | |
| | ***Note:*** This is a safe stopping point. | | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **10** | Remove the NE from the SN06.x OMC collection list. | Once the DCC cards are at SN07, no OMs can be collected until the NE is imported to the SN07 Subnet View.<br>1. To remove the NE from the SN06.X OMC collection list perform the following steps at the MG 9000 Manager mid-tier workstation:<br>a. To configure the OM collector, type<br>**# /opt/nortel/omcltr_06_2/bin/OMCollector config**<br>The system responds<br>`Starting OM Configuration Tool ...`<br>`**********`<br>`**********`<br>`*  Welcome to the Nortel Networks *`<br>`*`<br>`*  OM Collection Configuration Tool *`<br>`**********`<br>`**********`<br>`Please pick one of the following options:`<br>`[C]reate a new device collection list`<br>`[A]dd device(s) to the collection list`<br>`[R]emove device(s) from the collection list`<br>`[D]isplay the existing collection list`<br>`[S]how this menu again`<br>`[P]assword configuration`<br>`[H]elp menu`<br>`e[X]it`<br>`Enter your selection:`<br>b. To display the NEs the OM Collector is supporting, type<br>**> D**<br>Identify the NE to be removed from the collection list. | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| 10 | Remove the NE from the SN06.x OMC collection list. (Contd) | c. To remove the NE from the OM Collector, type **> R**<br>The system responds with:<br>`Enter IP address (X.X.X.X) or <ENTER> to end:`<br>d. Type the IP address of the NE to remove.<br>The system responds with:<br>`Enter IP address (X.X.X.X) or <ENTER> to end:`<br>***Note:*** Each NE should be removed as it is upgraded.<br>e. Press <ENTER> to end.<br>The system responds with:<br>`Deletion of device(s) is complete.`<br>`Please pick one of the following options:`<br>`[C]reate a new device collection list`<br>`[A]dd device(s) to the collection list`<br>`[R]emove device(s) from the collection list`<br>`[D]isplay the existing collection list`<br>`[S]how this menu again`<br>`[P]assword configuration`<br>`[H]elp menu`<br>`e[X]it`<br>`Enter your selection:`<br>f. To exit the tool, type X.<br>The system responds with:<br>`**********`<br>`*** OM Collection Configuration Tool is closing... **********` | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **11** | Create patched images of all MG 9000 loads | 1. After the MG 9000 cards have been upgraded to SN07 and all other MG 9000 Manager workstations have been upgraded to SN07, perform the following procedure to image the network element (NE) cards for use in upgrading the cards in other NEs.<br><br>***Note 1:*** Perform the following steps after the following conditions are met:<br>• the NPM is at SN07<br>• the suite of MG 9000 Manager servers are running SSPFS07, with both SN06.x and SN07 MG 9000 Managers are resident<br>• the old SN06.x MG 9000 Manager is not in control of the MG 9000 devices which are running SN07<br><br>***Note 2:*** The following steps will create patched images of all MG 9000 loads. This will be accomplished by upgrading, patching, and then imaging two MG 9000s (one DCC-OC3 MG 9000 and one DCC-IMA MG 9000). Ensure the NEs selected include all MG 9000 intelligent card types in the office.<br><br>First the user will upgrade all the intelligent cards on a DCC-OC3 MG 9000 using the latest available PI loads. After the upgrade, the user will patch all intelligent cards on the DCC-OC3 MG 9000 with any available patches that were not included on the PI load tape. After patching is complete, the user will take an image of the DCC-OC3 MG 9000 using the NPM.<br><br>Next, the user will upgrade a DCC-IMA MG 9000 using the PI loads just created. After the upgrade, the user will apply any available patches for any remaining intelligent card types (including the DCC-IMA) that were not patched during the DCC-OC3 MG 9000 upgrade. After patching is complete, the user will take an image of the DCC-IMA MG 9000 using the NPM.<br><br>a. Use the following to determine the next step.<br>• if there were additional patches added to the pre-patched image loadfile, go to step b<br>• if there were no additional patches added to the pre-patched image loadfile, go to stepc | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| 11 | Create patched images of all MG 9000 loads (contd) | b. Image one NE with OC3 DCC cards with SN07 patched images.<br>c. Apply remaining SN07 patches to all cards on this NE with OC3 DCC cards.<br>d. Import this NE with DCC OC3 cards to the SN07 MG 9000 Manager.<br><br>***Note:*** Make sure an audit is not in progress and is not scheduled for this NE.<br><br>Go to the SN07 Subnet View and click on the MG9000 menu and click on Import NE.<br>From the Import From XML File window, select the SN06.x import path<br><br>**/data/mg9kem/persistdata/xml/SN06/<ne_number>** for SN06,<br><br>or<br><br>**/data/mg9kem/persistdata/xml/SN06_2/<ne_number>** for SN06_2<br><br>which is to be upgraded.<br><br>Select Import. This will import and convert all the SN06.2 data which was previously exported. The NE icon will be created and a discovery/recovery process is started.<br>Refer to Performing an Import NE on page 830.<br>e. Take an image of the inactive cards on this NE with DCC-OC3. Refer to the “Performing a device image using the NPM” in *ATM Solutions Upgrade*, NN10261-450 or *IP Solutions Upgrade*, NN10344-450 for steps on performing a device image. Select SmartImage->MG9KDEVICES.<br>f. Upgrade one NE with DCC-DS1-IMA cards with the SN07 MG 9000 patched images just created in the previous step. Load all cards on this NE with the supplied image. | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| 11 | Create patched images of all MG 9000 loads (contd) | g. Import this NE with DS1-IMA DCC cards to the SN07 MG 9000 Manager.<br><br>***Note:*** Make sure an audit is not in progress and is not scheduled for this NE. Observe the Audit Tasks tab in the Frame View.<br><br>Go to the SN07 Subnet View and click on the MG9000 menu and click on Import NE.<br><br>From the Import From XML File window, select the SN06.x import path<br><br>**/data/mg9kem/persistdata/xml/SN06/<ne_number>** for SN06,<br><br>or<br><br>**/data/mg9kem/persistdata/xml/SN06_2/<ne_number>** for SN06_2<br><br>which is to be upgraded.<br><br>Select Import. This will import and convert all the SN06.2 data which was previously exported. The NE icon will be created and a discovery/recovery process is started.<br><br>Refer to Performing an Import NE on page 830.<br><br>h. Apply the remaining patches to all cards on this NE with DCC DS1-IMA cards.<br><br>i. Take an image of the inactive cards on this NE with DS1-IMA DCC cards that were not imaged in step e above. Refer to the “Performing a device image using the NPM” in *ATM Solutions Upgrade*, NN10261-450 or *IP Solutions Upgrade*, NN10344-450 for steps on performing a device image.<br><br>j. Use the images created in the previous steps to upgrade all the of the cards on all the remaining NEs to be upgraded to SN07 | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| 12 | Enable OM collection for NEs in SN07 | If this is the first NE to be upgraded, configure the OMCollector using the "Configuring OM Collector software" in *MG 9000 Performance Management*, NN10140-711.<br><br>As each NE is upgraded, OM Collection for that NE must be enabled by clicking the OMCollection checkbox in the MG 9000 Provisioning View which is accessed from Configuration->View/Modify NE Properties from the menu bar of the Subnet View for OM Collection to be enabled for an NE. For more information refer to *MG 9000 Performance Management*, NN10140-711. | |
| **13** | Delete the NE which was just upgraded. | Go to the SN06.x Subnet View. Select the NE to be deleted and from the menu bar, select Configuration->Delete NE. Click on Apply, OK as needed and exit.<br><br>Refer to the "Deleting an MG 9000 network element" procedure in *MG 9000 Configuration Management*, NN10096-511. | |
| **14** | Configure Enhanced ESA, if applicable (only applies to North America) | Go to the Switched Lines Services GUI and change the VMGs to support Enhanced ESA.<br><br>Refer to the "Provisioning ESA" procedure in *MG 9000 Configuration Management*, NN10096-511. | |
| | ***Note:*** This is a safe stopping point. | | |
| After all NEs are at SN07 and there is no need to downgrade to SN06.x proceed to the next step:<br><br>***Note:*** If it is necessary to downgrade the MG 9000 and MG 9000 Manager, perform the "Downgrading the MG 9000 Manager from SN07 to SN06.x" in Upgrading the MG 9000, NN10048-461, procedure, otherwise proceed to the next step. | | | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **15** | Run the pkgrm script on each server (master server and mid-tier server) to stop the SN06.x server application and uninstall the server application. The OM Collector software is located on the mid-tier server.<br><br>***Note:*** Once the packages have been removed, it will not be possible to downgrade without re-importing a saved data image and a resulting loss of service. | 1.<br>Perform the following steps:<br>a. Login as root.<br>b. To stop the SN06.x mid-tier server, type<br>for SN06<br>**> /opt/nortel/mg9kmtr_06/bin/mg9kmidtier stop**<br>for SN06.2<br>**> servstop MG9KMIDTIER_06_2**<br>c. To stop the SN06.x master server, type<br>for SN06<br>**> /opt/nortel/mg9ksrv_06/bin/mg9kserver stop**<br>for SN06.2<br>**> servstop MG9KSERVER_06_2**<br>d. To stop the SN06.x OM collector, which is located on the mid-tier server, type<br>for SN06<br>**> /opt/nortel/OMCollector/bin/OMCollector stop**<br>for SN06.2<br>**> servstop MG9KOMC_06_2**<br>e. To remove the master server SN06.x software, type<br>for SN06<br>**> pkgrm NTmg9ks06**<br>for SN06.2<br>**> pkgrm NTmg9ks62**<br>To continue, respond to the two prompts with Y. | |

**Table 1 MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| 15 | Run the pkgrm script on each server (continued) | f. To remove the mid-tier server SN06 software, type<br>for SN06<br>**> pkgrm NTmg9km06**<br>for SN06.2<br>**> pkgrm NTmg9km62**<br>To continue, respond to the prompt with Y.<br>g. To remove the OM collector SN06.2 software from the mid-tier server, type<br>for SN06<br>**> pkgrm NTomcltr**<br>for SN06.2<br>**> pkgrm NTomclt62**<br>To continue, respond to the two prompts with Y. | |
| | ***Note:*** After step 15 is performed, the MG 9000s cannot be downgraded to SN06 without service data loss. | | |
| | ***Note:*** Proceed to the next step only after the one night process (ONP) is complete. | | |
| 16 | After each node is upgraded to SN07, FTP the ESA data to database. | To ensure ESA data is correct, FTP the ESA data to the database. Refer to “Downloading ESA data from the Core” in *MG 9000 Configuration Management, NN10096-511*. | |
| **17** | Clean up old data in the NPM database. | Perform the procedure “Cleaning up old data in the NPM database” in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450. | |
| **18** | This procedure is complete. | | |

## SN06.2 to SN07 N240 two-server (cluster) upgrade checklist

Use the following table as a checklist for upgrading the MG 9000 Manager and MG 9000 from SN06.2 to SN07in a two-server (cluster)

configuration. Enter a check mark (√) in the √ column as each step or procedure is completed.

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **On the Inactive node** | | | |
| | ***Note:*** Ensure getpatch has been run on all SN07 patches that are applicable for the new SN07 applications prior to proceeding with the upgrade to SN07<br>Refer to "Transferring patches to the NPM database manually" in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450. | | |
| **1** | Upgrade the Succession Server Platform Foundation Software (SSPFS). | Perform procedure Upgrading SSPFS software in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450. | |
| **2** | Install any SSPFS MNCLs.<br><br>***Note:*** Only perform this step if you received a notification bulletin that an SSPFS MNCL is available for the release you just upgraded. | Refer to the instructions provided with the MNCLs. | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **3** | Upgrade the MG 9000 Manager to SN07. | 1. Perform the following steps to complete the MG 9000 Manager upgrade.<br>a. Telnet to the specific machine to be upgraded by typing<br>**`> telnet <server ip address>`**<br>b. Login as root<br>c. To verify you are on the inactive node, type<br>**`> bash`**<br>d. To verify all applications have stopped, type<br>**`> servquery -status all`**<br>e. To verify if the node in the cluster is active or standby unit, type<br>**`> ubmstat`**<br>f. To verify the unit is in standby and is in a normal state<br>**`> udstat`**<br>g. Perform procedure Upgrading MG 9000 Manager software from SN06.x to SN07 on page 805.<br>h. Configure the MG 9000 Manager master software by performing procedure Configuring the MG 9000 Manager master server software on page 818.<br>i. Configure the MG 9000 Manager mid-tier software by performing procedure Configuring the MG 9000 Manager mid-tier server software on page 823.<br>j. Configure the network elements with the OM collector. Refer to the “Installing OM Collector software” in *MG 9000 Performance Management*, NN10140-711.<br>k. Provision any new users, if required. Refer to *MG 9000 MG 9000 Security and Administration*, NN10162-611.<br><br>***Note:*** Previous SN06.2 users are maintained through the upgrade. | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **On the Active node** | | | |
| **4** | Stop the cluster. | Perform procedure "Stopping a cluster in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450. | |
| **On the newly Active node with SN07 software** | | | |
| **5** | Verify the node is the active unit and the health of the unit | To verify the node is the active unit by typing<br>**> ubmstat**<br>To check the health of the unit, type<br>**> servquery -status all** | |
| **6** | Launch client software from active node | 1. Install the MG 9000 Manager client software<br>• For Windows PC client installation, refer to Installing the MG 9000 Manager Windows PC client software on page 825<br>• For Sun workstation client installation, refer to Installing the MG 9000 Sun client software on page 827<br>2. Start the SN06.2 MG 9000 Manager client. Refer to *MG 9000 Security and Administration*, NN10162-611.<br>3. Start the SN07 MG 9000 Manager client. Refer to *MG 9000 Security and Administration*, NN10162-611.<br>***Note 1:*** During the upgrade process, when the user clicks on the SN07 link in the Application Launch Point, the SN07 application launches. At that point, the user must login. This allows the user into the SN07 application. However, when the SN06.2 link is selected, a second and different login box appears, meaning the user must log in again to access the SN06.2 application. This only occurs during this upgrade session.<br>***Note 2:*** SN06.2 and SN07 can run simultaneously. | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **7** | Clone the image of the upgraded node onto the other node | Perform procedure "Cloning the image of one node in a cluster to the other node" in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450. | |
| | ***Note 1:*** This is a safe stopping point<br>***Note 2:*** Before proceeding, ensure the GWC has been upgraded by referring to Upgrading the Gateway Controller on page 834. | | |
| **For each network element in SN06.2** | | | |
| **8** | Ensure all MG 9000 Patch Image (9PI) load files have been copied to the CS2000 Core Manager (SDM) to support upgrade / downgrade activity from DAT tape or CD-ROM. | Refer to "*Upgrading the CS S2000 Core Manager*, NN10060-461."<br>Refer to Installing MG 9000 loads into the CS 2000 Core Manager from DAT tape on page 909 or Installing MG 9000 loads into the CS 2000 Management Tools Manager from CDROM on page 916. | |
| **9** | Provisioning a floating IP address. | Refer to Provisioning a floating IP address on page 918. | |
| **10** | Upgrade the MTA card, if equipped. | Perform the procedure Downloading software into the MTA card on page 926. | |
| **11** | Upgrade the xDSL cards, if equipped | Perform the procedure Downloading software into the xDSL card on page 928. | |
| **12** | Perform a card upgrade in the SN06.2 subnet on the following cards on the NE: all DS1s, ABIs, ITPs, ITXs, and DCCs. | Perform the procedure Upgrading the MG 9000 from SN06.x to SN07 on page 923. | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **13** | Determine if the DCC cards software version is at 7. | From the Frame view, click on Actions->Software Upgrades in the menu bar. From the Software Upgrades view, click on Version List. Check the version of the DCC cards or click on the frame, shelf, card to view each DCC and make sure the software version indicates 7. Both DCC cards must be at the SN07 software version.<br><br>***Note 1:*** Upgrade should not progress until both DCC card versions are SN07.<br><br>***Note 2:*** Once the MG 9000 has been upgraded to SN07, no further provisioning should occur. | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **14** | Export data to XML file.<br><br>Wait for the Export To XML File window to indicate that the export is complete. | In the SN06.2 Subnet View, select the MG9000 menu and click on Export NE. From the ExportNE Contents to XML File window, select an NE and click on Export. Refer to Performing an Export NE on page 832.<br><br>Look for: Completed XML Export of NE: <ne number><br><br>***Note 1:*** After the exports are complete, tar the entire persistdata directory, located on the MG 9000 master server, and place the exported data onto another machine for vaulting purposes. The following files and directories may be in the persistdata directory:<br>• LoadFilesPersistData.dat<br>• xml<br>• ESA_SYSTEM_SD_V1.0.DTD<br><br>***Note:*** ESA_SYSTEM_SD_V1.0.DTD is generated only for SN06.2 MG 9000 Manager data, not for the SN06 MG 9000 Manager data.<br><br>• SubnetPersistData06_2.dat<br><br>Use the following information to tar the persistdata files and directories<br><br>tar cvf <filename>.tar /data/mg9kem/persistdata<br><br>It is recommended that the filename use the following format:<br><br><date.hostname_filename>.tar<br><br>for example,<br><br>OCT23.rtpd_persistdatabackup.tar<br><br>***Note 2:*** Keep a backup copy of the SN06.2 XML file in case a downgrade is required. | |
| | ***Note:*** This is a safe stopping point. | | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **15** | Determine if the sync reference/ timing signal source is correct. This must be correct to prevent alarms on the DCC and ITP cards when the upgrade is complete. | If the BITS cable was connected to the DCC card BITS connector during the hardware installation, using the Local Craft Interface (LCI) access the master shelf in the network element being upgraded, and select the active ITP card. From the menu, select Clock Sync->Provisioning. Ensure the MG 9000 is synched to the correct timing source, BITS or network:<br>• ITXBITS - if syncing to the ITX card<br>• DCCBITS - if syncing to the DCC cards and the cable is connected to the DCC card BITS connector<br>• Network - if syncing to the upstream network connection<br>Refer to *MG 9000 Configuration Management*, NN10096-511. | |
| **16** | Remove the NE from the SN06.2 OMC collection list. | Once the DCC cards are at SN07, no OMs can be collected until the NE is imported to the SN07 Subnet View. Refer to the “Configuring OM Collector software” in *MG 9000 Performance Management*, NN10140-711 to remove the NE from the SN06.2 OMC collection list. The NE OM Collection checkbox must be checked in the MG 9000 Provisioning View which is accessed from the Subnet View Configuration menu for OM Collection to be enabled for an NE. | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **17** | Create patched images of all MG 9000 loads | 1. After the MG 9000 cards have been upgraded to SN07 and all other MG 9000 Manager workstations have been upgraded to SN07, perform the following procedure to image the network element (NE) cards for use in upgrading the cards in other NEs.<br><br>***Note 1:*** Perform the following steps after the following conditions are met:<br>• the NPM is at SN07<br>• the suite of MG 9000 Manager servers are running SSPFS07, with both SN06.x and SN07 MG 9000 Managers are resident<br>• the old SN06.x MG 9000 Manager is not in control of the MG 9000 devices which are running SN07<br><br>***Note 2:*** The following steps will create patched images of all MG 9000 loads. This will be accomplished by upgrading, patching, and then imaging two MG 9000s (one DCC-OC3 MG 9000 and one DCC-IMA MG 9000). Ensure the NEs selected include all MG 9000 intelligent card types in the office.<br><br>First the user will upgrade all the intelligent cards on a DCC-OC3 MG 9000 using the latest available PI loads. After the upgrade, the user will patch all intelligent cards on the DCC-OC3 MG 9000 with any available patches that were not included on the PI load tape. After patching is complete, the user will take an image of the DCC-OC3 MG 9000 using the NPM.<br><br>Next, the user will upgrade a DCC-IMA MG 9000 using the PI loads just created. After the upgrade, the user will apply any available patches for any remaining intelligent card types (including the DCC-IMA) that were not patched during the DCC-OC3 MG 9000 upgrade. After patching is complete, the user will take an image of the DCC-IMA MG 9000 using the NPM. | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| 17 | Create patched images of all MG 9000 loads (contd) | a. Use the following to determine the next step.<br>• if there were additional patches added to the pre-patched image loadfile, go to step b<br>• if there were no additional patches added to the pre-patched image loadfile, go to step c<br>b. Image one NE with OC3 DCC cards with SN07 patched images.<br>c. Apply remaining SN07 patches to all cards on this NE with OC3 DCC cards.<br>d. Import this NE with DCC OC3 cards to the SN07 MG 9000 Manager.<br>***Note:*** Make sure an audit is not in progress and is not scheduled for this NE.<br>Go to the SN07 Subnet View and click on the MG9000 menu and click on Import NE.<br>From the Import From XML File window, select the SN06.x import path<br>**/data/mg9kem/persistdata/xml/SN06/<ne_number>** for SN06,<br>or<br>**/data/mg9kem/persistdata/xml/SN06_2/<ne_number>** for SN06_2<br>which is to be upgraded.<br>Select Import. This will import and convert all the SN06.2 data which was previously exported. The NE icon will be created and a discovery/recovery process is started.<br>Refer to Performing an Import NE on page 830.<br>e. Take an image of the inactive cards on this NE with DCC-OC3. Refer to the “Performing a device image using the NPM” in *ATM Solutions Upgrade*, NN10261-450 or *IP Solutions Upgrade*, NN10344-450 for steps on performing a device image. Select SmartImage->MG9KDEVICES.. | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| 17 | Create patched images of all MG 9000 loads (contd) | f. Upgrade one NE with DCC-DS1-IMA cards with the SN07 MG 9000 patched images just created in the previous step. Load all cards on this NE with the supplied image.<br>g. Import this NE with DS1-IMA DCC cards to the SN07 MG 9000 Manager.<br><br>***Note:*** Make sure an audit is not in progress and is not scheduled for this NE. Observe the Audit Tasks tab in the Frame View.<br><br>Go to the SN07 Subnet View and click on the MG9000 menu and click on Import NE.<br>From the Import From XML File window, select the SN06.x import path<br><br>**/data/mg9kem/persistdata/xml/SN06/<ne_number>** for SN06,<br><br>or<br><br>**/data/mg9kem/persistdata/xml/SN06_2/<ne_number>** for SN06_2<br><br>which is to be upgraded.<br><br>Select Import. This will import and convert all the SN06.2 data which was previously exported. The NE icon will be created and a discovery/recovery process is started.<br>Refer to Performing an Import NE on page 830.<br>h. Apply the remaining patches to all cards on this NE with DCC DS1-IMA cards.<br>i. Take an image of the inactive cards on this NE with DS1-IMA DCC cards that were not imaged in step e above. Refer to the “Performing a device image using the NPM” in *ATM Solutions Upgrade*, NN10261-450 or *IP Solutions Upgrade*, NN10344-450 for steps on performing a device image.<br>j. Use the images created in the previous steps to upgrade all the of the cards on all the remaining NEs to be upgraded to SN07 | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **18** | Delete the NE which was just upgraded. | Go to the SN06.2 Subnet View. From the menu bar, select Configuration->Delete Node. Click on Apply.<br>Refer to the "Deleting an MG 9000 network element" procedure in *MG 9000 Configuration Management*, NN10096-511. | |
| **19** | Configure Enhanced ESA, if applicable (only applies to North America) | Go to the Switched Lines Services GUI and change the VMGs to support Enhanced ESA.<br>Refer to the "Provisioning ESA" procedure in *MG 9000 Configuration Management*, NN10096-511. | |
| | ***Note:*** This is a safe stopping point. | | |
| After all NEs are at SN07 and there is no need to downgrade to SN06.2 proceed to the next step:<br><br>***Note:*** If it is necessary to downgrade the MG 9000 and MG 9000 Manager, perform the "Downgrading the MG 9000 Manager from SN07 to SN06.x" in Upgrading the MG 9000, NN10048-461 procedure, otherwise proceed to the next step. | | | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **20** | Run the pkgrm script on each server (master server and mid-tier server) to stop the SN06.2 server application and uninstall the server application.<br><br>***Note:*** Once the packages have been removed, it will not be possible to downgrade without re-importing a saved data image and a resulting loss of service. | 1. Perform the following steps:<br>a. Login as root.<br>b. To stop the SN06.2 mid-tier server, type<br>**> servstop MG9KMIDTIER_06_2**<br>c. To stop the SN06.2 master server, type<br>**> servstop MG9KSERVER_06_2**<br>d. To stop the SN06.2 OM collector, type<br>**> servstop MG9KOMC_06_2**<br>e. To remove the master server SN06.2 software, type<br>**> pkgrm NTmg9ks62**<br>To continue, respond to the prompt with Y.<br>f. To remove the mid-tier server SN06 software, type<br>**> pkgrm NTmg9km62**<br>To continue, respond to the prompt with Y.<br>g. To remove the OM collector SN06.2 software, type<br>**> pkgrm NTomclt62**<br>To continue, respond to the prompt with Y. | |
| | ***Note:*** Proceed to the next step only after the one night process (ONP) is complete. | | |
| **21** | Clone the image of the upgraded node onto the other node | Perform procedure “Cloning the image of one node in a cluster to the other node” in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450. | |
| | ***Note:*** After step 21 is performed, the MG 9000s cannot be downgraded to SN06 without service data loss. | | |
| 22 | After each node is upgraded to SN07, FTP the ESA data to database. | To ensure ESA data is correct, FTP the ESA data to the database. | |

**Table 2 MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server)**

| | Activity | Procedure | √ |
|---|---|---|---|
| **23** | Clean up old data in the NPM database. | Perform the procedure “Cleaning up old data in the NPM database” in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450. | |
| **24** | This procedure is complete. | | |

# Upgrading the MG 9000 Manager

The following procedures are included in this section:

- Upgrading MG 9000 Manager software on page 804
- Importing MG 9000 Manager data on page 830
- Exporting MG 9000 Manager data on page 832
- Patching MG 9000 Manager software on page 1776
- “Downgrading the MG 9000 Manager from SN07 to SN06.x” inUpgrading the MG 9000, NN10048-461
- “Upgrading the MG 9000 Manager software to a maintenance release” in Upgrading the MG 9000, NN10048-461

# Upgrading MG 9000 Manager software

## When to use this procedure

Use these procedures for upgrading the server, mid-tier, and client portions of the MG 9000 Manager. A procedure for upgrading software on a PC client is also provided.

***Note:*** The software must be installed in the order presented in Upgrading MG 9000 Manager software from SN06.x to SN07 on page 805.

The following procedures are included in this section:

- Upgrading MG 9000 Manager software from SN06.x to SN07
- Upgrading the MG 9000 Manager server
- Upgrading the MG 9000 Manager mid-tier
- Installing the MG 9000 Manager Sun client software
- Uninstalling the MG 9000 Manager Sun client software
- Installing the MG 9000 Manager Windows PC client software
- Removing an MG 9000 Manager JWS application from cache

## Prerequisites

There are no prerequisites.

## Action

### Upgrading MG 9000 Manager software from SN06.x to SN07

***At the MG 9000 Manager***

**1** Stop the SN06.x MG 9000 client applications.

**2** Use the information in the following table to determine the next step.

| If the MG 9000 Manager software to be upgraded runs on | Do |
|---|---|
| an N240 cluster (two-server) configuration | step 9 |
| a t1400/N240 simplex (one-server) configuration | step 3 |

**3** Stop the OM Collector by typing

for SN06

```
> /opt/nortel/OMCltr_06/bin/OMCollector stop
```

for SN06

```
> servstop MG9KOMC_06_2
```

**4** Stop the SN06.x mid-tier server application by typing

for SN06

```
> /opt/nortel/mg9kmtr_06/bin/mg9kmidtier stop
```

for SN06.2

```
> servstop MG9KMIDTIER_06_2
```

**5** Stop the SN06.x server application

for SN06

```
> /opt/nortel/mg9ksrv_06_2/bin/mg9kserver stop
```

for SN06.2

```
> servstop MG9KSERVER_06_2
```

***Note:*** Before moving to the next step to upgrade the SSPFS platform, perform a backup of the SSPFS file system using the "Full backup of file system procedure" in *ATM/IP Security and Administration*, NN10281-600.

**6** To verify the MG 9000 mid-tier and server applications have stopped, type

```
> servquery -status all
```

**7** Use the information in the following table to determine the next step.

| If the MG 9000 Manager software to be upgraded runs on | Do |
|---|---|
| an N240 cluster (two-server) configuration, the SSPFS has already been upgraded | step 9 |
| a t1400/N240 simplex (one-server) configuration | step 8 |

**8** Upgrade both the mid-tier server and the master server to the SN07 SSPFS platform.

***Note 1:*** Ensure the master server is restarted before mid-tier server.

***Note 2:*** If the mid-tier server comes up before the master server, it will go through a restart loop until the master server comes up.

Details about upgrading the SSPFS platform are provided in procedure “Upgrading SSPFS software” in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.

**9** Install any patches for SSPFS using the NPM.

***Note:*** If this is an N240 cluster configuration, install the patches using the NPM on the inactive side.

**10** Verify that the DB Host IP address is correct. Perform the following steps:

**a** Change the directory by typing

for SN06

```
cd /opt/nortel/mg9ksrv_06/bin
```

for SN06.2

```
cd /opt/nortel/mg9ksrv_06_2/bin
```

**b** Enter the following command:

**`./mg9kserver config`**

The system responds with

```
WARNING: Server is currently running, its
recommended that the server be shutdown
before making any configuration setting
changes.
Main Configuration Menu

1) Change Distribution Policy
2) Change SESM IP Address
3) Change Oracle IP Address
4) Change Debug Level for logs
5) Change Persistence settings
6) Change ESA data download settings
7) Change EM Factory Sleep
8) Display current settings
9) Exit from Main Menu

Please make a selection =>
```

**c** Enter 6 (for SN06) or 8 (for SN06.2) to display current setting.

The system responds with the following:

```
            CURRENT SETTINGS
Package Name              :NTmg9ks62
Version                   :NTMG9KS_6_2_481_0
Server Mode               :MASTER
Master Server IP Address :47.xxx.xx.98
SESM IP Address           :47.xxx.xx.66
Oracle IP Address       :47.xxx.xx.66
Maintenance Release Upgrade  :No
Initialize Database     :YES
Security Authentication Host  :47.xxx.xx.98
ESA data download time  :1:30 AM
ESA data device name    :/SFDEV
ESA data file name         :ESA_SYSTEM_SD$XML
```

**d** Enter 7 (for SN06) or 9 (for SN06.2) to exit from the Configuration menu.

**e** Verify that the Oracle IP address is correct

**f** Enter the following command by typing

**# echo $DB_HOST**

The system responds with DB Host IP address

```
# 47.xx.xx.66
```

This IP address should match the Oracle IP address above.

**11** The next step is determined by the information in the following table.

| If the DB Host IP address is | Do |
|---|---|
| correct | Step 13 |
| not correct | Step 12 |

**12** To change the DB Host IP address, perform the following steps:

**a** Enter the following command

**#./mg9kserver config**

The system responds with

```
Main Configuration Menu

1) Change Distribution Policy
2) Change SESM IP Address
3) Change Oracle IP Address
4) Change Debug Level for logs
5) Change Persistence settings
6) Change ESA data download settings
7) Change EM Factory Sleep
8) Display current settings
9) Exit from Main Menu

Please make a selection=>
```

**b** To change the Oracle IP address, enter 3.

The system responds with the following:

```
Oracle IP Address Configuration Menu

1) Enter new Oracle IP Address
2) Exit to Main Menu

Please make a selection [Current:
47.xxx.xx.66 ] => 1

WARNING: Changing the Database Host will
effect all applications! Improper database
configuration will result in loss of service
and possible loss of data. Applications which
use the database server must be shutdown
before continuing.

Oracle Server is currently: 47.xxx.xx.66

Do You Want To Change the Oracle Server, Type
"yes" or "no":
```

**c** To change the Oracle server, type

**> Yes**

**d** Enter the IP Address of the Oracle Server

**> 47.xxx.xx.100**

The system responds with the following:

```
Database change successful

Please quit this shell and login again to
inherit the new settings.

Applications need to be reconfigured with the
new database host.
```

**13** Install the SN07 master server application by performing the procedure Upgrading the MG 9000 Manager master server on page 814.

**14** Use the following table to determine the next step.

| If the server being upgrade is | Do |
|---|---|
| an N240 cluster configuration | step 17 |
| an N240 one-server or t1400 configuration | step 15 |

**15** Start the SN07 master server application by typing

```
> /opt/nortel/mg9ksrv_07/bin/mg9kserver start
```

***Note:*** Messages may appear indicating that a "<file_name>_patch failed to stay up." These messages can be ignored.

**16** Ensure the SN06.2 server application is running by typing

for SN06

```
> /opt/nortel/mg9ksrv_06/bin/mg9kserver status
```

***Note:*** If the SN06.2 server application is not running, type

**> /opt/nortel/mg9ksrv_06/bin/mg9kserver start**

for SN06.2

```
> servquery -status all
```

and verify the following is output

```
MG9KSERVER_06_2 RUNNING
```

***Note:*** If the SN06.2 server application is not running, type

**> servstart MG9KSERVER_06_2**

**17** Install the SN07 mid-tier server application by performing the procedure Upgrading the MG 9000 Manager mid-tier server on page 816.

**18** Use the following table to determine the next step.

| If the server being upgrade is | Do |
|---|---|
| an N240 cluster configuration | step 21 |
| an N240 one-server or t1400 configuration | step 19 |

**19** Start the SN07 mid-tier server application by typing

```
> /opt/nortel/mg9kmtr_07/bin/mg9kmidtier start
```

***Note:*** Messages may appear indicating that a "<file_name>_patch failed to stay up." These messages can be ignored.

**20** Ensure the SN06.x mid-tier application is running by typing

for SN06

```
> /opt/nortel/mg9kmtr_06/bin/mg9kmidtier
status
```

***Note:*** If the SN06 mid-tier application is not running, type

**> /opt/nortel/mg9kmtr_06/bin/mg9kmidtier start**

for SN06.2

```
> servquery -status all
```

and verify the following is output

```
MG9KMIDTIER_06_2 RUNNING
```

***Note:*** If the SN06.2 mid-tier application is not running, type

**> servstart MG9KMIDTIER_06_2**

**21** Install the SN07 performance collector and formatter (PCF) software. Refer to *MG 9000 Performance Management*, NN10140-711 for the PCF software installation procedure. Configure the PCF software after the installation is complete.

If this is an N240 cluster configuration, install the software on the inactive side.

**22** Apply any MG 9000 Manager software patches. Refer to Patching MG 9000 Manager software on page 1776.

**23** Use the following table to determine the next step.

| If the server being upgrade is | Do |
|---|---|
| an N240 cluster configuration | step 24 |
| an N240 one-server or t1400 configuration | step 27 |

**24** Patch the inactive node of the cluster by performing the procedure “Patching the inactive side of a cluster during an upgrade” in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.

**25** Telnet to the cluster IP address, login to the active unit and perform a failover of the system by typing

```
> init 6
```

**26** Perform the procedure “Cloning the image of one node in a cluster to the other node” in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.

**27** Install the SN07 GUI client application by performing the installation procedure based on the platform type used for the client, PC or Sun workstation. Refer to the Installing the MG 9000 Sun client software on page 827 or Installing the MG 9000 Manager Windows PC client software on page 825 procedure.

**28** Provision a userid with appropriate privileges for the upgrade process. Add a new user to group “succssn” and “emsadm.” To allow access to the GUI, from the mid-tier server type

```
> useradd -g succssn -G emsadm [userid]
```

where emsadm is the privilege to be assigned to the userid. Refer to *MG 9000 Administration and Security* for details.

**29** To enter the password for this userid, type

```
>passwd [userid]
```

***Note:*** The password must be entered twice.

**30** Start any SN07 3rd party application(s), especially those using the OSS alarm interface.

**31** Configure the network elements with the OM collector. Refer to the “Installing OM Collector software” in *MG 9000 Performance Management*, NN10140-711.

**32** Start the SN07 OM Collector by typing

```
> servstart MG9KOMC_07
```

**33** Start the OM Collector by typing

for SN06

```
> /opt/nortel/OMCltr_06/bin/OMCollector start
```

for SN06.2

```
> servstart MG9KOMC_06_2
```

**34** Restart the master server application by typing

for SN06

```
> /opt/nortel/mg9ksrv_06/bin/mg9kserver start
```

for SN06.2

```
> servstart MG9KSERVER_06_2
```

**35** Restart the mid-tier server application by typing

for SN06

```
/opt/nortel/mg9kmtr_06/bin/mg9kmidtier start
```

for SN06.2

```
> servstart MG9KMIDTIER_06_2
```

**36** Start the SN06.x GUI client application.

**37** Start the SN07 GUI client application.

***Note 1:*** Two Subnet Views should appear at the GUI Client. One Subnet View for SN06.x and one Subnet View for SN07. All NEs should still be in the SN06.x Subnet View.

***Note 2:*** A discover/recover and audit of all the SN06.x NEs should occur in the SN06.x Subnet View.

**38** This procedure is complete.

If this is a simplex upgrade, return to step 1a of the MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server) on page 777 and continue with the SN06.x to SN07 upgrade process.

If this is a two-server upgrade, return to step 3h of the MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server) on page 790 and continue with the SN06.2 to SN07 upgrade process.

## Upgrading the MG 9000 Manager master server

### *At the workstation dedicated as the master server*

1 Login as root (superuser) and insert the Succession MG 9000 Manager software CD into the CD-ROM drive. This server is also running the OpenOrb NamingService.

***Note:*** If this is an N240 cluster configuration, install the software on the inactive side.

2 List the available files on the Nortel Networks load disk. To list the files, change directory to the CD-ROM drive and list the contents by typing

**> cd /cdrom/cdrom0**

**> ls**

The system responds with the following example output:

```
# cd /cdrom/cdrom0
# ls
BWTool.exe NTMG9KS_7_31_0.PKG
NTMG9KM_7_31_0.PKG NTOMCLTR_7_31_0.PKG
```

3 At the prompt (#), use pkgadd to install the server portion (NTmg9ks07.pkg) of the software. To directly install the software from the CD, enter the following command:

**# pkgadd -d /cdrom/cdrom0/<mgemserver package>**

where <mgemserver package> is the MG 9000 Manager server package name, for example NTMG9KS_7_31_0.PKG

The system responds with the following:

```
The following packages are available:

 1 NTmg9ks07  Succession MG 9000 Manager Server
        (sparc) 7.44

Select package (s) you wish to process (or 'all'
to process all packages). (default: all)
[?,??,q]:
```

4 Enter “1” and press return to begin the server installation process.

The system responds with the following:

```
Processing package instance <NTmg9ks07> from
</NTmg9ks07.pkg>

Succession MG 9000 Manager Server (sparc) 7.44

Copyright (c) 1998-2003 Nortel Networks
All Rights Reserved

This product is protected by copyright and
distributed under licenses restricting copying,
distribution and decompilation.


## Executing checkinstall script.
Using as the package base directory.
## Processing package information.
## Processing system information.
   135 package pathnames are already properly
installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be
executed with super-user permission during the
process of installing this package.

Do you want to continue with the installation of
<NTmg9ks07> [y,n,?]
```

5 Enter Y to continue with the installation.

***Note:*** Verify that the “Installation of <NTmg9ks07> was successful.” If there are any errors please contact your next level of support.

6 Eject the CD-ROM by typing

```
# eject cdrom0
```

7 Obtain the IP address or hostname of the current master server by typing

```
# hostname
```

8 This procedure is complete. If this activity is part of an MG 9000 Manager upgrade, return to step 14 in procedure Upgrading MG 9000 Manager software from SN06.x to SN07 to continue with the upgrade process.

## Upgrading the MG 9000 Manager mid-tier server

### *At the workstation dedicated as mid-tier server*

1 Login as root (superuser) and insert the CD containing the Succession MG 9000 Manager software into the CD-ROM drive.

***Note:*** If this is an N240 cluster configuration, install the software on the inactive side.

2 At the prompt (#) use pkgadd to install the mid-tier portion (NTmg9km07.pkg) of the software. If you are directly installing from the CD-ROM use the following command to read the CD-ROM, and list the contents to read the release number:

```
# cd /cdrom/cdrom0/
# ls
# pkgadd -d /cdrom/cdrom0/NTmg9km_7_xx_0.pkg
```

where xx is the release number.

The system responds with the following information.

```
The following packages are available:
1 NTmg9km07 Succession MG 9000 Manager Midtier
Server
                    (sparc) 7.44

Select package(s) you wish to process (or 'all'
to process all packages). (default: all)
[?,??,q]: all
```

3 Enter “1” and press return to begin the server installation process.

The system responds as follows:

```
Executing checkinstall script.
Using </opt> as the package base directory.
Processing package information.
Processing system information.
1 package pathname is already properly
installed.
```

***Note:*** If a message appears with a confirmation prompt to overwriting conflicting files, respond Y. If existing files are not overwritten, the MG 9000 Manager mid-tier server upgrade cannot continue.

```
Verifying disk space requirements.
Checking for conflicts with packages already
installed.Checking for setuid/setgid programs.

This package contains scripts which will be
executed with super-user permission during the
process of installing this package.

Do you want to continue with the installation of
<NTmg9km07> [y,n,?]
```

**# Y**

***Note:*** Verify that “Installation of <NTmg9km_7_xx_0> was successful.” If there are any errors please contact your next level of support.

**4** The installation continues automatically and installs all the mid-tier server files in /opt/nortel/mg9kmtr_07 subdirectory as noted in the system response.

```
Installing Succession MG 9000 Manager Midtier
Server as <NTmg9km07>

## Installing part 1 of 1.
.
.
.
Configuring system, please wait ...

Installation of <NTmg9km07> was successful.
```

After the installation is compete, a message appears reporting that the installation was successful.

**5** This procedure is complete. If this activity is part of an MG 9000 Manager upgrade, return to step 18 of procedure Upgrading MG 9000 Manager software from SN06.x to SN07 to continue with the upgrade process.

## Configuring the MG 9000 Manager master server software

***At the workstation dedicated as the MG 9000 Manager master server***

1 Collect previous configuration data before proceeding. To display previous configuration data, type

**> /opt/nortel/mg9ksrv_06_2/bin/mg9kserver config**

The system responds with the following:

```
WARNING: Server is currently running, its
recommended that the server be shutdown before
making any configuration setting changes.
Main Configuration Menu

1) Change Distribution Policy
2) Change SESM IP Address
3) Change Oracle IP Address
4) Change Debug Level for logs
5) Change Persistence settings
6) Change ESA data download settings
7) Change EM Factory Sleep
8) Display current settings
9) Exit from Main Menu
```

2 Enter 8 to display current settings.

The system responds with the following example output:

```
CURRENT SETTINGS
Package Name                    :NTmg9ks62
Version                       :NTMG9KS_6_2_481_0
Server Mode                     :MASTER
Master Server IP Address        :47.xxx.xx.134
SESM IP Address                 :47.xxx.xx.137
Oracle IP Address               :47.xx.xx.137
Maintenace Release Upgrade      :NO
Initialize Database             :YES
Security Authentication Host    :47.xx.xx.134
ESA data download time          :1:30 AM
ESA data device name          :/SFDEV
ESA data file name             :ESA_SYSTEM_SD$XML
```

3 Exit the tool by entering 8 (for SN06) or 9 (for SN06.2).

4 To configure the master server, type

**> /opt/nortel/mg9ksrv_07/bin/mg9kconfig.sh**

***Note:*** The database for SN07 is not created until the server is restarted.

**5** The system responds with the following

```
Please enter the IP Address or hostname of CS2M
server?
Press the enter key to accept the default?
Default: [] =>
```

***Note:*** Only enter a Hostname if DNS is properly configured. Nortel recommends using IP addresses only.

**6** Enter the IP address for the CS2M server or select the default address in response to the following:

```
Please enter the IP Address or hostname of the
CS2M server? Press the enter key to accept the
default ?
Default: [] => x.x.x.x
```

**# <CS2M server IP address>**

**7** Enter the IP address where the Oracle server is being hosted in response to the following.

```
Please enter the IP Address or hostname of the
Oracle host server?
Press the enter key to accept the default ?
Default: [47.xxx.xx.220] =>
```

***Note:*** Only enter a Hostname if DNS is properly configured. Nortel recommends using IP addresses only. This information will be needed when configuring the mid-tier server.

This is usually the same IP address as the CS2M server, unless a dedicated Oracle server is being used, which requires a different IP address.

**# <Oracle IP address>**

***Note:*** Only enter a Hostname if DNS is properly configured. Nortel recommends using IP addresses only.

**8** Enter the IP address of the Security Authentication Host in response to the following:

***Note:*** The default IP is the MG 9000 mid-tier server IP address.

```
Please enter the IP address or hostname of the
Authentication server?
Press the enter key to accept the default ?
Default: [47.xxx.xx.235] =>
```

This is usually the same IP address as the MG 9000 mid-tier server IP address.

**9** Enter the IP address or Hostname of the server where image files are stored.

```
Please enter the IP address or hostname of the
server that will be used to store load images.

NOTE: The FTP server must have over write
privileges.

Press the enter key to accept the default ?
Default: [x.x.x.x] =>
```

This is typically the SDM address. It must have over write privileges. Communication to the server is verified.

**10** Enter yes if Integrated EMS (IEMS) is to be the Northbound interface for Logs.

```
Please enter yes if you want IEMS to be the
Northbound interface for Logs? Press the enter
key to accept the default (y/n)?
Default: [y] =>
```

***Note:*** Answering Y to this question means the syslog output of the master server has already been set to IEMS using the command line interface.

**11** Enter the User ID that is used to FTP images to the FTP server entered in the previous step.

```
Enter the user id that will be used to ftp Images
to the Image server.

Press the enter key to accept the default ?
Default: [] =>
```

**12** Enter the User ID and password to the Image server. This must have over write privileges.

```
Enter the user id that will be used to ftp Images
to the Image server.

Press the enter key to accept the default?
Default: [] => xxxx
Enter Password: xxxxxx
```

**13** Enter the directory where the images will be placed for each type of card.

```
Enter the directory that the image will be
placed in for the following cards:

SCI: Press the enter key to accept the default ?
Default: [/swd/mg9k] =>

SCO: Press the enter key to accept the default ?
Default: [/swd/mg9k] =>

ITP: Press the enter key to accept the default ?
Default: [/swd/mg9k] =>

ABI: Press the enter key to accept the default ?
Default: [/swd/mg9k] =>

DS1: Press the enter key to accept the default ?
Default: [/swd/mg9k] =>
```

**14** Verify the system response.

```
*********************************************
Setup Server As : Master
Master Server IP Address : 47.xxx.xx.207
CS2M IP Address: 47.xxx.xx.220
Security Authentication Host : 47.xxx.xx.220
Get Northbound logs from IEMS : y
Oracle IP Address : 47.xxx.xx.8
Image Server : 47.xxx.xx.207
Image Server User ID : maint
SuperCore IMA Image Directory : /swd/mg9k
SuperCore OC3 Image Directory : /swd/mg9k
ITP Image Directory : /swd/mg9k
ITX Image Directory : /swd/mg9k
ABI Image Directory : /swd/mg9k
DS1 Image Directory : /swd/mg9k
*********************************************
Is the above information correct?
Press the enter key to accept the default (y/n)?
Default : [n] => y
```

**15** Start the MG 9000 Manager server application. To start the server, type

```
> servstart MG9KSERVER_07
```

**16** For additional help on available options, execute the following command.

```
# /opt/nortel/mg9ksrv_07/bin/mg9kserver help
```

**17** This procedure is complete.

If this is a simplex upgrade, return to step1b of the MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server) on page 777 and continue with the SN06.x to SN07 upgrade process.

If this is a two-server upgrade, return to step 3i of the MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server) on page 790 and continue with the SN06.2 to SN07 upgrade process.

## Configuring the MG 9000 Manager mid-tier server software

***At the workstation dedicated as the MG 9000 Manager mid-tier server***

**1** Collect the current configuration by typing

for SN06

**`# /opt/nortel/mg9kmtr_06/bin/mg9kmidtier config`**

for SN06.2

**`# /opt/nortel/mg9kmtr_06_2/bin/mg9kmidtier config`**

The system responds with the following.

```
WARNING: Server is currently running, its
recommended that the server be shutdown before
making any configuration setting changes.

Main Configuration Menu


1) Change IP Address of Master Server
2) Enable / Disable SSL Connections
3) Change Debug Level for logs
4) Display current settings
5) Exit from Main Menu
```

**2** Select 4 from the list to display the current settings.

The system responds with the following.

```
CURRENT SETTINGS
Package Name                    :NTmg9km62
Version                        :NTMG9KM_6_2_481_0
Master Server IP Address        :106.40.34.134
SSL enabled                     :false
Security Type                   :PAM Security
```

**3** To configure the mid-tier server, type

**`# /opt/nortel/mg9kmtr_07/bin/mg9kconfig.sh`**

**4** Enter the IP address or hostname of the master server obtained in step 7 of Upgrading the MG 9000 Manager master server

***Note:*** Only enter a Hostname if DNS is properly configured. Nortel recommends using IP addresses only.

**`# <IP address of Master server>`**

Press Return to continue.

**5** The system prompts you to make sure the information provided is accurate.

```
.

.

.

Is the above information correct? Press the
enter key to accept the default (y/n)? Default:
[n] =>
```

**6** Enter Y and continue.

```
Configuring system, please wait ...
Set JNLP softlinks for NTmg9km07...

Configuration complete ...
```

**7** Restart the MG 9000 Manager mid-tier application. To start the application, type

```
> servstart MG9KMIDTIER_07
```

**8** This procedure is complete.

If this is a simplex upgrade, return to step1e of the MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server) on page 777 and continue with the SN06.x to SN07 upgrade process.

If this is a two-server upgrade, return to step 3j of the MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server) on page 790 and continue with the SN06.2 to SN07 upgrade process.

## MG 9000 Manager client configuration

### Installing the MG 9000 Manager Windows PC client software

#### *At the Windows PC client*

1 From a web browser, launch Succession OAM&P Applications Launch Point page at:
http://<SN07 MG9KEM Midtier Server IP or hostname>. Click on Application Launcher.

The Application Launch Point window appears containing two links, one for SN06.x and one for SN07. Click on the SN07 “MG9000 Element Manager” link. The Application Launch Point window appears. Click on the” MG9000 Element Manager” link. Enter the username and password in the login when prompted.

***Note:*** When starting the MG 9000 Manager from a Microsoft Windows platform, Windows may ask for a Security Certificate Approval. Windows does not display the Security Certificate Approval window on top of all other open windows. It may become necessary to iconify all open windows to see the Security Certificate Approval window. The security settings in the browser determine if the user will be asked for certificate approval.

2 Use the following figure and the information in the following table to determine the next step.




| If Java Web Start (JWS) software | Do |
|---|---|
| is already installed in the client machine | step 8 |
| is not installed in the client machine, as evidenced by the preceding message | step 3 |

3 Select the link "Java™ Web Start Install Guide" to visit "Client Software Installation" page.

4 Visit "Java 2 Runtime Environment Install Guide" under "Microsoft Windows" section for online documentation.

5 Visit "Java 2 Runtime Environment Software Download" under "Microsoft Windows" section to download Java Runtime Environment.

6 Save j2re-1_4_1_02-windows-i586-i.exe and execute the JRE software.

7 Follow the instructions in JRE software to install JRE 1.4.1_02

8 The PC client is setup to launch MG 9000 Manager SN07 client applications.

9 This procedure is complete.

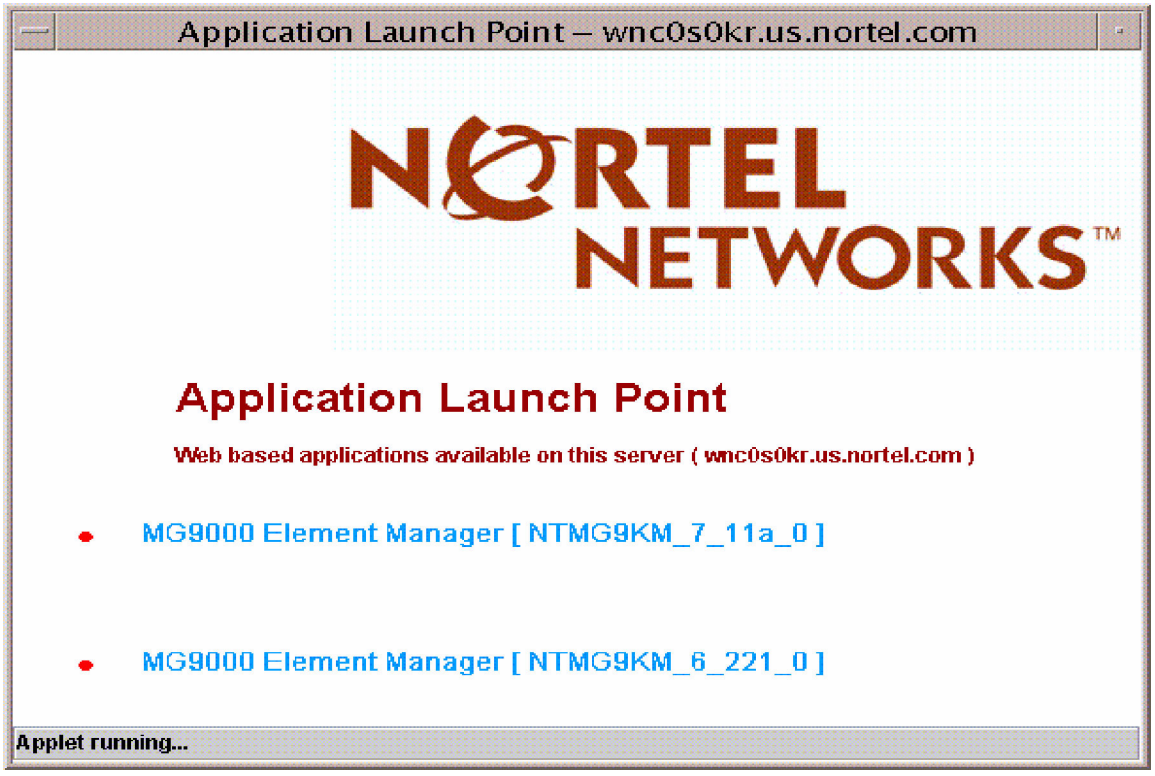
## Installing the MG 9000 Sun client software

### *At the client workstation*

1 From a web browser, launch Succession OAM&P Applications Launch Point page at: http://<SN07 MG9KEM Midtier Server IP or hostname>. Click on Application Launcher.

The Application Launch Point window appears containing two links, one for SN06.x and one for SN07. Click on the SN07 “MG9000 Element Manager” link. The following figure shows the Application Launch Point with the SN06.x and SN07 MG 9000 Manager links. Enter the username and password in the login when prompted.

***Note:*** The top link that appears in the launch point window is for the SN07 client, the bottom link is for the SN06 client.



2 Use the following figure and the information in the following table to determine the next step.




| If Java Web Start (JWS) software | Do |
|---|---|
| is already installed in the client machine | step 14 |
| is not installed in the client machine, as evidenced by the preceding message | step 3 |

3 Select the link “Java™ Web Start Install Guide” to visit “Client Software Installation” page.

4 Visit “Java 2 Runtime Environment Install Guide” under “Sun Solaris” section for online documentation.

5 Visit “Java 2 Runtime Environment Software Download” under “Sun Solaris” section to download Java Runtime Environment.

6 Save j2re-1_4_1_02-solaris-sparc.sh to your home directory.

7 Change execute permissions

```
$ chmod +x j2re-1_4_1_02-solaris-sparc.sh
```

8 Execute JRE, this will create a JRE subdirectory called j2re1.4.1_02 in your home directory. Remember the path of this directory as you will need this path later when configuring JWS.

```
$ ./ j2re-1_4_1_02-solaris-sparc.sh
```

9 Follow the instructions in JRE software to install JRE 1.4.1_02

10 In your j2re1.4.1_02 subdirectory there is a zip file called javaws-1_2_0_02-solaris-sparc-i.zip. Copy this zip file to your home directory.

11 Install JWS by unzipping the zip file and executing “install.sh”.

```
$ unzip ./javaws-1_2_0_02-solaris-sparc-i.zip
```

```
$ ./install.sh
```

12 Accept the license agreement and enter the path to JRE from step 8.

13 Follow the remaining online directions.

14 The Sun Solaris client is now setup to launch MG9KEM SN07 client applications.

15 Exit the browser and launch the browser again for settings to take effect.

16 This procedure is complete.

### Removing an MG 9000 Manager JWS application from cache

#### *At the MG 9000 Manager client PC*

1 Access the Java Web Start Application Manager by selecting Start->Programs->Java Web Start. The Java Web Start Application Manager appears.

2 Select View->Downloaded Applications from the menu bar.

3 Select an MG 9000 Manager JWS application to be deleted.

4 Select Application->Remove Application from the menu bar.

5 This procedure is complete.

The following procedure is provided as an optional method for accessing a JWS application on a Sun workstation.

### Accessing JWS application on a Sun workstation

#### *At the client workstation*

1 Change directory to where the Java Web Start application is installed and enter the following command

```
> cd <path/javaws>
```

2 To launch the Java WebStart application manager, type

```
> javaws &
```

3 Select View->Downloaded Applications from the menu bar.

4 This procedure is complete.

# Importing MG 9000 Manager data

## Purpose of these procedures

These procedures provide the steps for importing MG 9000 Manager data in an upgrade scenario.

## When to use these procedures

Use the procedures when it is necessary to import MG 9000 Manager XML data.

The Import NE command is used to import data during an upgrade.

***Note:*** An import NE can only be used on undiscovered NEs which have previously been exported. If the NE is provisioned, the Import command will not show the NE as able to import. The only NEs that will be listed in the window will be undiscovered or non-existent NEs. The Import can be used if rolling back to a previous software release.

## Prerequisites

This procedure has no prerequisites.

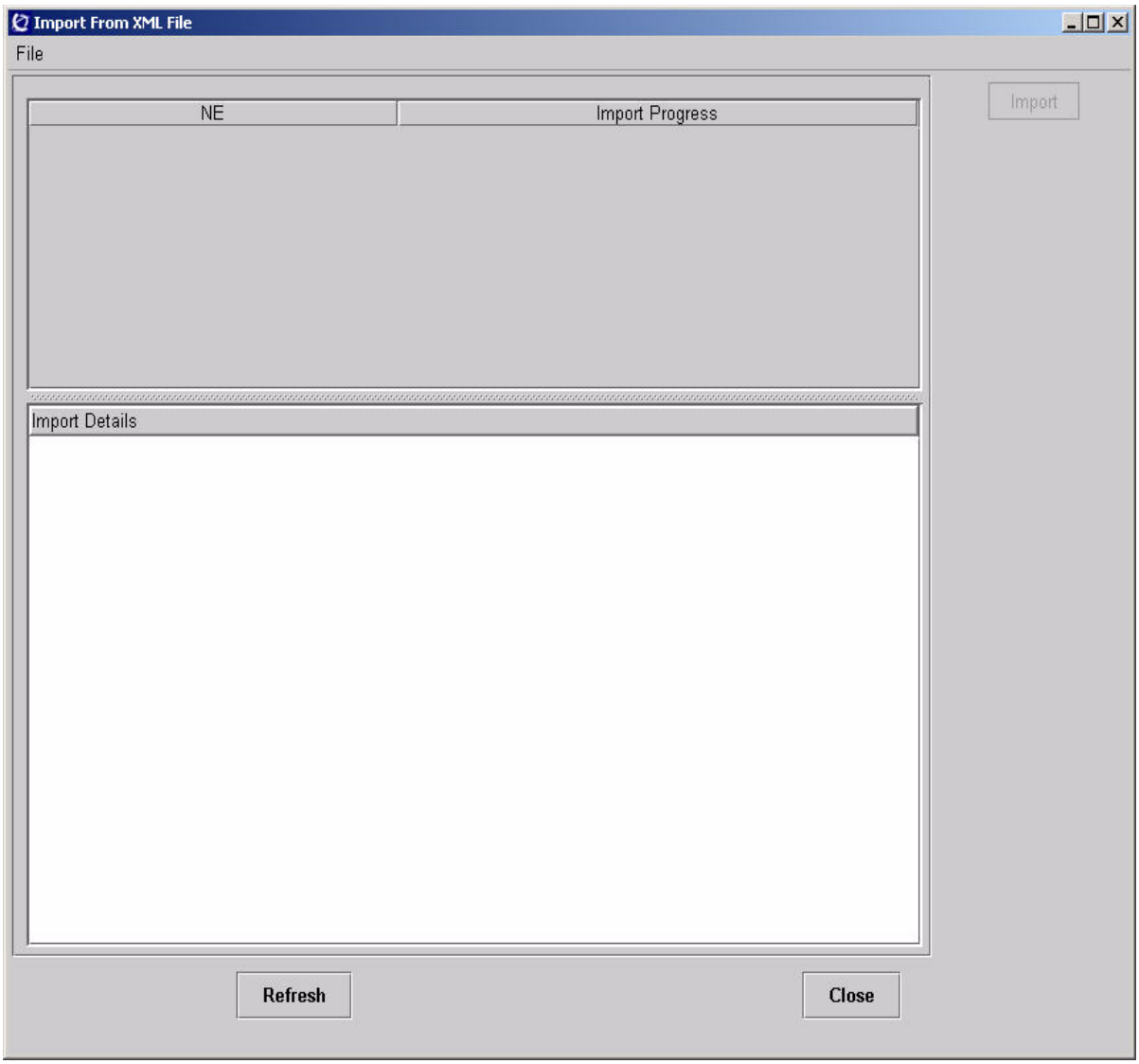
## Action

### Performing an Import NE

***At the MG 9000 Manager***

1 From the Subnet View, select MG9000->ImportNE from the menu bar. The Import from XML file window appears. The following figure shows the Import from XML file window.

## Import from XML file window




2 When upgrading from SN06 to SN07, click on the NE with path named /data/mg9kem/persistdata/xml/SN06/ <ne_number>.

When upgrading from SN06.2 to SN07, click on the NE with path named /data/mg9kem/persistdata/xml/SN06_2/ <ne_number>.

3 Click Import. The progress will be displayed in the Import details pane. Close the window. The Import NE will cause a discovery and an audit to run. Observe the NE icon in the Subnet View appears with a discovery arrow. When the discovery arrow disappears, the Import is complete.

4 This procedure is complete.

# Exporting MG 9000 Manager data

## Purpose of these procedures

This procedures provides the steps for exporting MG 9000 Manager data in an upgrade scenario.

***Note:*** The Export NE command is no longer available in SN07. This procedure is used to support software upgrades from SN06.X to SN07.

## When to use these procedures

Use the procedures when it is necessary to export MG 9000 Manager XML data.

The Export NE command is used to export the customer's data in preparation for an upgrade. The command writes out the customer's MG 9000 Manager data into XML files that are used when upgrading the MG 9000 Manager and MG 9000.

## Prerequisites

This procedure has no prerequisites.

## Action

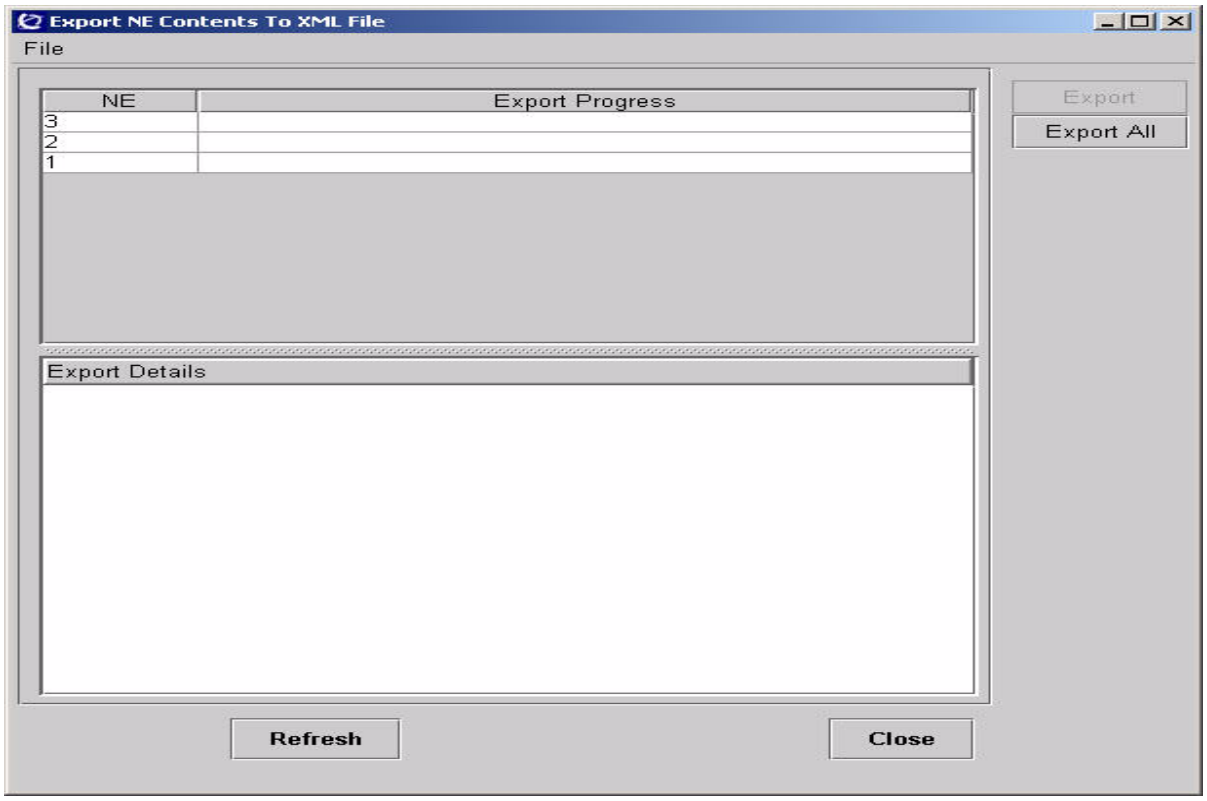
### Performing an Export NE

***At the MG 9000 Manager***

**1** From the Subnet View, select MG9000->ExportNE from the menu bar. The NE Export to XML file window appears. The following figure shows the NE Export to XML file window.

***Note:*** Perform this procedure after provisioning activities are complete.

## NE Export to XML file window




2 Click on the NE, click on Export, then wait for the message “Completed XML Export” appears in the window indicating the export action is complete before closing the window.

***Note:*** Use the Export All button when performing an export in support of an MR release upgrade.

3 This procedure is complete.

# Upgrading the Gateway Controller

## Upgrade strategy

There are no direct software upgrades for the GWC. Instead GWC software upgrades are supplied to the GWC image loaded on the CS 2000 Management Tools server.

Upgrading the GWC occurs when a new software load image is delivered to the customer site. Read the entire GWC upgrades Overview section of this NTP thoroughly to learn the different types of upgrades and conditions applied to each upgrade.

The actual GWC software upgrade process is not an automated process, but is instead a set of manual actions you must carry out in a specific sequence on several Carrier VoIP network components.

Additionally, GWC software updates may be incrementally delivered through a GWC software patches. Gateway Controller patches are applied according to the release specifications for the patch. GWC software patches are released and applied to the GWC image files using the Network Patch Manager (NPM), an application in the CS 2000 Management Tools suite. The release specifications can be found by running a patch list report using the NPM **Tasks|Reports** menu. Some patches are applied only after other patches have been removed. Other patches are applied only under special circumstances. Patches can be applied during an upgrade or on their own as corrective content.

***Note:*** Currently, GWC cards are upgraded one at a time. Parallel upgrades of GWC cards is not supported.

## Software delivery methods

Upgrade loads are delivered using one of the following delivery methods:

- CD-DROM
- Electronic Software Delivery (ESD)

Delivered load are installed on the CS 2000 Core Manager (SDM) or Core and Billing Manager. Any patch files delivered along with the upgrade load are delivered on CD-ROM and installed on the NPM server. Patches may be included in the load image.

To view any patches that are available with the load image, refer to procedure View the contents of a load file image on page 889. If you

want to see what patches are inside the load file, you still must retrieve patch files so that NPM will have the ability to remove the imaged patches.

***Note:*** Starting in SN06, Network Patch Manager implements new login authorization policies. Refer to the CS 2000 Management Tools section in the ATM/IP Solution-level Configuration Management NTP, NN10409-500, to ensure that NPM is properly configured so that you can log onto the NPM GUI or CLUI to perform patching activities.

Software patches can also be delivered using electronic software delivery (ESD). For more information on delivering patches, refer to section Patch file acquisition on page 839.

Necessary procedures or checklists used to complete this process are found in “Succession patching” section of the Solution Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

Your existing Regional Customer Service Team has knowledge of your ESD implementation methodology. You can also contact the technical assistance support (TAS) hotline after hours for any urgent issues related to ESD.

For more information about how your site’s ESD is implemented, contact your site network administrator. Also, refer to the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP) and the document Electronic Software Delivery Customer Implementation Guide.

## Tools and utilities

A GWC software upgrade requires the CS 2000 SAM21 Manager client interface. If GWC software requires patching, the Network Patch Manager (NPM) interface is used to install a patch into GWC software. NPM is an application in the CS 2000 Management Tools suite. This patched load image is optionally saved back to the software load location on the CS 2000 Core Manager or CBM and is available to other GWCs when they reboot. A patched load is saved through the CS 2000 GWC Manager interface. For more information about configuring NPM, refer to the CS 2000 Management Tools section in the ATM/IP Solution-level Configuration Management NTP, NN10409-500. For more information about using NPM, refer to the “Succession patching” section in the Solutions Upgrades NTP, NN10261-450 (for ATM) or NN10344-450 (for IP).

### Integrated Element Management System

Many FCAPS activities may now be performed using the Integrated Element Management System (EMS). In addition, access to the

CS 2000 GWC Manager and the CS 2000 SAM21 Manager, is now provided using the Integrated EMS. For more information, refer to the Integrated EMS Basics NTP, NN10329-111.

To launch the CS 2000 GWC Manager or the CS 2000 SAM21 Manager, refer to the following procedures in the Integrated EMS Basics NTP, NN10329-111:

- "Launching GWC Manager"
- "Launching SAM21 Manager"

## Overall GWC upgrade procedure

The following procedures describe how to upgrade the GWC software and apply patches as part of the same process.

***Note:*** Starting in SN07, the call agent identifier (ID) must be set for the CS 2000. This should typically be done prior to upgrading your GWC cards. For details, refer to section "CS 2000 call agent identifier required in SN07" in the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

1. If necessary, complete the following sub-steps using one of the tools available at www.nortelnetworks.com, under Support -> Software Downloads -> Succession -> Succession Communication Server 2000 -> Tools. For instructions on how to use each tool, refer to the Readme file that can be found under each corresponding link.
   a. Identify patches that have been released against your CD-ROM after it has been shipped - use the Pre Upgrade Patch Calculator tool. Download these patches (if any) to site and retrieve the patch files for the NPM to process using the NPM CLUI **getpatch** command.
   b. Perform site-specific audit to identify any missing patches - use the Patch Audit for Inform List tool.
2. If necessary, backup your existing software load file sets using procedure Create a backup of the GWC load file on page 869.
3. Install the new load using one of the following procedures:
   - Deliver and install GWC package using Electronic Software Delivery on page 846
   - Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 841
4. See if any patches are contained within the load image by referring to procedure View the contents of a load file image on page 889.

5. Upgrade software on a seed GWC unit that is inactive using procedure Upgrade a standby GWC card software load on page 854.
6. If a day or more has passed between completing step 1a and performing the upgrade, repeat step 1b, then continue the procedure.
7. Patch the same seed GWC unit using the following procedures:
   a. Audit the GWC unit for necessary patch activity using procedure Performing a device audit using the NPM on page 1669.
   b. Transfer patches to the Network Patch Manager (NPM) database using procedure Transferring patches to the NPM database manually on page 1664.
   c. You may also define reports for a GWC using procedure Defining reports using the NPM on page 1745.
   d. Apply patches using procedure Applying patches using the NPM on page 1674.
   e. Activate patches using procedure Activating patches using the NPM on page 1690.
   f. Deactivate any obsolete patches using procedure Deactivating patches using the NPM on page 1701.
   g. Remove any obsolete patches using procedure Removing patches using the NPM on page 1712.
8. Complete procedure Take a manual GWC software image on page 885.
9. Perform a warm SwAct on the GWC units in the node.
   Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for a procedure to perform a warm SwAct.

   ***Note:*** Instructions for steps 9, 10 and 11 in this procedure are also available within the procedure Upgrade a standby GWC card software load on page 854 in this NTP.

10. Perform the following steps on the new standby GWC unit.
    Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for procedures to perform each of the following tasks.
    a. Busy the new standby unit.
    b. Lock the new standby unit.

c. Update the new standby unit with the patched GWC load using the CS 2000 SAM21 Manager. Refer to the appropriate steps in the procedure Upgrade a standby GWC card software load on page 854.

d. Unlock the new standby unit.

11. Access the next GWC node and perform the following steps. Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for procedures to perform each of the following tasks.

a. Busy the standby unit.

b. Lock the standby unit.

c. Update the standby unit with the patched GWC load using the CS 2000 SAM21 Manager. Refer to the appropriate steps in the procedure Upgrade a standby GWC card software load on page 854.

d. Unlock the standby unit.

e. SwAct the GWC units in the node.

f. Busy the new standby unit.

g. Lock the new standby unit.

h. Update the new standby unit with the patched GWC load using the CS 2000 SAM21 Manager. Refer to the appropriate steps in the procedure Upgrade a standby GWC card software load on page 854

i. Unlock the new standby unit.

12. Repeat step 11 for each GWC node until all units in each node are rebooted from the new image.

***Note:*** Nortel recommends that you apply all Released (R) and Propagated (P) status patches, take the image, and then apply Verification (V) status patches. It is best not to have V status patches in a saved image since these patches are normally applied to only one GWC.

## Patching procedures

Patching activities occur when new patches become available and need to be installed and activated. They also occur when an older patch becomes obsolete and must be deactivated and/or removed. For more information about patching activities refer to the “Succession patching” section in the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

Although most patch files apply to any Nortel customer site, some patch files are created for a particular customer's site-specific GWC changes. Not all patches made available will apply to all customer sites. Apply all patches to the Gateway Controller (GWC), including activatable (ACT) patches that apply to your site. Contact Nortel customer support to determine which activatable patches are to be activated in your site. Do not activate any other GWC ACT category patches unless advised to do so by Nortel customer support.

### Patch file acquisition

Patch files can be released either at upgrade time or in between upgrades. When patch files are made available during upgrade activity, they are sent on a separate CD-ROM delivered with the new software load. When patch files become available in between upgrade periods, they are delivered by way of Electronic Software Delivery (ESD) to the server supporting your CS 2000 Management Tools software using one of the following methods.

- Drop box - patch files are pushed from Nortel Networks to an external drop box location. The drop box can exist on Nortel Networks' Customer Access Network (CAN), or the customer's wide area network (WAN).
- Web distribution - patches are pulled through the Internet from a secure Nortel Networks web page and stored on a customer-provided server. Web distribution is done through www.nortelnetworks.com. Patches are located under Support -> Software Downloads -> Succession -> Succession Communication Server 2000 -> Software.

***Note:*** Use the filter criteria to only display a selected set of patches.

Also, to facilitate patch management, the following two tools are available under Support -> Software Downloads -> Succession -> Succession Communication Server 2000 -> Tools:

- Pre Upgrade Patch Calculator - use it to identify patches that have been released against your CD-ROM after it has been shipped.
- Patch Audit for Inform List - use it to perform site-specific audit to identify any missing patches.

***Note:*** For instructions on how to use each of these tools, refer to the Readme file that can be found under each corresponding link.

### Patch activation

Once a patch has been received into the NPM database, a patch can be activated if:

- the patch is not on hold
- the patch has a category of ACT
- the patch has been applied to a GWC card
- the device is not on hold

### NPM CLUI User authentication for patching activities

Starting in SN06 NPM CLUI authentication is implemented by a new login method which prompts for a user ID and password, then interacts with the SSPFS servlet application on the CS 2000 Management Tools server for authentication. For more information about user authentication and the NPM CLUI, refer to the CS 2000 Management Tools section in the ATM/IP Solution-level Security and Administration NTP, NN10402-600.

## Managing firmware on GWC cards

The following procedures allow you to ensure that you have the latest firmware version for GWC cards in your system and that any problems with your GWC firmware are resolved:

- To upgrade the version of firmware on GWC cards in your system, refer to procedure Firmware flash a GWC card on page 871.
- To resolve problems with the firmware on a GWC card, refer to procedure Force a firmware flash of a GWC card on page 877.

# Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM

## Purpose of this procedure

This procedure describes how to install GWC software loads onto the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM) from CD-ROM. The software load is installed in the /swd/gwc directory on the CS 2000 Core Manager or CBM.

***Note:*** For information on how to deliver and install GWC load using the Electronic Software Delivery (ESD) method, refer to procedure Deliver and install GWC package using Electronic Software Delivery on page 846

## When to use this procedure

Use this procedure to install a Maintenance Non-Computing Load (MNCL) or a standard software release (NCL) GWC load.

## Prerequisites

This procedure has no prerequisites.

## Action

***At the CS 2000 Management Tools frame (Sun Microsystems t1400 or 240)***

**1** Insert the CD-ROM into the CD-ROM tray.

***At the CS 2000 Management Tools terminal***

**2** Log in and then use the **su** command to gain root privilege.

```
Trying <hostname>....
Connected to <hostname>.
Escape character is '^'.

Authorized use only, activities logged.
login: username
Password: <password>
Last login: Fri Jan 30 12:48:10 from <otherhost>
prompt:>
prompt:> su - root
Password: <root_password>
#
```

**3** Execute the installation script by typing

**# /opt/nortel/sspfs/Scripts/platform_load_install.sh**

and pressing the Enter key.

**Example response:**

```
        Welcome to the Platform Installation Tool Version 3.3
 ================================================================
   RPM INSTALLATION/REMOVAL
  ============================
  1) Install RPM from CDROM        2) Install RPM from Disk
  3) Uninstall RPM                 4) Query all RPMs

  TAR INSTALLATION/REMOVAL
  ============================
  5) Install SC load from Tape     6) Install SC load from cdrom
  7) Install SC load from Disk     8) Remove a SC Load
  9) Install 3PC Load from Tape   10) Install 3PC Load from Disk

  OTHER
  ======
 L) Install SOS/MS/PMLOADS      D) Install SOS/MS/PMLOADS from disk
  C) Change Rotation Parameters  P) View Rotation Parameters
  V) Platform Version Installed  X) Exit

  Please choose one of the following: 1
```

**4** Install the software by typing

**> 1**

and pressing the Enter key.

The system displays the contents of the .rpm package.

**Example response:**

```
          Verifying CDROM is mounted
 /cdrom/cdrom on /vol/dev/disk/c0t0d0/cdrom read
 only/mosuid/mapl-case/noglobal/rr/traildot/dev=16c0001
 on Sat Mar 27 16:34:13 2004
            CDROM is mounted.
            Listing file names in the rpm on the cd.

/swd/gwc/gn070be.imag

             Do you want to continue (y/n)? Y
```

***Note:*** If the system displays the following message: `There is no cd in the CDROM drive, please check drive`, ensure that the CD-ROM is inserted in the tray for this unit.

**5** Confirm that you want to proceed with the installation by typing

**> Y**

and pressing the Enter key.

The software is extracted from the .rpm package. The .rpm package is transferred to the CS 2000 Core Manager or CBM.

**Example response:**

```
      Extracting files from the rpm archive on the cd.

Installing RPM package gn070be_plat-1.0-041304.moarch.rpm
Sun Microsystems Inc.  Sun 5.8   Generic Patch  December 2002
gn070be_plat-1.0-041304.noarch.rpm  100% 11MB 750.4KB   00:14
root@47.135.214.127's password: <enter root password>
```

**6** Enter the root password for the CS 2000 Core Manager or the CBM.

The system installs the software on the CS 2000 Core Manager or CBM. If CBM is used, the .rpm package is then copied to the inactive CBM unit and another prompt for the root password is displayed. If this happens, enter the root password again and press the Enter key.

After the load file is installed on the CS 2000 Core Manager or CBM, the transferred .rpm package is deleted from the CS 2000 Core Manager or CBM.

**Example response:**

```
      Extracting files from the rpm archive on the cd.

Installing RPM package gn070be_plat-1.0--41304.moarch.rpm
Sun Microsystem Inc.  SunOs 5.8  Generic Patch December 2002
gn070be_plat-1.0-041304.noarch.rpm  100% 11MB 8.2MB/s   00:40
root@47.135.214.127's password: <enter root password>
Mate IP is 47.135.214.129
Sun Microsystem Inc.  SunOs 5.8  Generic Patch December 2002
root@47.135.214.129's password: <enter root password>


         ********Please hit ENTER key to continue*******
```

**7** Exit the installation program by typing

```
# x
```

and pressing the Enter key.

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

| If the GWC load is being installed on the | Do |
|---|---|
| CS 2000 Core Manager | go to step 9 |
| CBM | go to step 15 |

***At the CS 2000 Core Manager console or terminal window***

**9** Log in to the CS 2000 Core Manager as the root user.

```
AIX Version 4
 (C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

**10** Access the gwc directory by typing

```
# cd /swd/gwc
```

and pressing the Enter key.

**11** Execute the GwcConfig.sh script by typing

```
# ./GwcConfig.sh
```

and pressing the Enter key.

***Note:*** The script checks if the appropriate configuration data is present in the gwc directory. If the data is not present, the system prompts you to enter the hostname and the IP address of the SAM21 EM server.

**12** If prompted, enter the hostname of the SAM21 EM server and press the Enter key. Otherwise, continue with step 14.

**13** If prompted, enter the IP address of the SAM21 EM server and press the Enter key. Otherwise, continue with step 14.

**14** Log out of the CS 2000 Core Manager by typing

```
# exit
```

and pressing the Enter key.

***At the CS 2000 Management Tools terminal***

**15** Eject the CD-ROM from the CD-ROM tray by typing

```
# eject cdrom
```

and pressing the Enter key.

**16** Log out of the CS 2000 Management Tools server.

**17** This procedure is complete.

# Deliver and install GWC package using Electronic Software Delivery

## Purpose of this procedure

This procedure describes how to transfer Gateway Controller (GWC) software loads from Nortel Networks to a customer drop box using the Electronic Software Delivery (ESD) method, and how to install the transferred load onto the CS 2000 Core Manager or Core and Billing Manager (CBM).

***Note:*** For information on how to install GWC load from CD-ROM, refer to procedure Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 841.

## When to use this procedure

Use this procedure after receiving electronic notification for the following software loads:

- GWCC0070.n.V.NCL.NAP.VAULT.nn.D.tar.gz - for standard NCL release
- GWCW0070.n.V.NCL.NAP.VAULT.nn.D.tar.gz - for standard International NCL release
- GWC0M070.n.V.NCL.NAP.VAULT.nn.D.tar.gz - for maintenance (MNCL) release

*where*

**n**
is an integer value such as 7 and is part of the product order code

**vault**
is a string that identifies the Nortel Networks software vault that holds the software

**nn**
is an integer value that indicates the repository version of the software

## Prerequisites

Your operating company must have an ESD agreement with Nortel Networks. When the agreement was established, the operating company furnished Nortel Networks with the location of an electronic drop box and a user name and password pair for delivering software loads. When Nortel Networks delivers a software load to the drop box, an electronic mail notification is sent to the e-mail address specified by the telephone operating company when the ESD agreement was established.

## Action

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

**1** Make a temporary directory to store the ESD software by typing

**`$ mkdir /data/iso_esd`**

and pressing the Enter key.

**2** Change directory to the newly created location by typing

**`$ cd /data/iso_esd`**

and pressing the Enter key.

**3** Ensure that enough disk space is available for the ESD software (500 MByte is recommended) by typing

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

and pressing the Enter key.

*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.*

```
$ df -k /data
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d20      3082223  144125 2876454     5%    /data
```

2876454 / 1000 = 2876 MB free

**4** Transfer the ESD software files from the drop box on the repository server by typing

**`$ ftp <repository_server>`**

and pressing the Enter key.

*where*

**<repository_server>**
is the machine owned by the telephone operating company that was selected to be the destination for the ESD software files

Log in and change directory to the drop box location on the repository server.

5 Change the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

6 Retrieve the ESD software load by typing

```
ftp> get <esd_filename>.tar.gz
```

and pressing the Enter key.

*where*

**<esd_filename>**
is the ESD filename for the GWC software load

**Example**
**ftp> get GWCC0070.70.V.NCL.NAP.VAULT.8.D.tar.gz**

***Note:*** Determine the actual ESD filename from the Nortel Networks notification, or by listing the contents of the drop box with the **ls** command.

7 Repeat step 6 for all ESD software loads recorded in the notification from Nortel Networks.

8 End the FTP session by typing

```
ftp> bye
```

and pressing the Enter key.

9 Extract the ESD software load from the tape archive format by typing

```
$ gtar xvzf <esd_filename>.tar.gz
```

and pressing the Enter key.

*where*

**<esd_filename>**
is the ESD filename for the GWC software load

**Example**
**$ gtar xvzf GWCC0070.70.V.NCL.NAP.VAULT.8.D.tar.gz**

*The ESD software load is uncompressed, and a new directory named after the ESD software filename is created. The directory name is the name of the ESD filename without the .tar.gz suffix. The contents of the ESD software load are placed in this new directory.*

10 Access the newly created directory by typing

```
$ cd <esd_filename_directory>
```

and pressing the Enter key.

*where*

**<esd_filename_directory>**
is the new directory created to store the extracted software load

**Example**
**$ cd GWCC0070.70.V.NCL.NAP.VAULT.8.D**

11 Become the root user by typing

```
$ su - root
```

and pressing the Enter key.

12 When prompted, enter the root password.

13 The ESD software is formatted as an ISO 9660 image. Mount the ISO 9660 image (using the mount_iso.ksh script) by typing

```
# /opt/nortel/sspfs/Scripts/mount_iso.ksh mount
/data/iso_esd/<esd_directory>/<iso_image>.img.
tape
```

and pressing the Enter key.

*where*

**<esd_directory>**
is the directory created in step 9

**<iso_image>**
is the name of the iso image

***Note:*** A space is required after the word mount and before the word /data.

**Example**
**# mount_iso.ksh mount**
**/data/iso_esd/GWCC0070.70.V.NCL.NAP.VAULT.8D/**
**GN070_load.iso.tape**

*A response is printed to the terminal. Use following table to determine if the command was successful.*

### mount_iso.ksh command responses

| Response | Meaning and action |
|---|---|
| `Is is very important for the user of this command to know that if you mount an iso image. It is a MUST that you umount an image before removing the image file. If the file is deleted while the OS has it mounted, it can be harmful to the runtime applications on this unit` | This response indicates success. |
| `Provided full path to ISO image does not exist` | Verify the location and name of the ISO 9660 image, such us /data/iso_esd/GWCC007.../...img.tape, and retry. |
| `ISO Image Already Mounted` | Enter **mount_iso.ksh umount** to unmount whatever ISO 9660 image is currently mounted, and retry. |
| `Error creating the image device location` | This response indicates an operating system error with the loopback file driver. Retry the command, and if it fails a second time, contact Nortel Networks support personnel. |
| `ERROR MOUNTING <ESD_filename>` | This response indicates that either the ISO 9660 file is corrupt, or the `/tmpmnt/noarch` directory has been deleted. |

*The contents of the ESD software file are available in directory `/tmpmnt/noarch`.*

**14** Use the following table to determine your next step.

| If you want to install the software | Do |
|---|---|
| later | go to step 15 |
| now | go to step 16 |

**15** Copy the contents to a location on the CS 2000 Management Tools server by typing

```
# cp /tmpmnt/noarch/*.* <directory_name>
```

and pressing the Enter key.

*where*

**<directory_name>**
is a directory on the CS 2000 Management Tools server, for example /data/iso_esd

***Note:*** Ensure that you have write permission to this directory, and that the same file permissions are set at the old and copied locations.

When installing the software at the later date, complete step 16, but in sub-step e, specify the new location of the software instead of typing /tmpmnt/noarch.

Continue with step 23.

**16** Complete the following steps to install the software on the CS 2000 Core Manager or CBM.

**a** List the contents of the /tmpmnt/noarch directory by typing

```
# ls /tmpmnt/noarch
```

and pressing the Enter key.

Record the name of the .rpm file.

**b** Execute the installation script by typing

```
# platform_load_install.sh
```

and pressing the Enter key.

**c** When prompted, select the option "Install RPM from Disk" by typing

```
> 2
```

and pressing the Enter key.

**d** When prompted, enter the .rpm filename and press the Enter key.

e When prompted, enter the location of the .rpm file by typing

**# /tmpmnt/noarch**

and pressing the Enter key.

*The system installs the software on the CS 2000 Core Manager or CBM.*

*After the load file is installed on the CS 2000 Core Manager or CBM, the transferred .rpm package is deleted from the CS 2000 Core Manager or CBM.*

f Exit the installation program by typing

**# x**

and pressing the Enter key.

| If your office is configured with a | Do |
|---|---|
| CS 2000 Core Manager | go to step 17 |
| CBM | go to step 23 |

***At the CS 2000 Core Manager console or terminal window***

**17** Log in to the CS 2000 Core Manager as the root user.

```
AIX Version 4
 (C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

**18** Access the gwc directory by typing

**# cd /swd/gwc**

and pressing the Enter key.

**19** Execute the GwcConfig.sh script by typing

**# ./GwcConfig.sh**

and pressing the Enter key.

***Note:*** The script checks if the appropriate configuration data is present in the gwc directory. If the data is not present, the system prompts you to enter the hostname and the IP address of the SAM21 EM server.

**20** If prompted, enter the hostname of the SAM21 EM server and press the Enter key. Otherwise, continue with step 22.

**21** If prompted, enter the IP address of the SAM21 EM server and press the Enter key. Otherwise, continue with step 22.

**22** Log out of the CS 2000 Core Manager by typing

```
# exit
```

and pressing the Enter key.

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

**23** Unmount the ESD file by typing

```
# mount_iso.ksh umount
```

and pressing the Enter key.

**24** This procedure is complete.

# Upgrade a standby GWC card software load

## Purpose of this procedure

This procedure describes how to upgrade the software load that GWC cards boot from, located on the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM).

## When to use this procedure

Use this procedure after installing a newer version of the GWC software load onto the CS 2000 Core Manager (SDM) or CBM. This procedure must be applied to each node installed in the SAM21 shelf that is being upgraded.

## Prerequisites and guidelines



**CAUTION**

No provisioning activity can occur on the system while the GWC software upgrade is in progress.

The GWC software load filesets must be installed on the CS 2000 Core Manager (SDM) or CBM. Refer to one of the following procedures:

- Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 841
- Deliver and install GWC package using Electronic Software Delivery on page 846

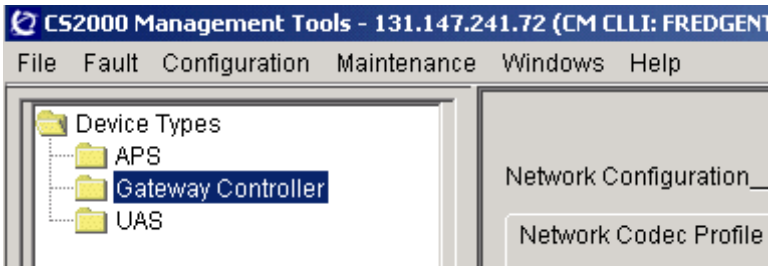
While upgrading the software on a GWC card, the port on the LAN router connected to the GWC card must be set to the Ethernet parameter of “auto-negotiate”. This action must be performed after the card is locked and before the card is unlocked. Refer to step 9 in this procedure.

If the Communications Server LAN (CS LAN) is provided by Nortel Networks Passport 8000 series router switches, refer to Re-provision Passport port to auto-negotiate on page 867 for a procedure to reconfigure the port on the CS LAN router to “auto-negotiate”.

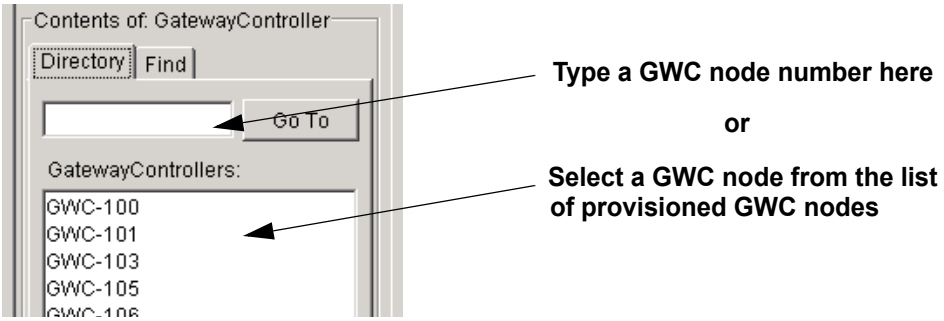
## Action

### *At the CS 2000 GWC Manager client*

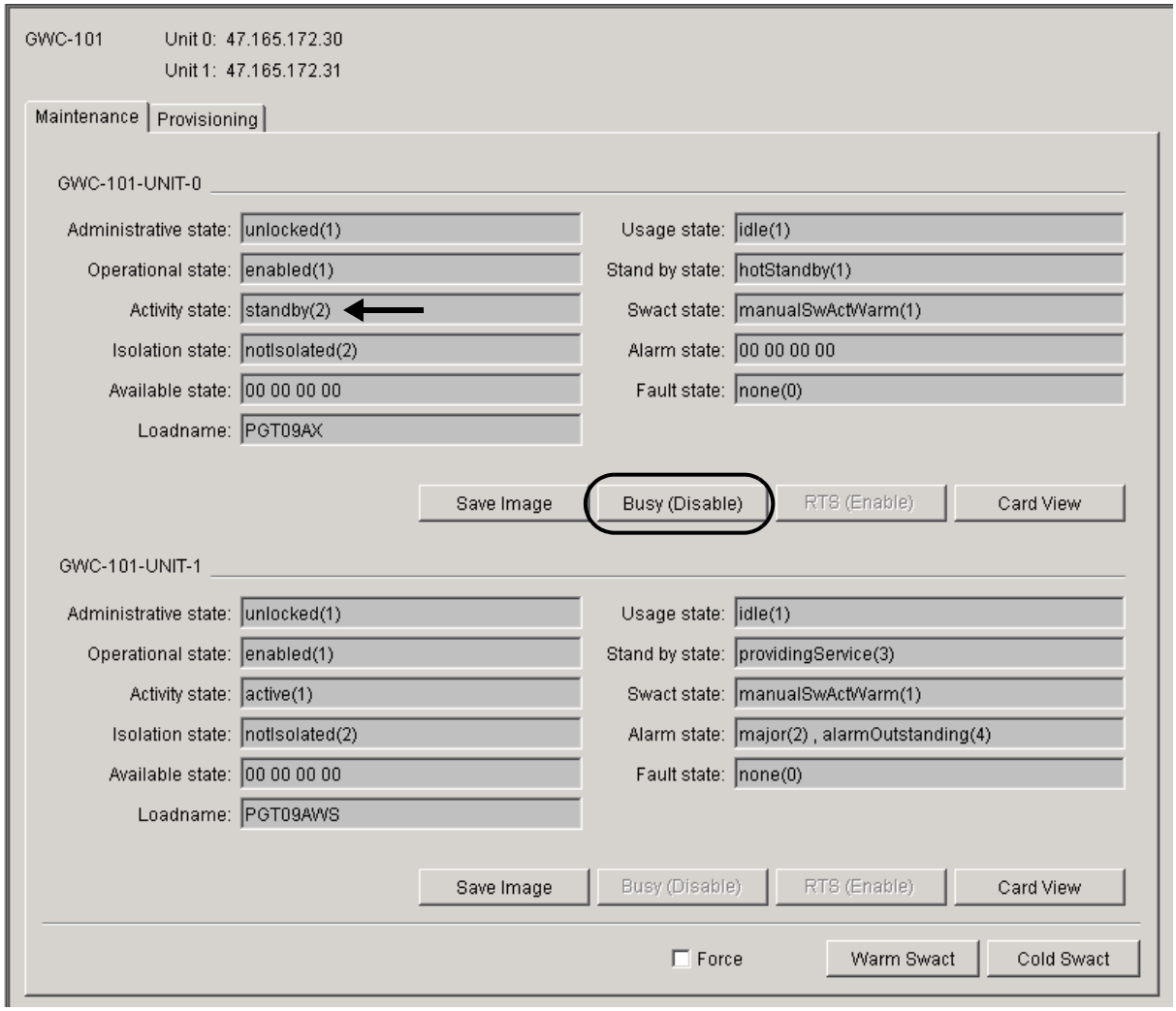
**1** At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types directory tree in the far left frame.



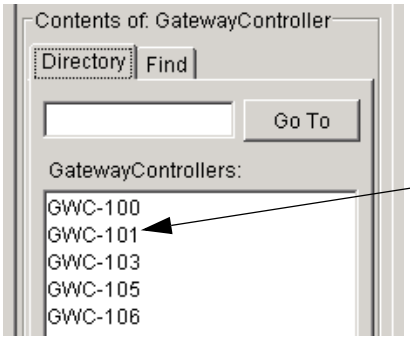

**2** From the Contents of: Gateway Controller frame, select the GWC node that you wish to busy for an upgrade.



**3** Busy the standby GWC card in the node to upgrade by clicking the **Busy (Disable)** button. Confirm this action at the prompt.




**4** From the Contents of: Gateway Controller record the GWC node number for the GWC card you just busied. You will need this information later in this procedure.




**Record the GWC node number of the GWC card that you just busied.**

5 Use the following table to determine your next step.

| If | Do |
|---|---|
| you need to re-provision the port on the Passport switch to “auto-negotiate” (the CS LAN is provided by Nortel Networks Passport 8000 series router switches) | go to step 6 |
| otherwise | go to step 7 |

***At the CLI for the Passport***

6 Determine the slot and port on the Passport that connects to the device by typing

**> show ip arp info <ip_address>**

and pressing the Enter key.

**ip_address**
is the physical IP address of the GWC card.

The slot and port are reported. Record the slot and port number. You will need this information later in this procedure.

*Example response:*

```
prompt:cpu> show ip arp info 172.30.242.25
================================================================================
                                      Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL
--------------------------------------------------------------------------------
172.30.242.25    00:90:69:1a:d4:fc   200   1/2   DYNAMIC 272
```

***Note:*** *If the response indicates MLT instead of the slot and port, perform this operation from the mate Passport unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.*

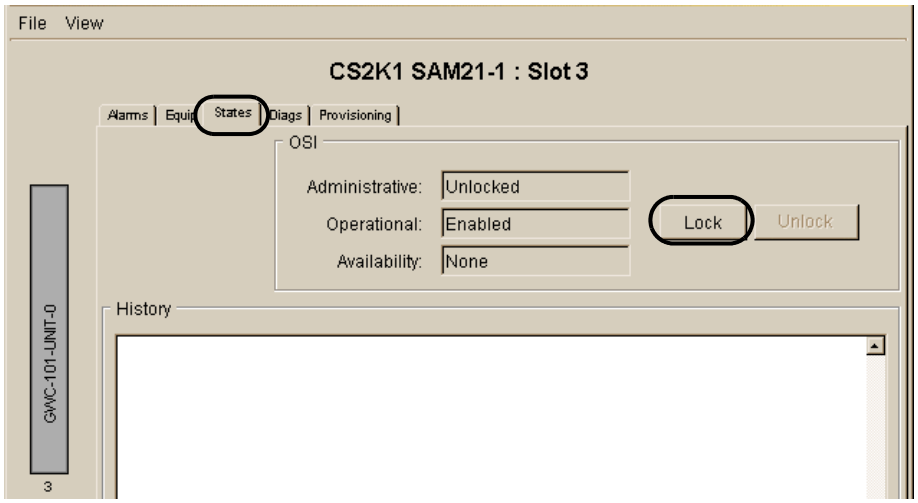
### *At the CS 2000 GWC Manager client*

**7** Click the **Card View** button for the card you busied in step 3. This action opens the CS 2000 SAM21 Manager.



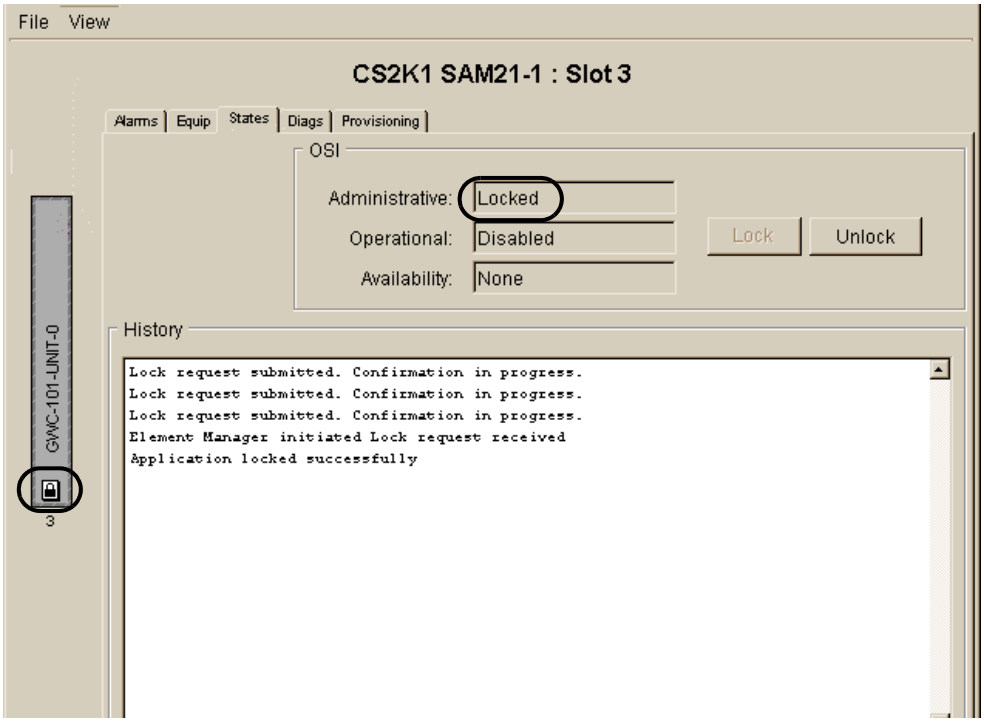

### *At the CS 2000 SAM21 Manager client*

**8** In the card view, select the **States** tab and then click the **Lock** button to lock the card.

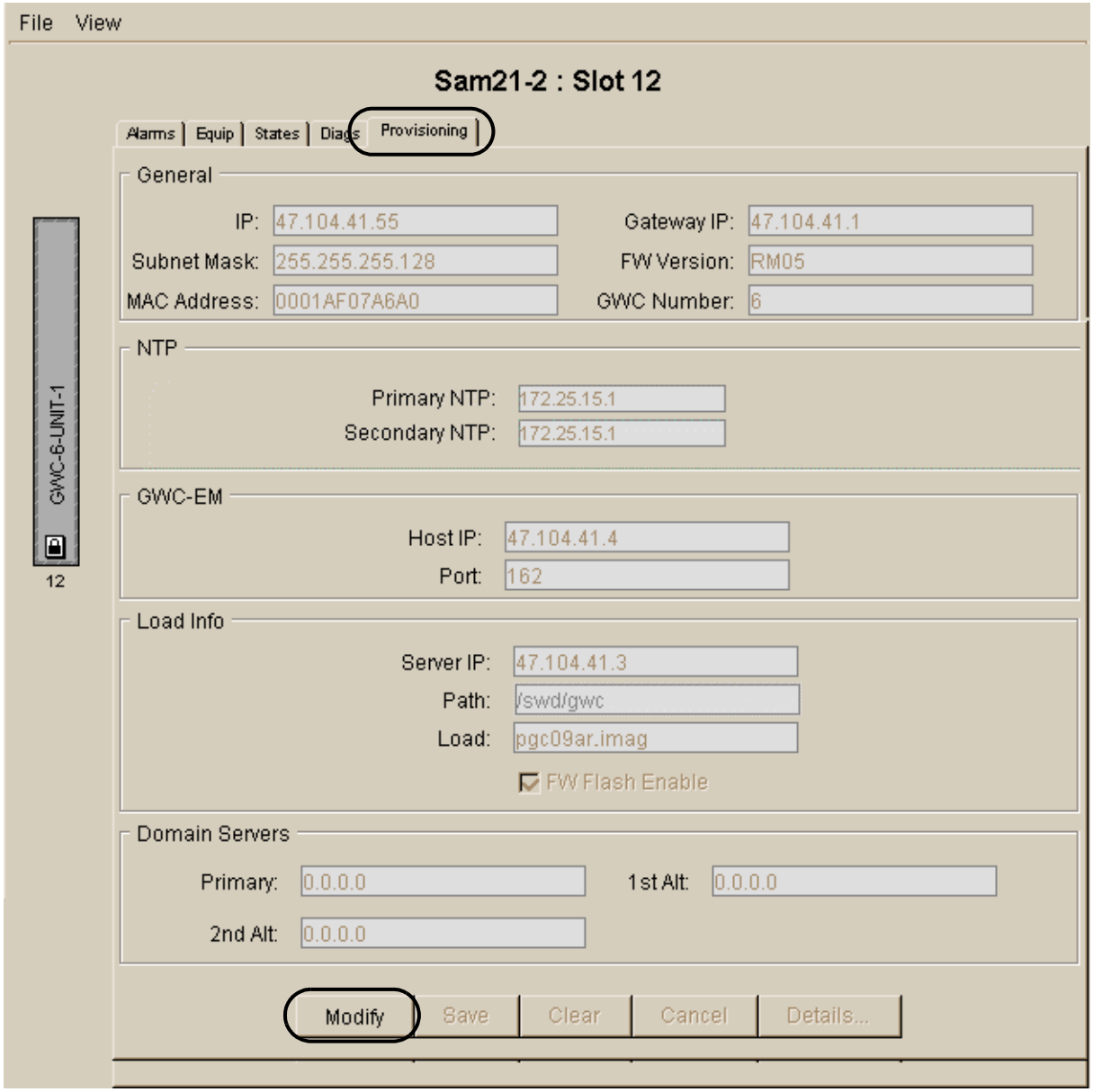


9 Observe the History display to confirm that the card has been locked. Look for the text “Application locked successfully”. Also, notice the lock icon on the card graphic at the left of the screen and the Administrative state “Locked”.

***Note:*** If the CS LAN is provided by Nortel Networks Passport 8000 series router switches, re-provision the port on the Passport switch to “auto-negotiate”. Refer to Re-provision Passport port to auto-negotiate on page 867.



**10** Select the **Provisioning** tab and click the **Modify** button to make changes to the load file name.



**11**

**CAUTION**

The Path: field must be set to /swd/gwc.

Other processes are tied to this directory. For example, the GWC load delivery software places the load in the /swd/gwc directory. Also, GWC auto-imaging is a network file system (NFS) mount of the /swd/gwc directory.

Type the new load file name in the **Load:** field.

***Note:*** Ensure that the FW Flash Enable check box is selected.

**12** Use the following table to determine your next step.

| If | Do |
|---|---|
| field **GWC Number:** is blank or the current value of the field does not match the number recorded in step 4 | go to step 13 |
| otherwise | go to step 14 |

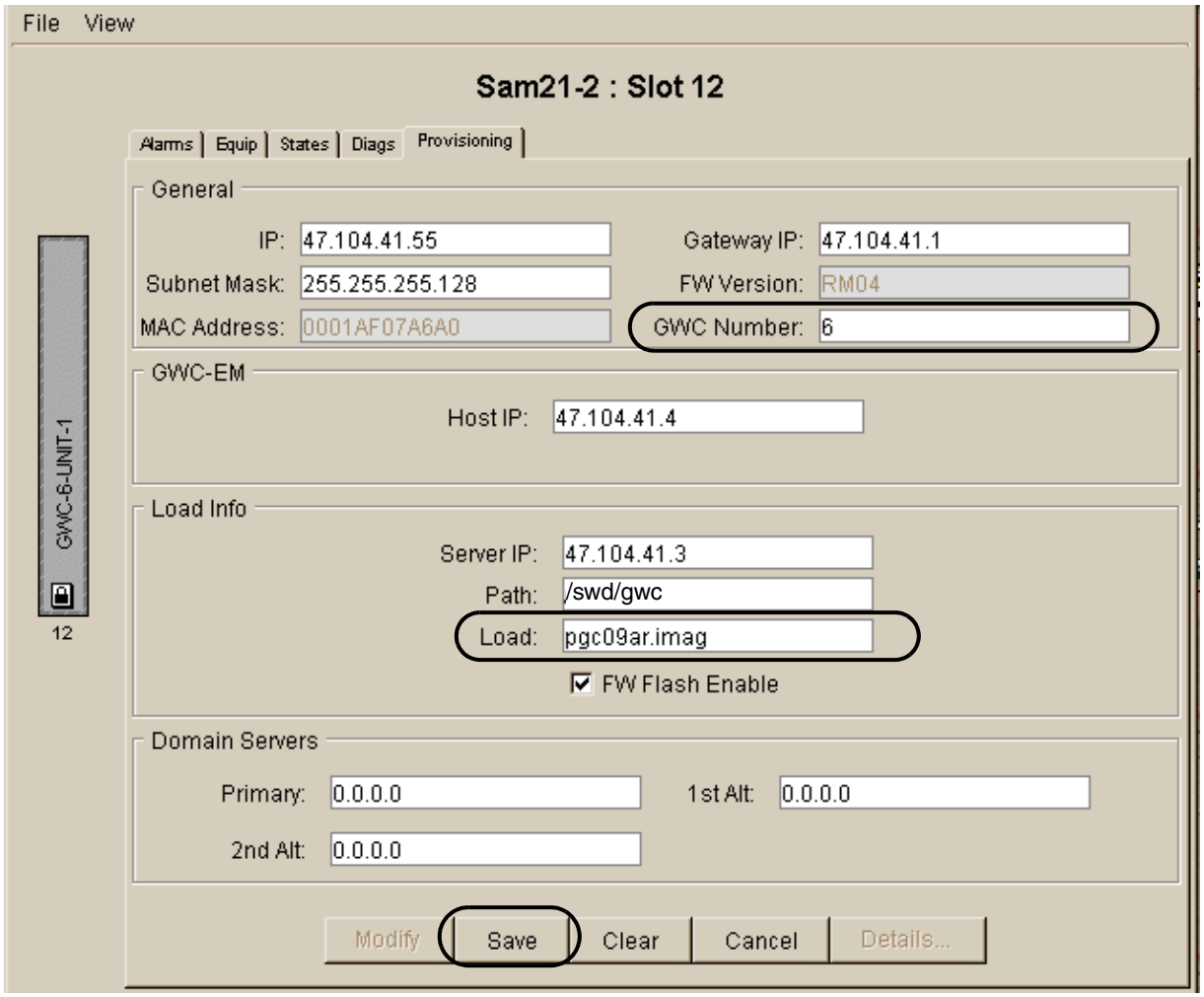
**13** Type the GWC number in the **GWC Number:** field that you recorded in step 4. Refer to the following figure to locate these fields.

***Note:*** Beginning in SN05 and going forward, there is a requirement to enter the GWC number into this field which is used to label the GWC in the CS 2000 SAM21 Manager shelf view panel. This number is manually assigned and no error checking is performed to ensure it matches with the number in the CS 2000 GWC Manager. A number from 0 to 255 can be assigned for each GWC pair in the node.

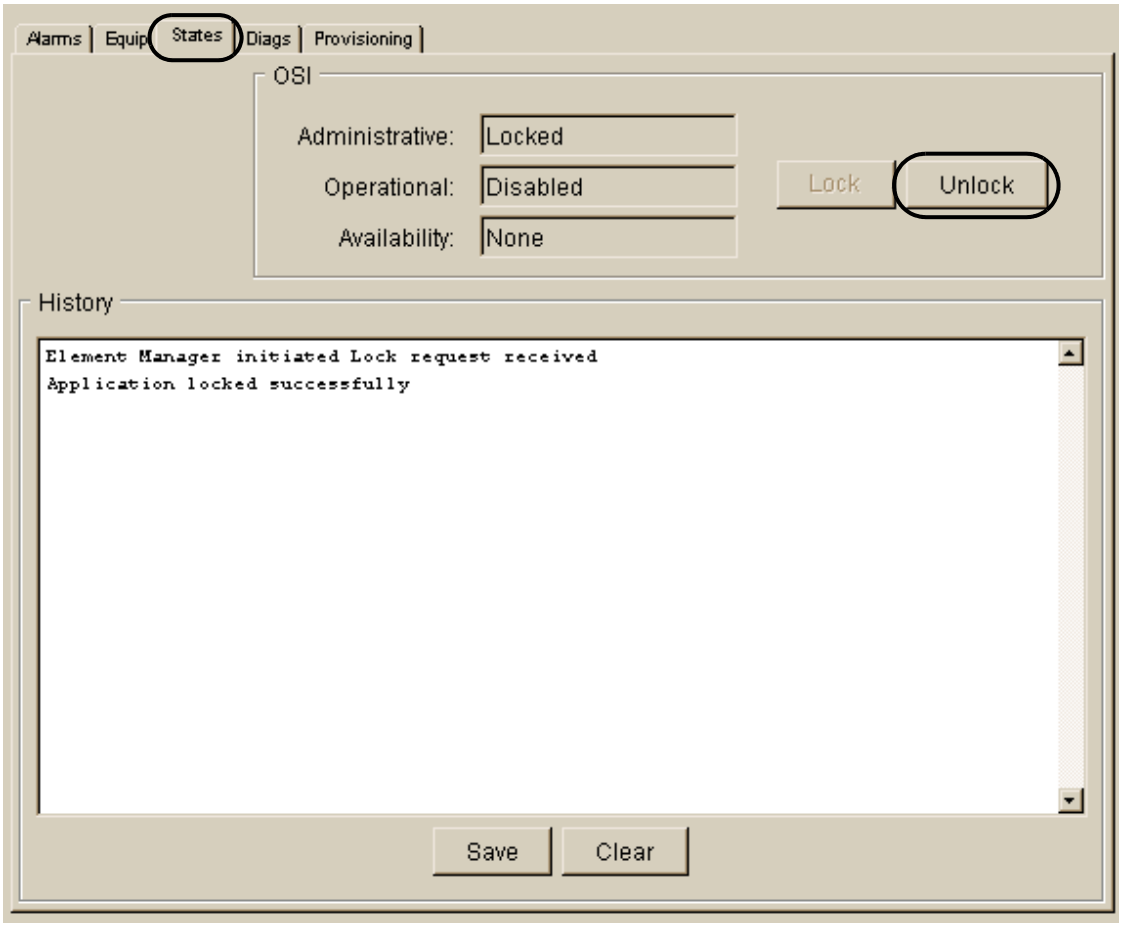
For example, if GWC cards in shelf slots 1 and 2 are paired together as a node, then during provisioning of these cards, the number 0 could be entered for each of these cards to identify that cards in slots 1 and 2 belong to GWC 0. Ensure that the GWC number entered at the CS 2000 SAM21 Manager matches the value given the cards in the CS 2000 GWC Manager as described in step 4.

**14** Click the **Save** button.

***Note:*** If the load name or path name are incorrect, you will be prompted with a “Load Validation Failure” message. You can choose to force the change or return to the provisioning panel to correct the error.



**15** Click the **States** tab to display the status of the GWC card.

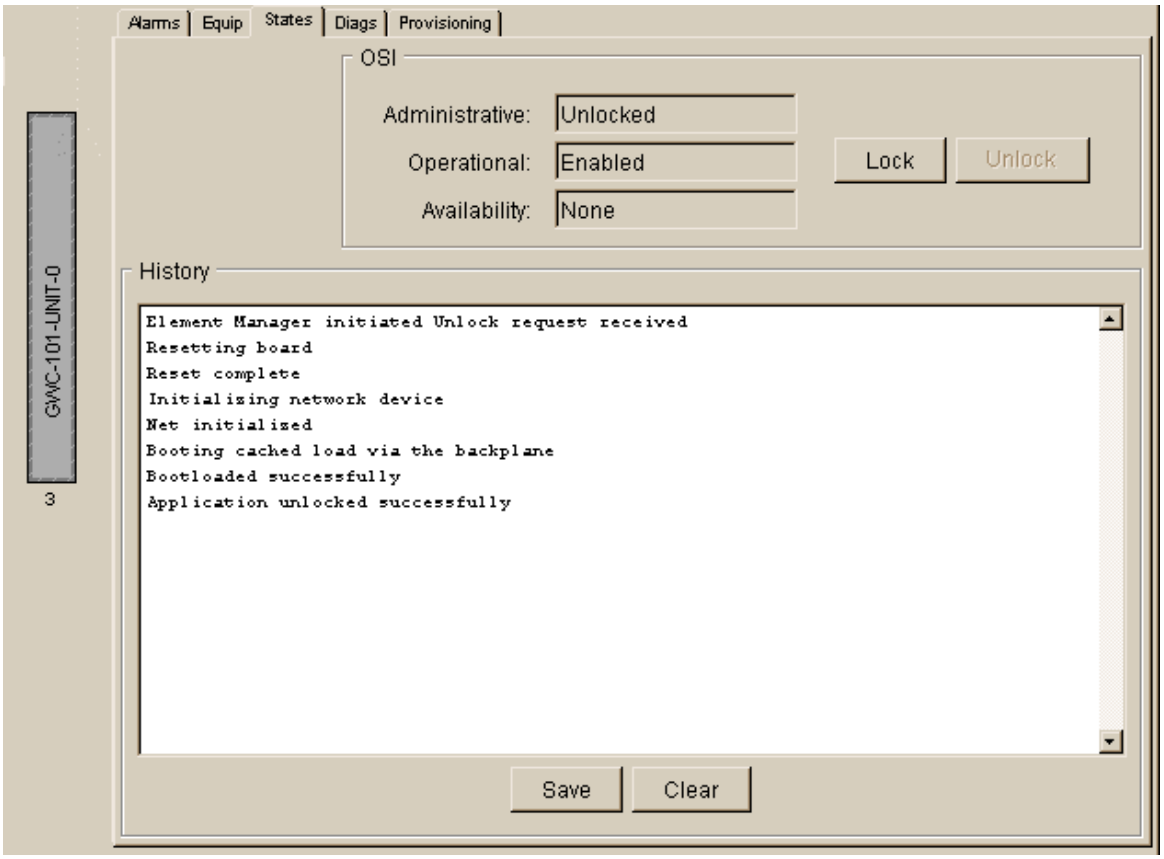


**16** Click the **Unlock** button to unLock the “Inactive” GWC card. This causes the card to reset and load from the new load image. The inactive unit should automatically return to service (RTS).

**17** Observe the History display until the screen message “Bootloaded successfully” appears.

***Note:*** If the card status does not display “Application unlocked successfully”, then click the **Lock** button in the card view and wait for the “Application locked successfully” message. Then, click the **Unlock** button again.

If you are still unable to successfully unlock a GWC card, contact your next level of support.



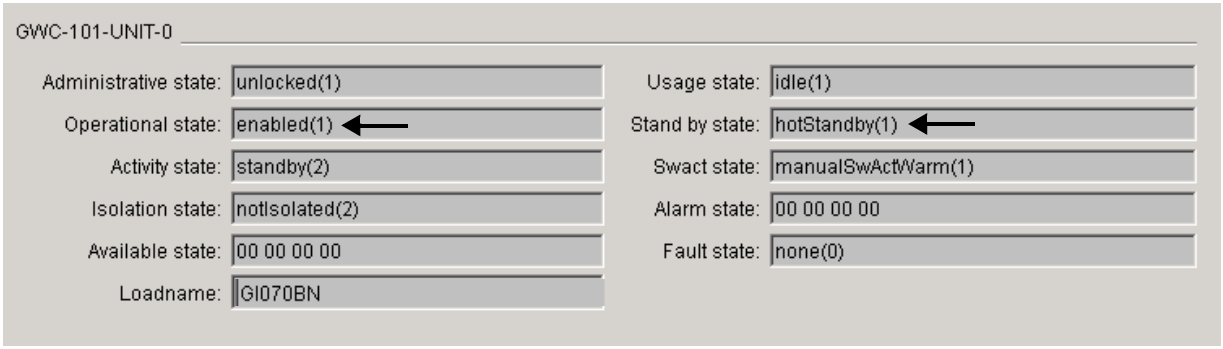
### *At the CS 2000 GWC Manager*

**18** Determine the next action to take.

| If patching | Do |
|---|---|
| is needed but has not been completed | perform the following procedures in the order listed, then continue with step 15:<br><br>Transferring patches to the NPM database manually on page 1664,<br><br>Applying patches using the NPM on page 1674,<br><br>Activating patches using the NPM on page 1690<br><br>Take a manual GWC software image on page 885; |
| has been completed | continue with step 19 |
| is not needed | continue with step 19 |

**19** Verify that the inactive GWC has an Operational State of “enabled” and a standby state of “hotstandby”.

If the inactive GWC does not come into an Operational State of “enabled” and a Standby state of “hotstandby”, then refer to the section “GWC does not RTS” in the “Troubleshoot GWC upgrades” section of “Upgrading the Gateway Contoller” NN10196-461. If error recovery fails, stop this procedure and contact your next level of support.

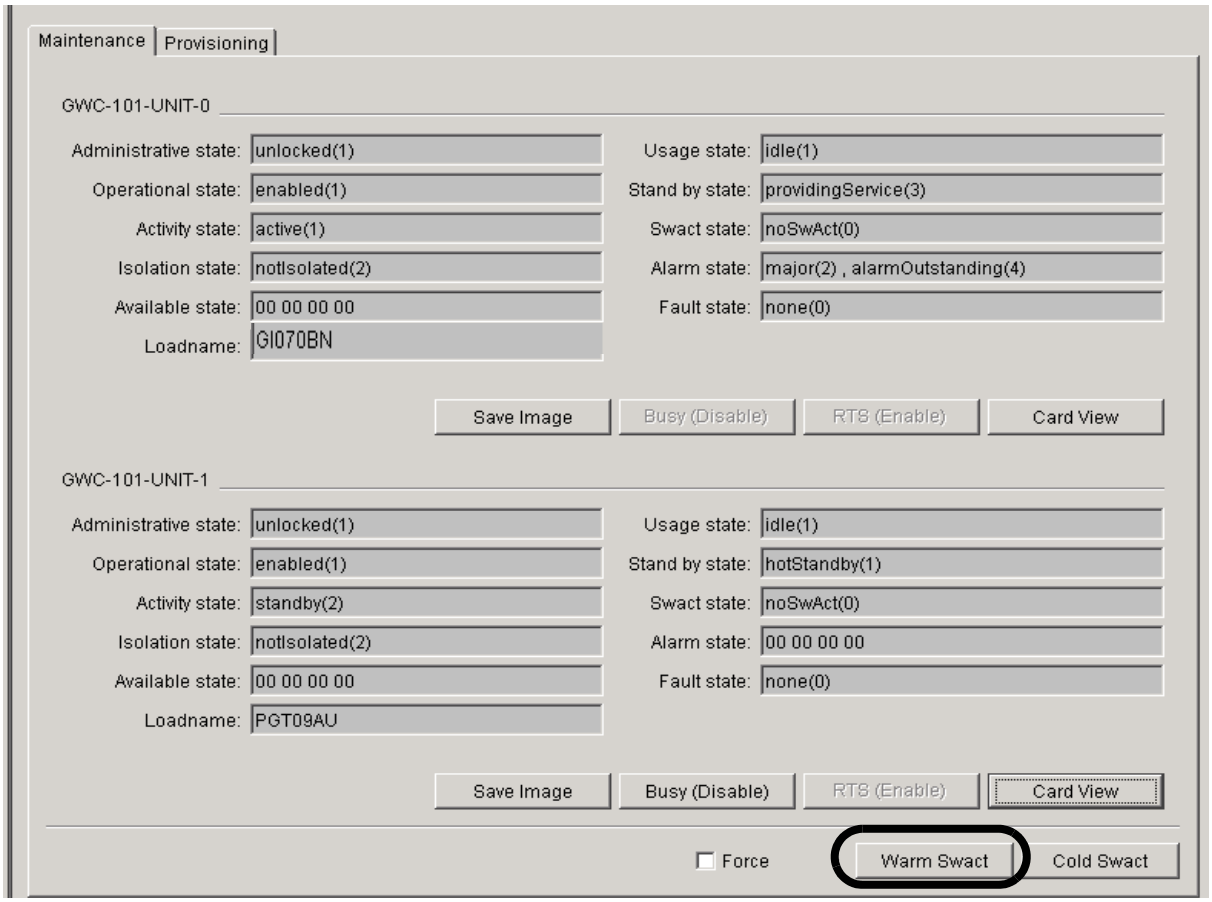


### *At the CS 2000 GWC Manager*

**20** Perform a Warm SwAct by clicking the **Warm Swact** button.

***Note:*** If the SwAct fails or the inactive unit does not RTS in 1 minute, then refer to the section “Warm SwAct Failed” in the “Troubleshoot GWC upgrades” section of “Upgrading the Gateway Contoller” NN10196-461.

If the GWC card does not successfully execute a warm SwAct using the Troubleshooting procedure, then perform the procedure rollback instructions located in “Upgrading the Gateway Contoller” NN10196-461.



**21** Determine your next action:

| If you need to upgrade | Do |
|---|---|
| the mate GWC card (now the new standby GWC card) in the same node | step 3 and complete this procedure |
| cards in another GWC node | step 2 and complete this procedure |

***Note:*** Otherwise, proceed to the next step. You only need to perform this procedure once for each card in a GWC node.

**22** The procedure is complete.

***Note:*** To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure on page 836.

## Re-provision Passport port to auto-negotiate

To enable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Passport router switch.

***Note:*** Make sure you use READ/WRITE/ALL (RWA) login and/or password privileges when performing this procedure. For more information about RWA privileges, refer to the Passport 8600 Routing Switch documentation and choose Getting Started.

### *At the CLI for the Passport*

**1** Use the numbers recorded in step 6 and set the slot and port to auto-negotiate by typing

**> config ethernet <slot>/<port> auto-negotiate enable**

and pressing the Enter key.

*The slot and port are reconfigured to auto-negotiate and the prompt returns.*

```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

2 Verify the port configuration by typing

**> show ports info config <slot>/<port>**

and pressing the Enter key.

*The slot and port configuration is displayed.*

```
prompt:cpu> show ports config info 1/2

================================================================================
                                    Port Config
================================================================================

PORT                 AUTO  SFFD  ADMIN       OPERATE     DIFF-SERV  QOS MLT
NUM   TYPE           NEG.        DUPLX SPD   DUPLX SPD   EN   TYPE  LVL ID
--------------------------------------------------------------------------------
1/2   100BaseTX      true  false  half  100   full  100   fals  core  1   0
```

3 Commit the change by typing

**> save config**

and pressing the Enter key.

4 Go to step 10 to continue with the procedure “Upgrade a standby GWC card software load”.

# 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 on page 836.

# Firmware flash a GWC card

## Purpose of this procedure

Use this procedure to flash the firmware of a GWC card when the version of firmware on the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM) is different from the firmware version on one or more GWC cards.

## When to use this procedure

Use this procedure when a new GWC firmware load has been delivered on the shelf controller tape (see release notes for the SAM21 shelf controller) and loaded on to the CS 2000 Core Manager or CBM. At this point, the firmware version on the GWC card needs to be upgraded.

***Note:*** This procedure flashes the firmware on the GWC card only if the version of the firmware on the CS 2000 Core Manager or CBM is different from the firmware version on the card. If you need to flash the firmware on a card that contains the same version of the firmware as the CS 2000 Core Manager or CBM, then refer to Force a firmware flash of a GWC card on page 877 in this NTP.

## Prerequisites

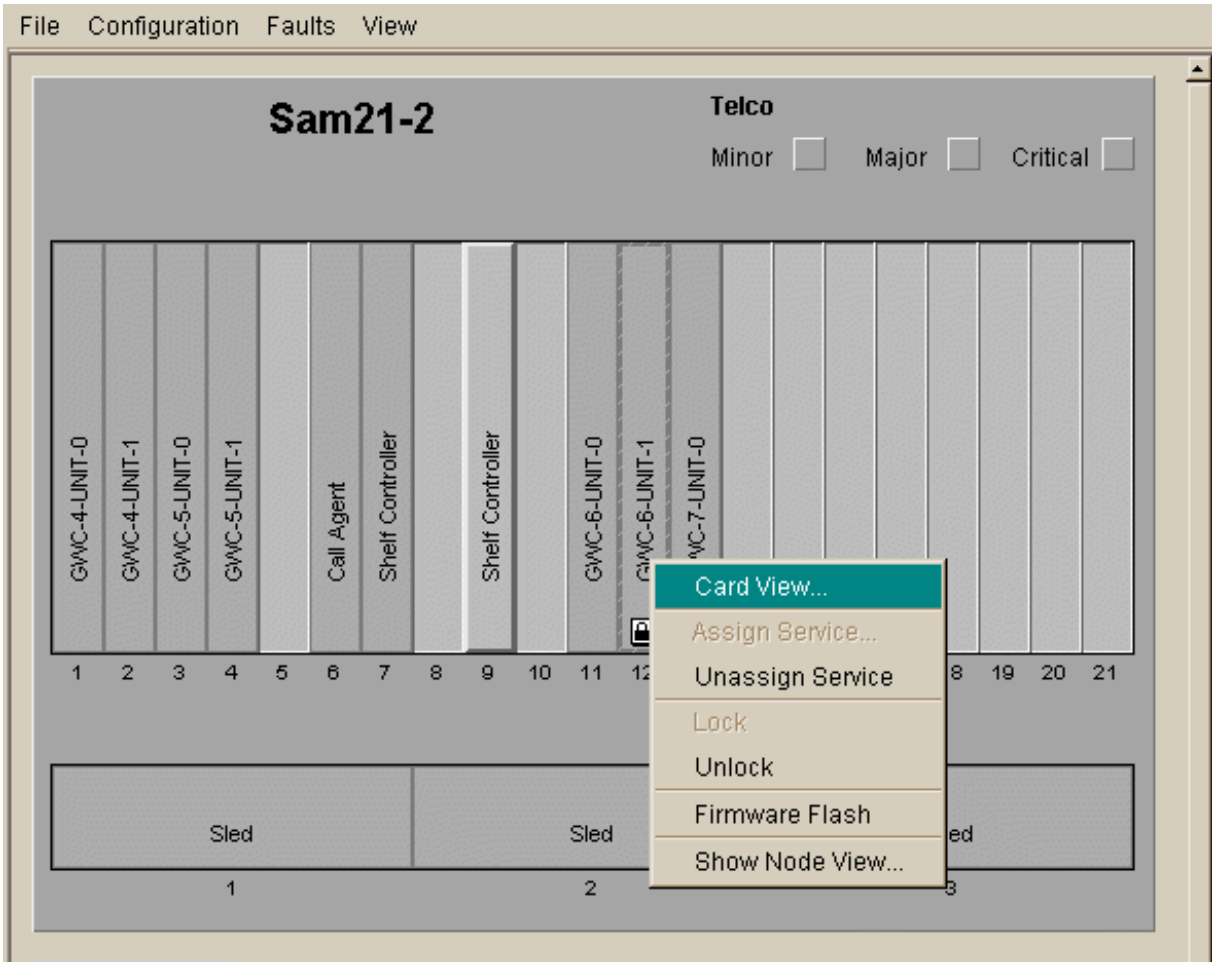
The GWC card you wish to flash must first be locked. Refer to the procedure "Lock a GWC card" in the Gateway Controller Security and Administration NTP, NN10213-611.

Locate the new firmware load for the GWC card that was delivered with the shelf controller software.

## Action

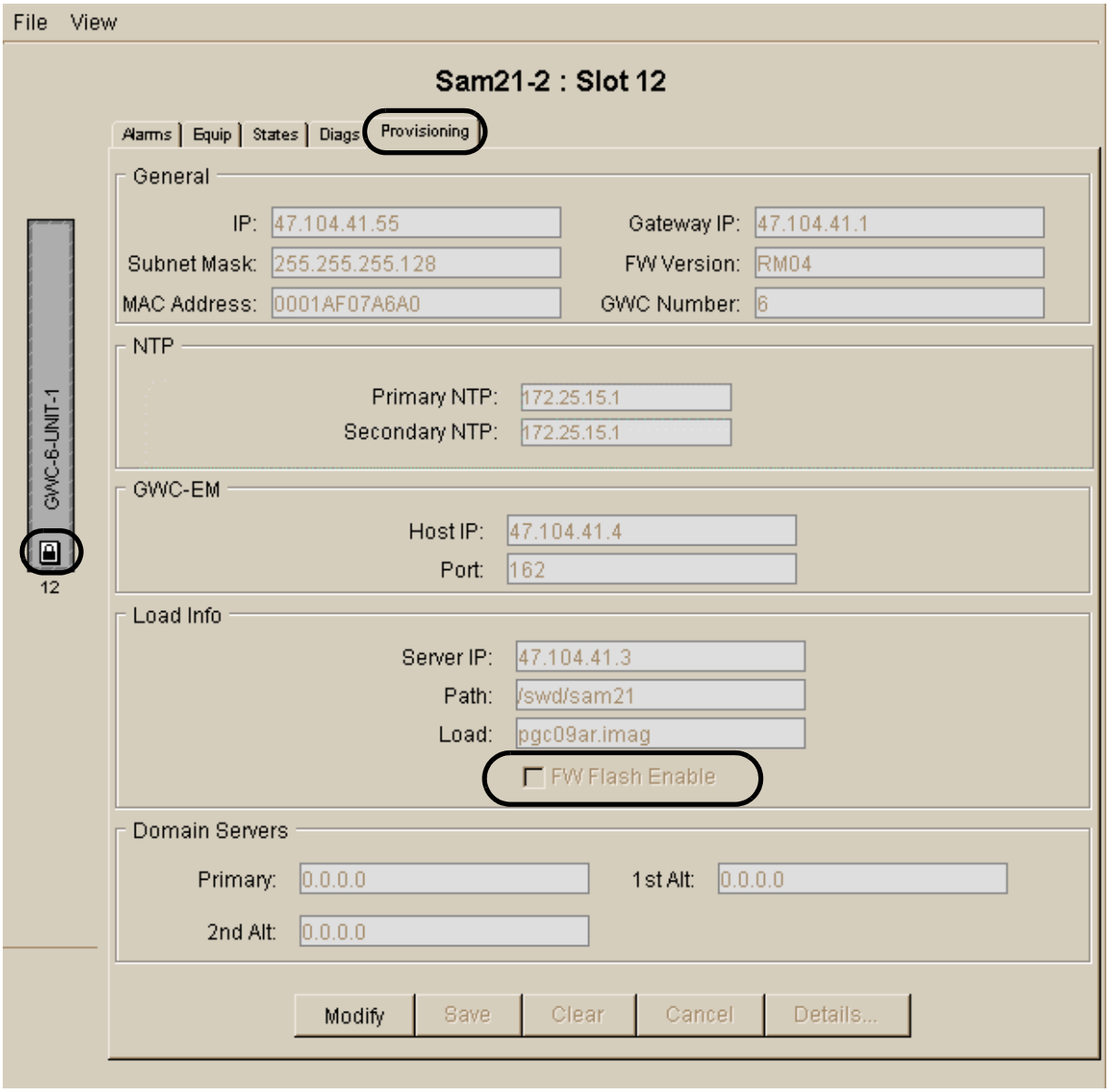
### *At the CS 2000 SAM21 Manager client*

**1** From the Shelf View window, right-click on the GWC card scheduled for flashing and select **Card View** from the pop-up menu.



2 Select the **Provisioning** tab in the Card View.

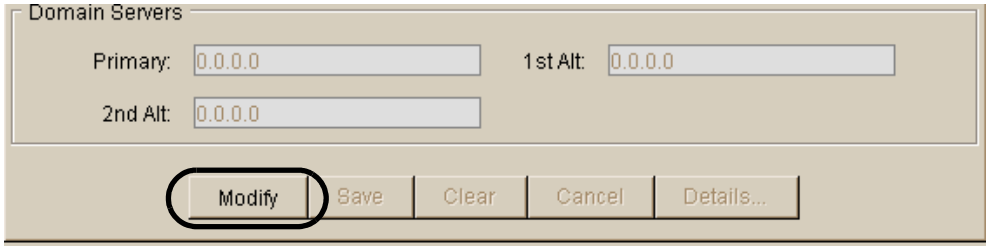
***Note:*** The lock icon should be displayed on the card graphic at the left of the screen. This indicates that the card is locked.



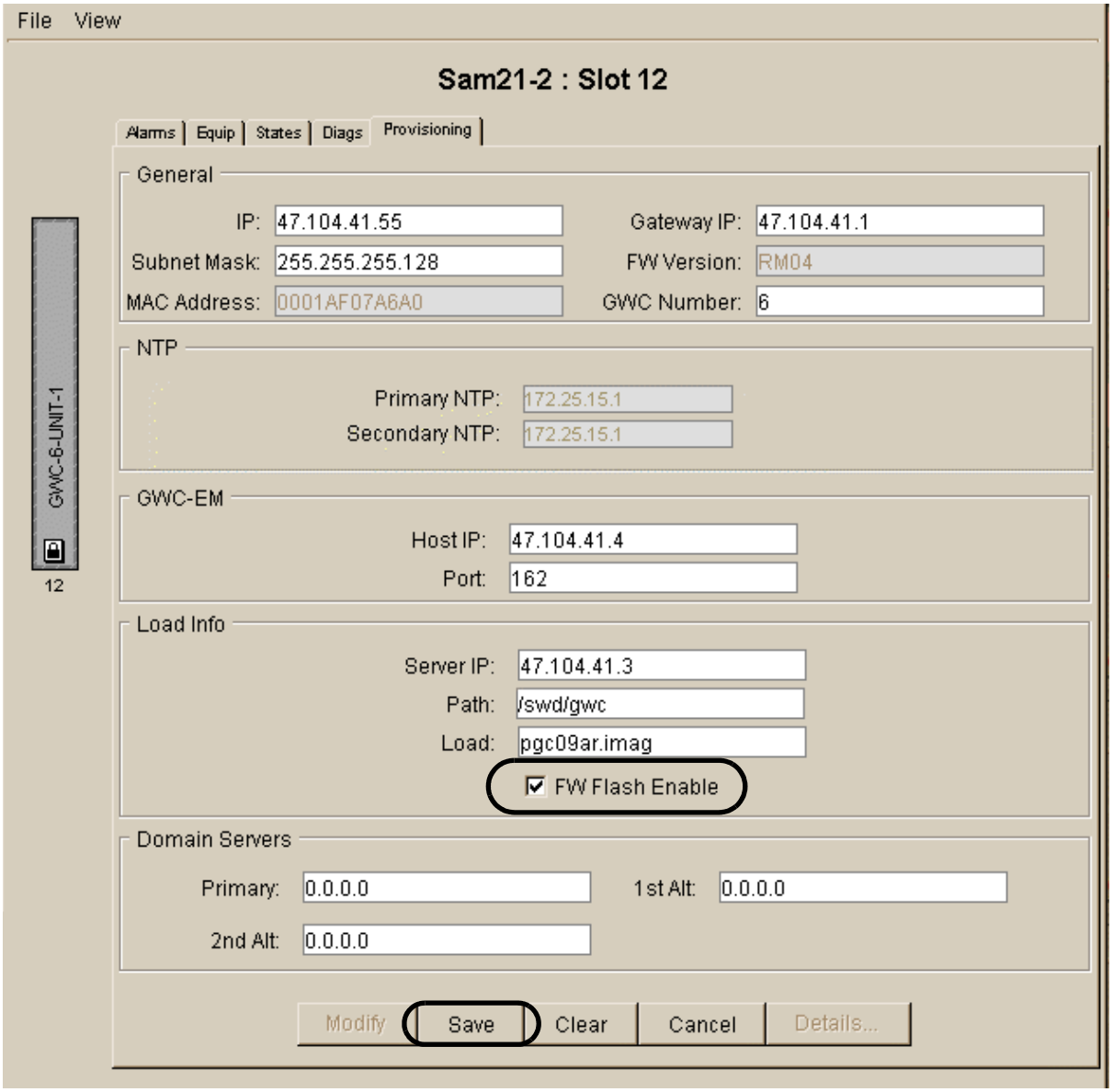

3 If the “FW Flash Enable” checkbox is already selected and a new firmware version is available, the process has already been started. Skip to step 7.

If the **Firmware Flash Enable** checkbox is not selected, continue with step 4.

**4** Click the **Modify** button at the bottom of the screen.




**5** Select the “FW Flash Enable” checkbox.

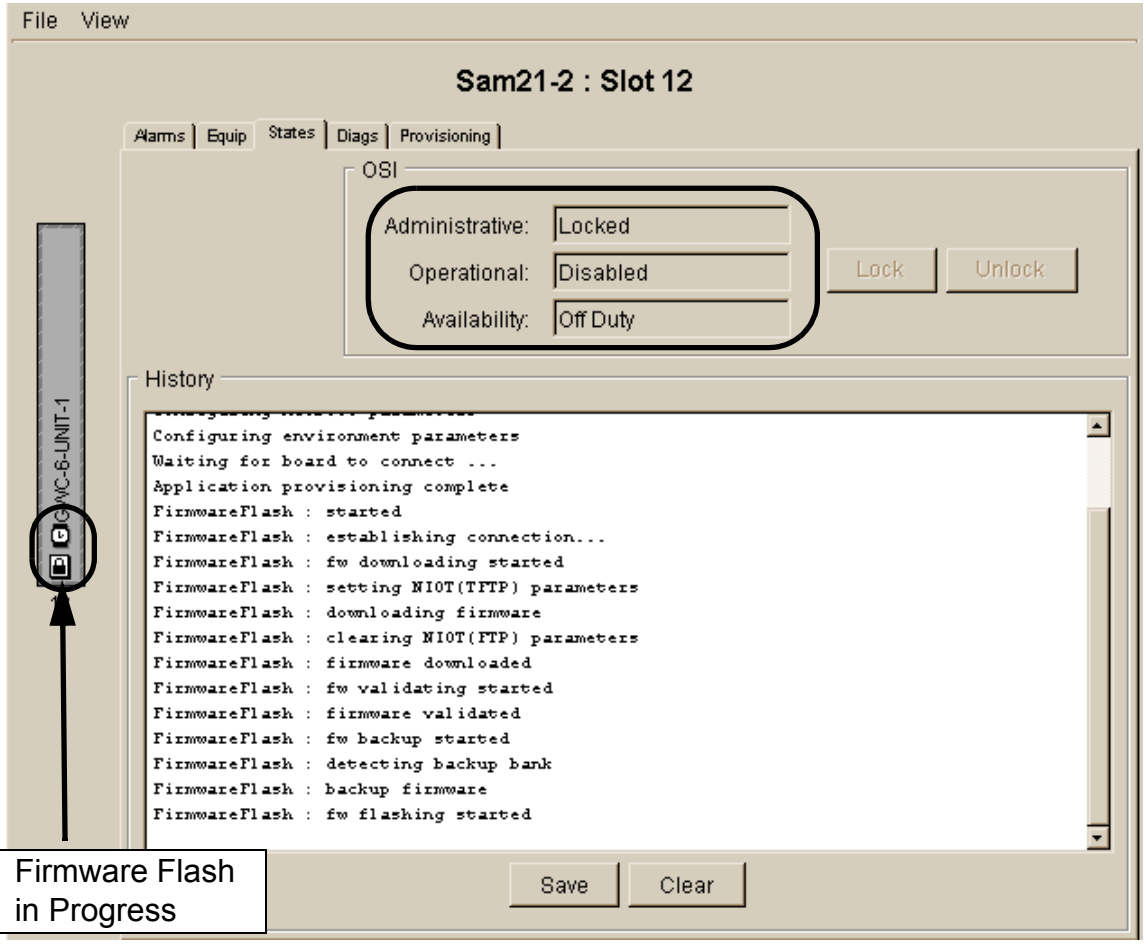


6 Click the **Save** button at the bottom of the screen.

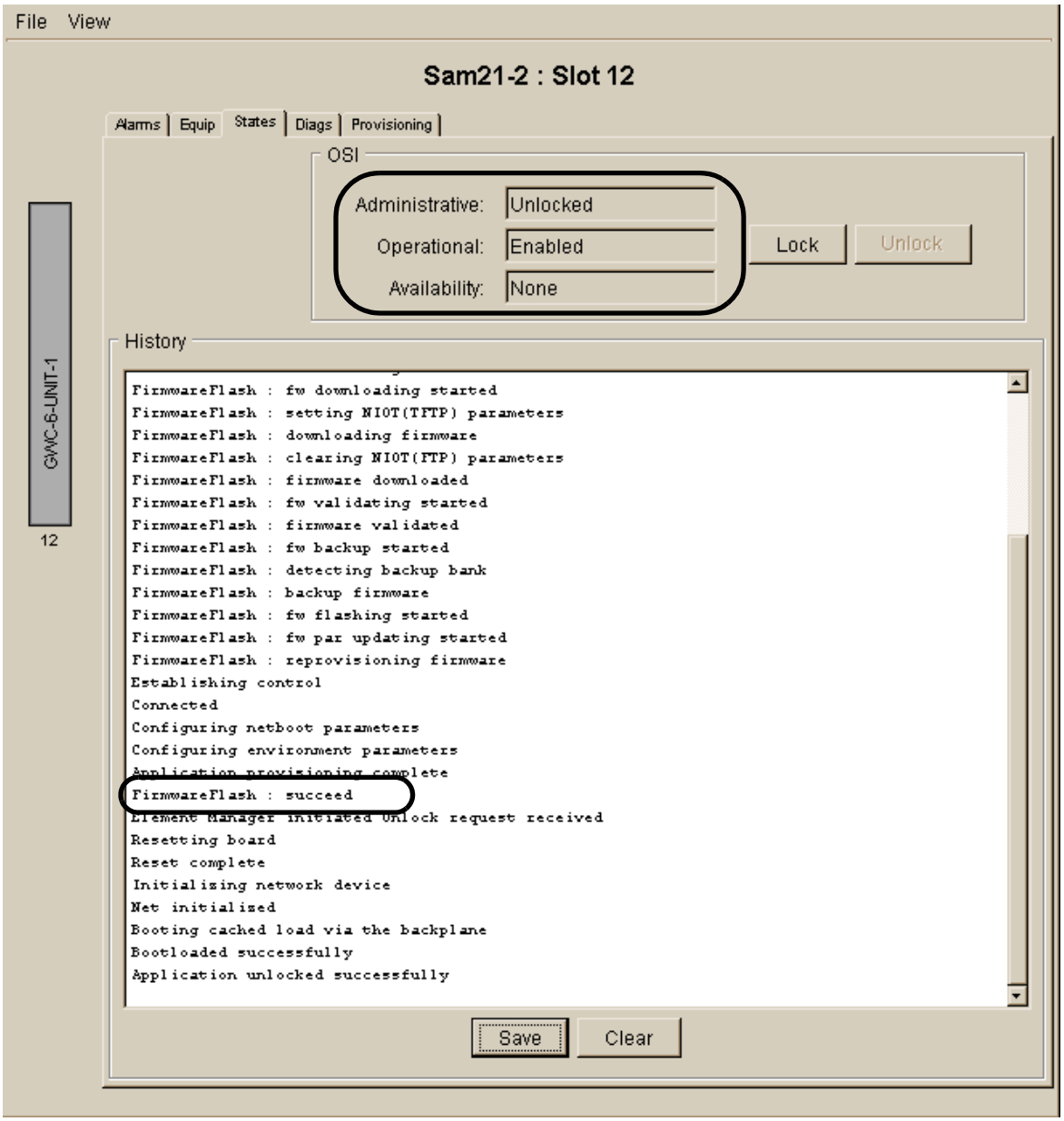
Firmware flashing will begin immediately if a new GWC firmware load is available.

7 Select the **States** tab in the card view.

Observe that the firmware flash icon appears on the GWC card graphic at the left of the screen during the firmware flash. Also observe the card state transition from "locked-disabled-none" to "locked-disabled-off duty". Observe the various firmware flash progress messages in the History window. (Your messages may vary from the graphic below.)



8 The firmware flash icon disappears once firmware flashing is complete. Verify that the firmware flash completed without errors by reviewing the text in the History window. Click the **Unlock** button to unlock the card.




9 Return to step 1 and repeat this procedure for other GWC cards requiring a firmware upgrade.

10 The procedure is complete.

# Force a firmware flash of a GWC card

## Purpose of this procedure

This procedure forces firmware flashing of a GWC card without any dependency on the firmware version on the card, or the firmware version on the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM). This procedure forces firmware flashing of a GWC card even when the CS 2000 Core Manager or CBM and the card have the same firmware version.

***Note:*** If you use the procedure Firmware flash a GWC card on page 871 in this NTP, you will not be able to flash a GWC card's firmware if it has the same firmware version as the CS 2000 Core Manager or CBM.

## When to use this procedure

Use this procedure when the firmware on a GWC card is corrupt, or when you suspect a problem with the firmware on a card. This procedure allows you to solve these problems by flashing the same version of the firmware on the CS 2000 Core Manager or CBM.

## Prerequisites

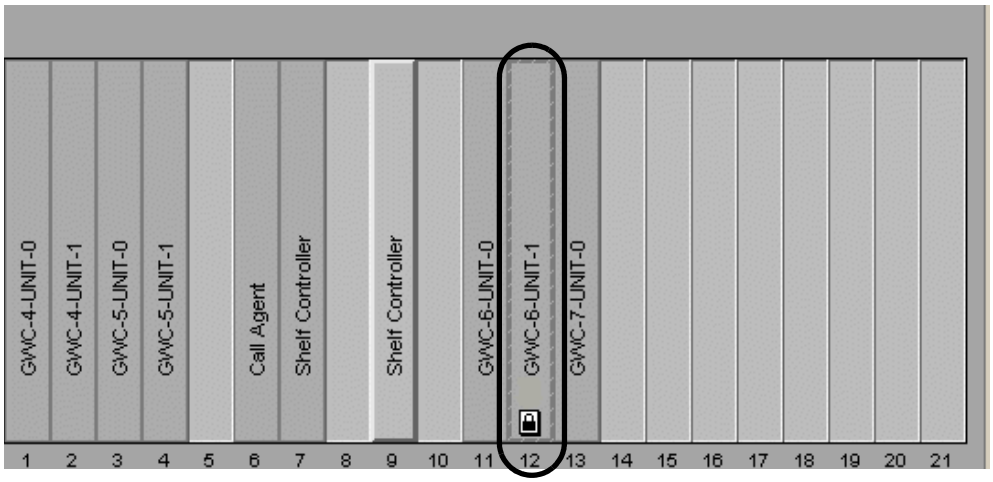
The GWC card you wish to flash must first be locked. Refer to the procedure "Lock a GWC card" in the Gateway Controller Security and Administration NTP, NN10213-611.

## Action

### *At the CS 2000 SAM21 Manager client*

**1** From the Shelf View window, confirm that the GWC card you want to flash is locked. The lock icon should appear at the bottom of the card.

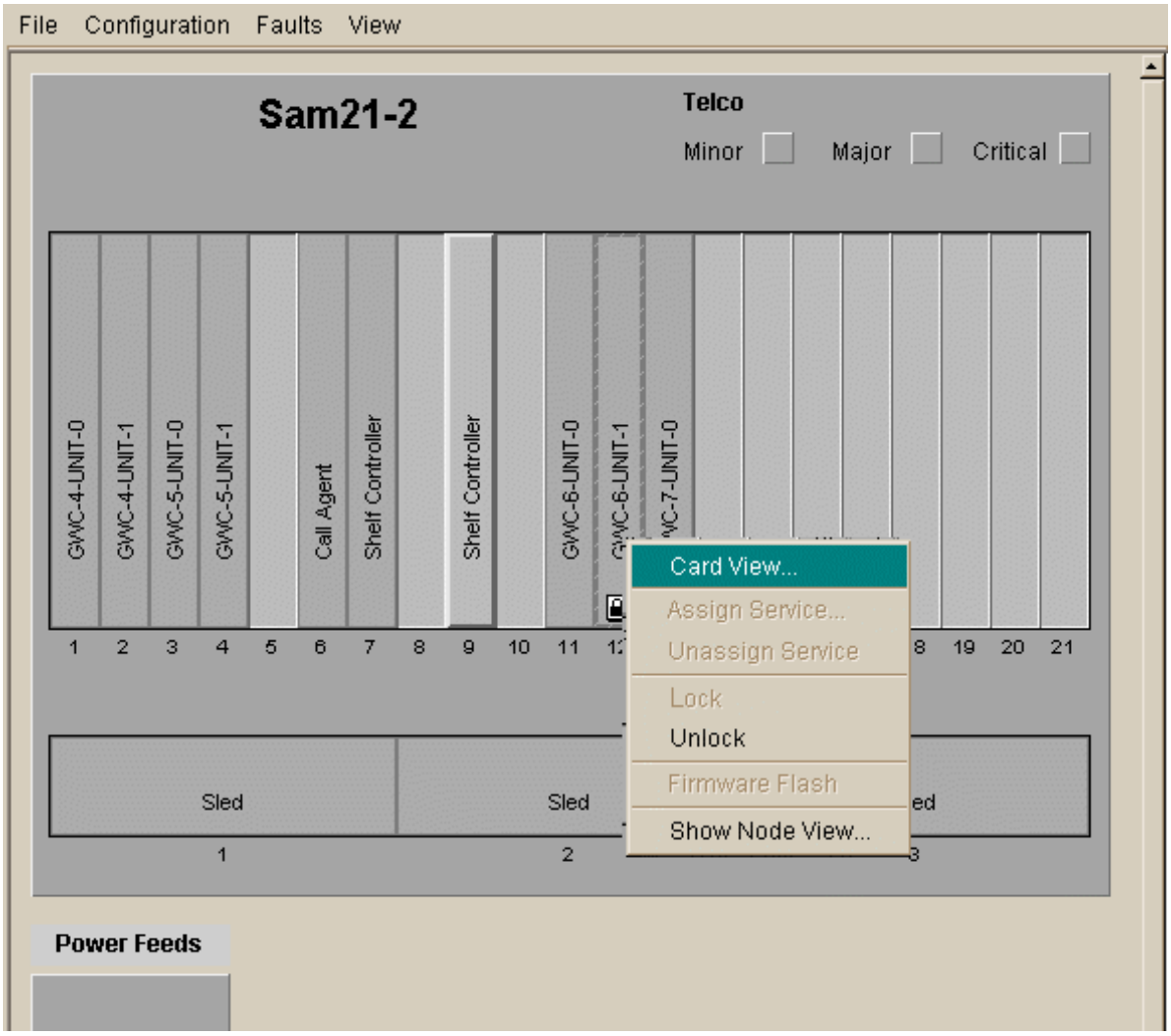
***Note:*** If you have just locked the card using the Card View, click on the **View** menu and select **Shelf View**.




**2** From the Shelf View window, right-click on the GWC card scheduled for flashing and determine your next action.

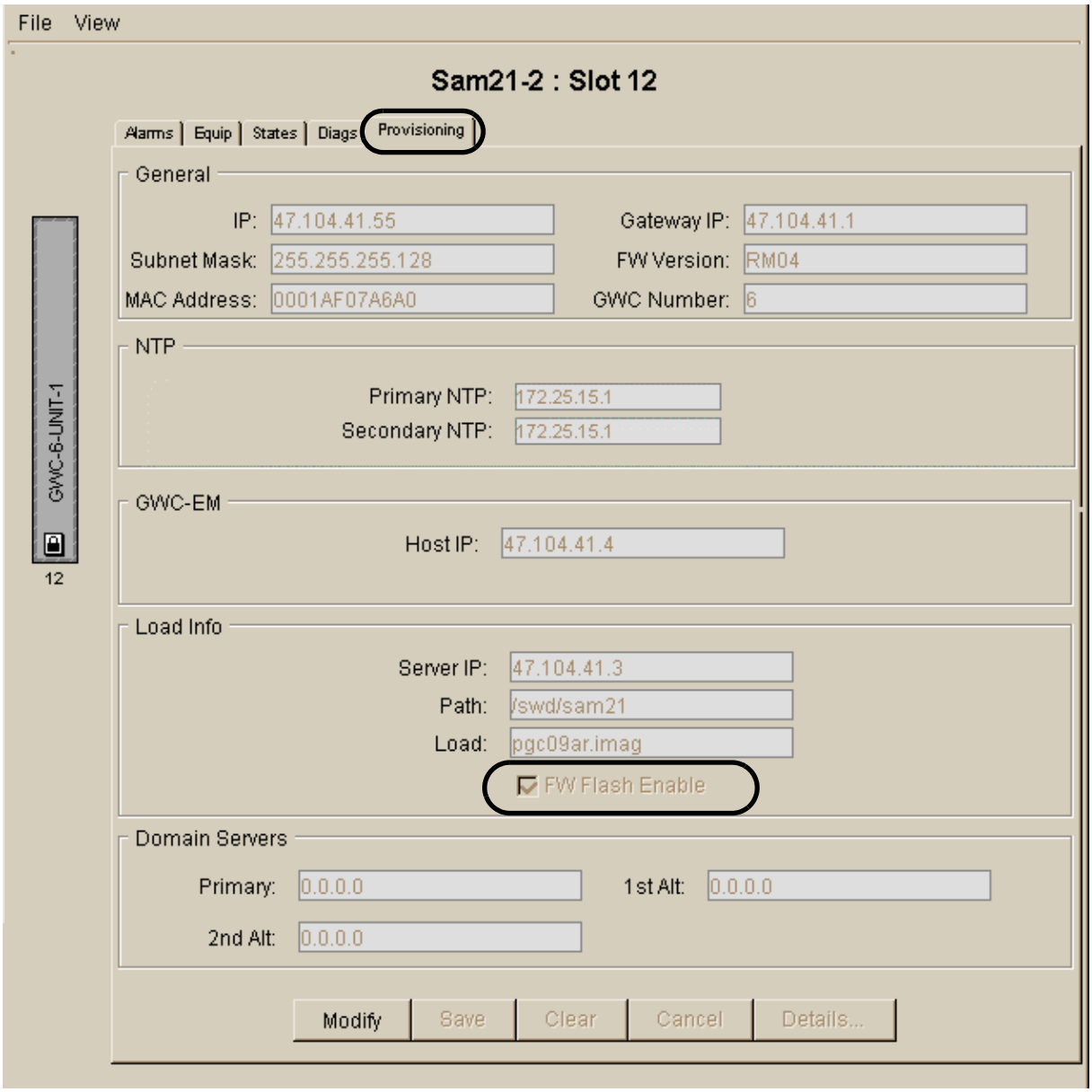
| If | Do |
|---|---|
| If the “Firmware Flash” option is available | skip to step step 8 |
| If the “Firmware Flash” option is not available (the text is faded in the pop-up menu) | go to step 3 |

3 From the Shelf View window, right-click the GWC card scheduled for flashing and select **Card View**.

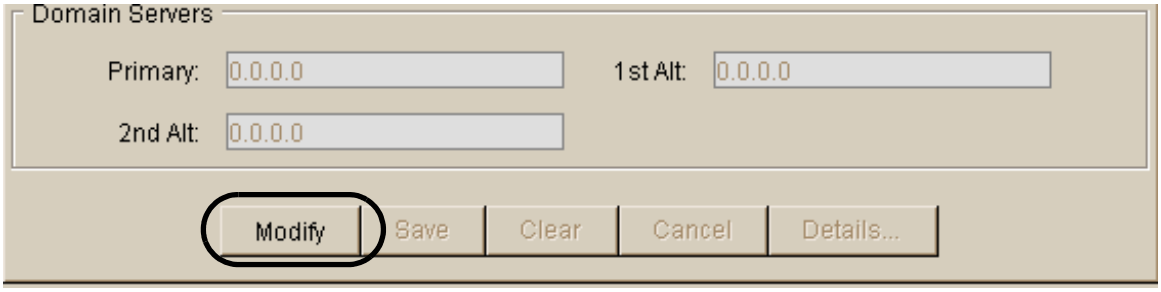


4 In the Card View, select the **Provisioning** tab.

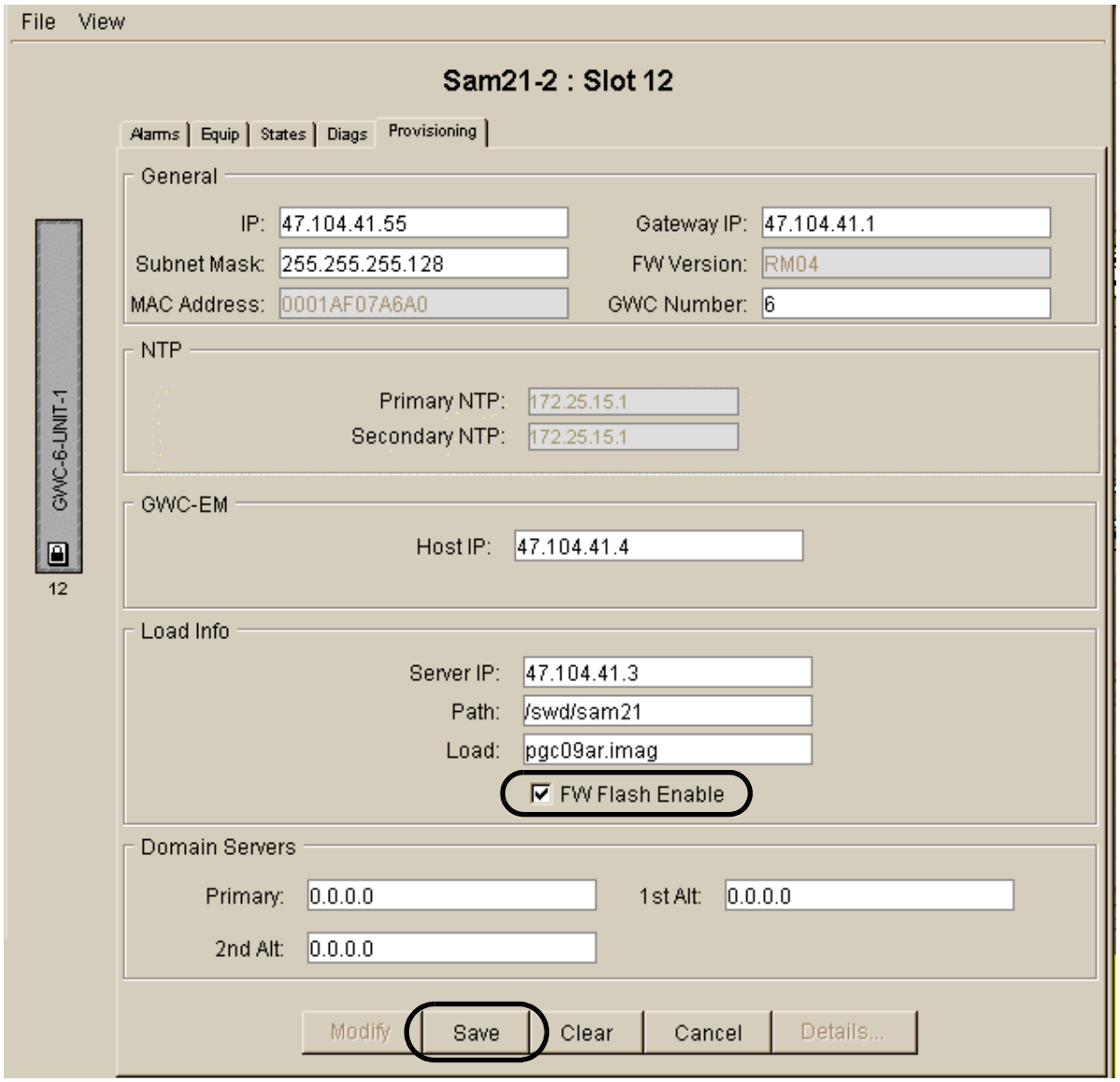
In the Provisioning panel, notice that the **FW Flash Enable** check box is selected. You cannot force a firmware flash if this option is selected.

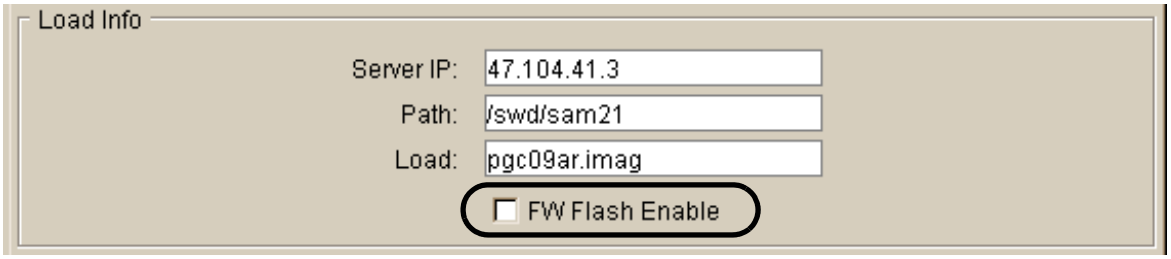


**5** In the Provisioning panel, click the **Modify** button.



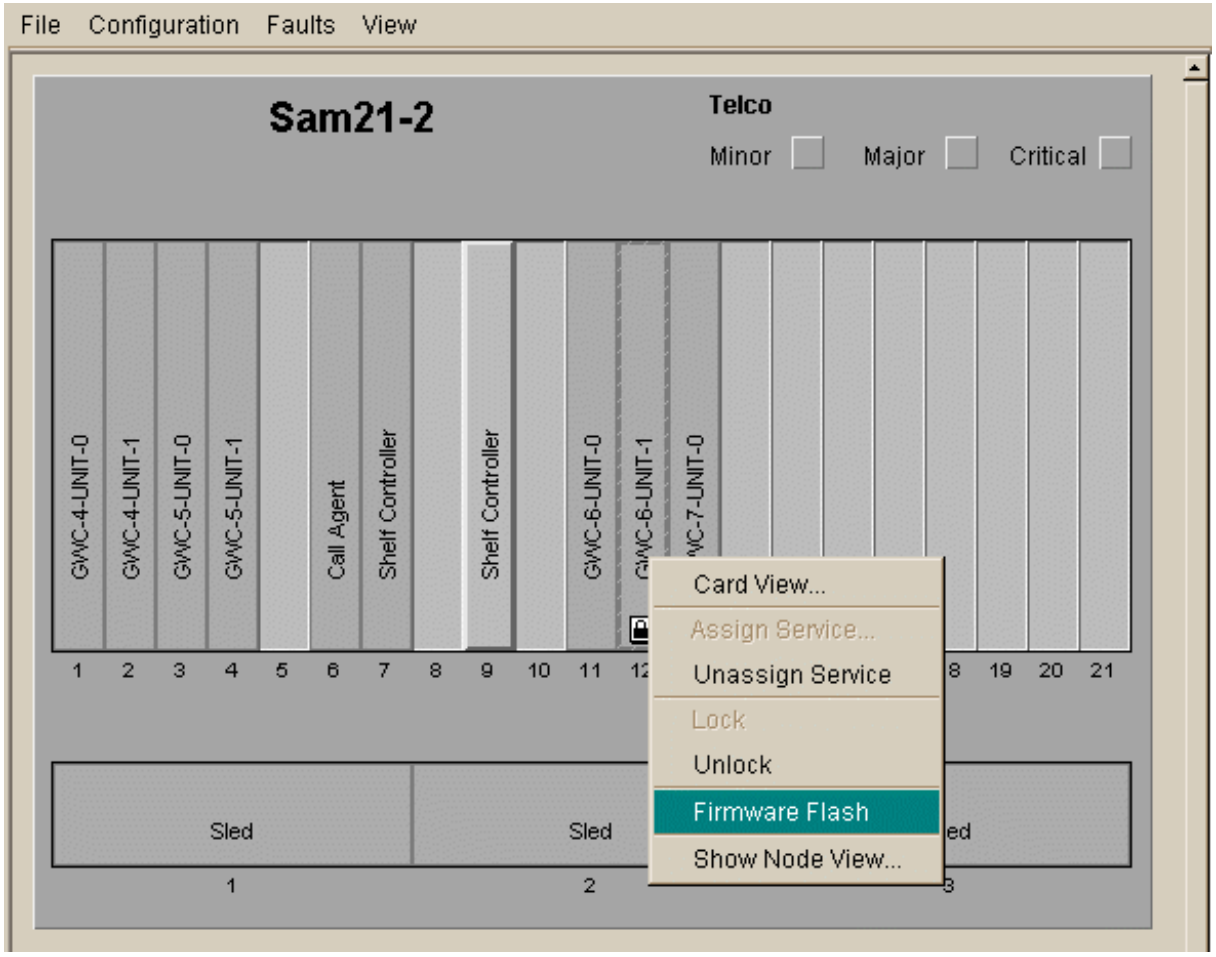

**6** In the Provisioning panel, de-select the “FW Flash Enable” check box.





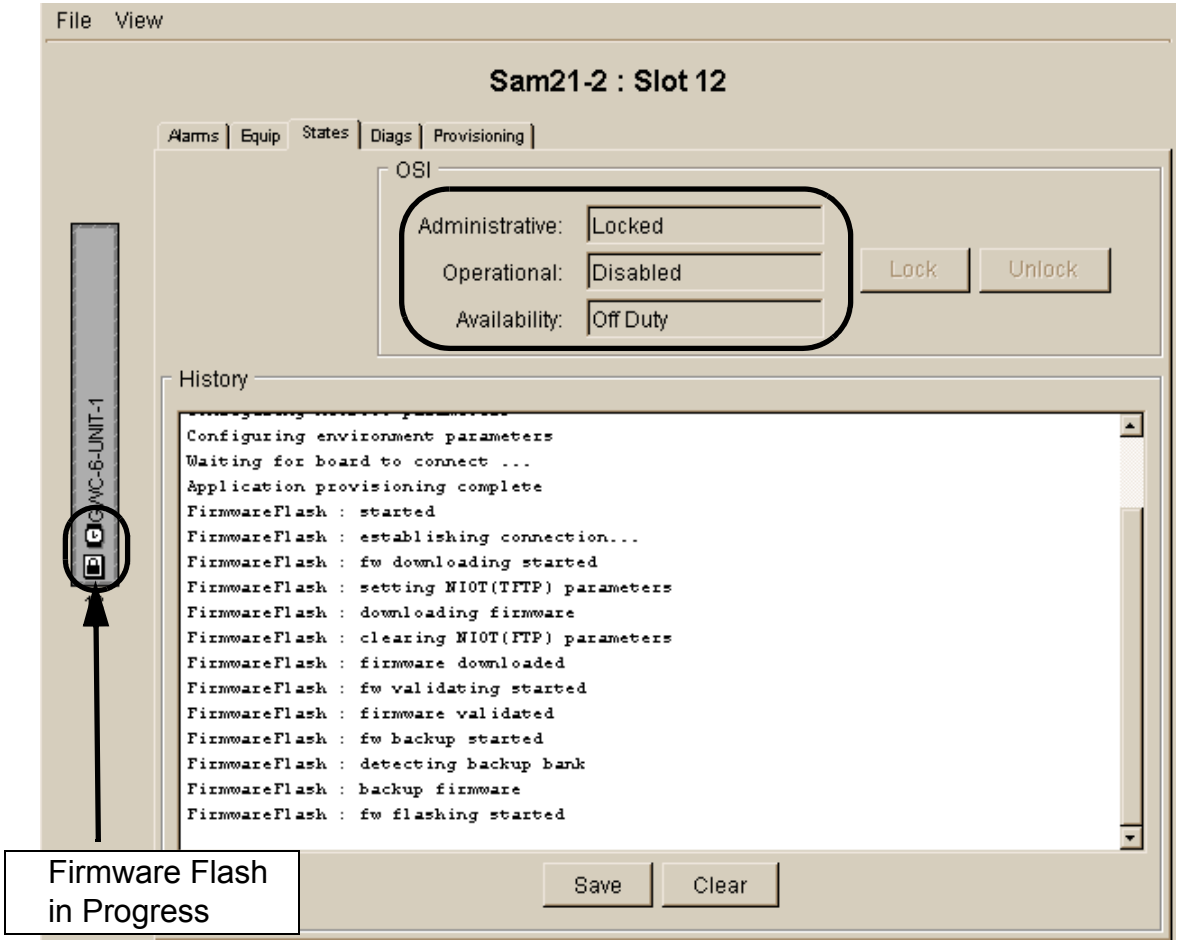

**7** Click the **Save** button at the bottom of the screen to save the provisioning change.

**8** From the Shelf View window, right-click the GWC card scheduled for flashing and select **Firmware Flash** from the pop-up menu.

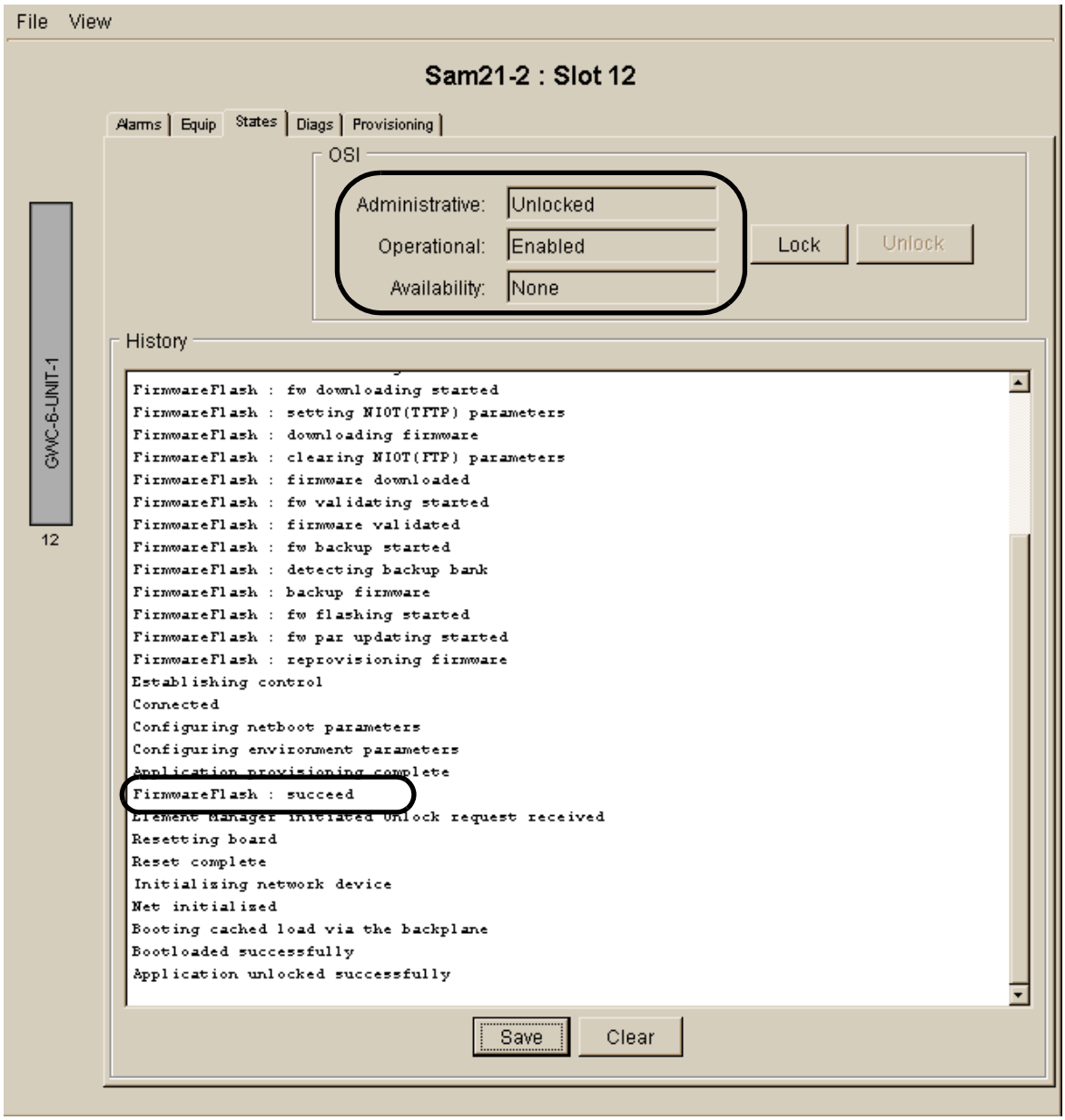


**9** Select the **States** tab in the card view.

Observe that the firmware flash icon appears on the GWC card graphic at the left of the screen during the firmware flash. Also observe the card state transition from "locked-disabled-none" to "locked-disabled-off duty". Observe the various firmware flash progress messages in the History window. (Your messages may vary from the graphic below.)



**10** The firmware flash icon disappears once firmware flashing is complete. Verify that the firmware flash completed without errors by reviewing the text in the History window. Click the **Unlock** button to unlock the card.




**11** Return to step 1 and repeat this procedure for any other GWC cards that require a firmware flash.

**12** The procedure is complete.

# Take a manual GWC software image

## Purpose of this procedure

This procedure describes how to save a software image to the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM).

***Note:*** A procedure also exists to enable the auto-imaging of a GWC software load once daily. Refer to "Enable or disable GWC software auto-imaging" in Upgrading the Gateway Controller, NN10196-461.

## When to use this procedure

Use this procedure as a part of upgrading GWC software for an office or as a part of maintenance activity.

Take an image after all patches have been applied to GWC software. Refer to your site operating procedures for information about soak time and how many patches to apply before taking an image. In the absence of this information, Nortel Networks recommends taking an image immediately after applying R or P status patches.



**CAUTION**

Do not invoke the Save Image function during patching activities. Doing so can cause an invalid or incomplete image to be taken.

## Prerequisites

This procedure has no prerequisites.

## 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.

**2** Change directory to the GWC software directory.

**Example**
**# cd /swd/gwc**

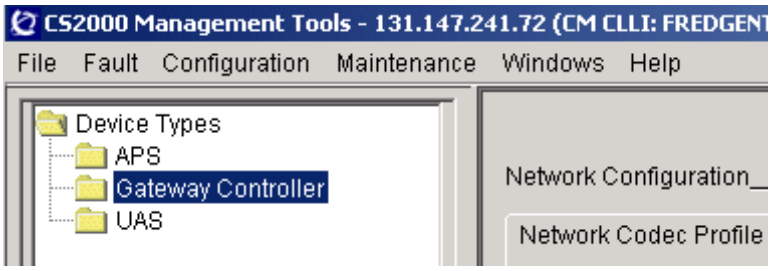
**3** Copy the existing GWC software load file to a backup.

**Example**
**# cp pgc06as.imag pgc06as.imag.bak**

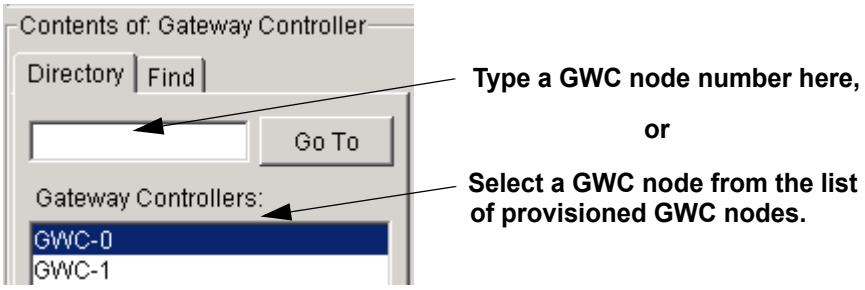
***Note:*** You can use any name for the backup file name.

***At the CS 2000 GWC Manager client***

**4** At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types directory tree in the far left frame.



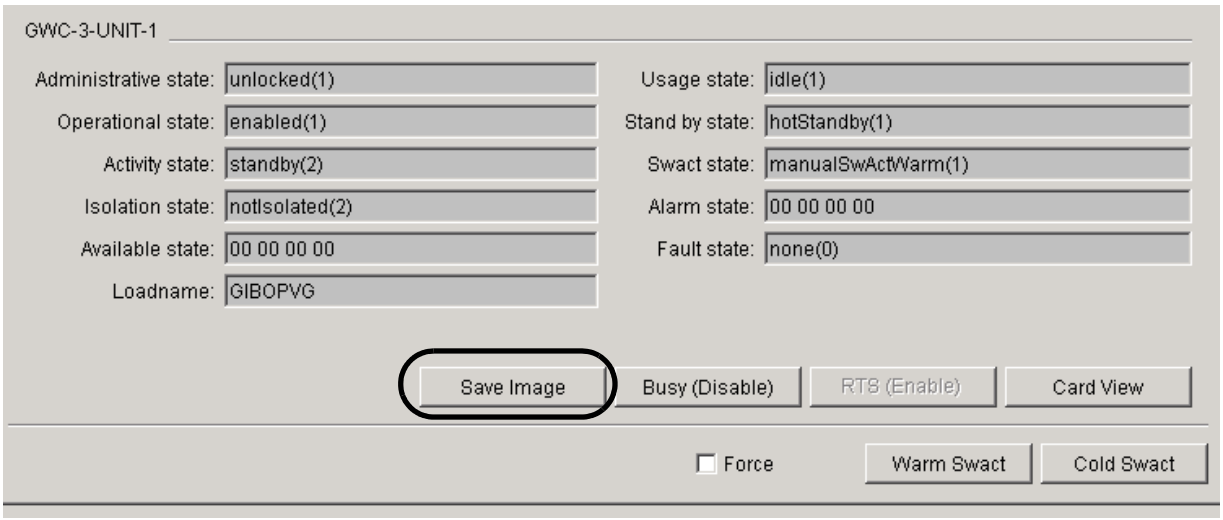

**5** From the Contents of: Gateway Controller frame, select the appropriate GWC node from which you wish to take an image.




**6** Select the **Maintenance** tab to view the Maintenance panel.

**7** In the Maintenance panel, identify the GWC card in the node that has an upgraded load already installed.

**a** Click the **Save Image** button for that card to save the software image back to the CS 2000 Core Manager or CBM.




**b** At the following warning message, click **OK** to continue with saving the GWC card's software image on the CS 2000 Core Manager. To stop the operation, click **Cancel**.




***Note:*** The Save Image command overwrites the existing GWC software load file on the CS 2000 Core Manager or CBM. If the load file name is a link on the file system, the link is replaced with a file of the same name. Nortel Networks does not support using links to load files.

**CAUTION**

Do not invoke the Save Image function during patching activities. Doing so can cause an invalid or or corrupt image to be saved.

8 This procedure is complete.

***Note 1:*** To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure on page 836.

***Note 2:*** To return to the Overall GWC downgrade procedure, refer to downgrade procedures in “Upgrading the Gateway Controller, NN10196-461.

## Troubleshooting

The /swd/gwc directory needs to have privileges set to read, write, execute for world access.

***At the CS 2000 Core Manager or CBM console***

1 Log in to the CS 2000 Core Manager or CBM as the root user.

2 Change directory to the /swd directory by typing

**# cd /swd**

and pressing the Enter key.

3 Change the permissions for the gwc directory and its file contents by typing

**# chmod 777 gwc/***

and pressing the Enter key.

4 This procedure is complete.

# View the contents of a load file image

## Purpose of this procedure

This procedure allows you to view the content of the current load file located on the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM). You can view the list of patches that have been applied and activated on the load file image. A load file is created by taking an image of a software load present on a GWC device. You may take an image manually or automatically.

***Note:*** Perform this procedure on the CS 2000 Management Tools server since the gwclfinfo command is a SESM script, and the /swd/gwc load directory is NFS-mounted on the CS 2000 Management Tools server as /var/opt/nortel/gwc directory.

## When to use this procedure

Use this procedure to confirm the contents of a load file image on the CS 2000 Core Manager or CBM before rebooting GWC devices from the file.

Use this procedure to determine if delivered load contains patches.

## Prerequisites

This procedure has no prerequisites.

## Action

Use the following table to determine your first step.

| If your office has | Do |
|---|---|
| a CS 2000 Core Manager installed | go to step 1 |
| a CBM installed | go to step 5 |

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

1 Access the directory where the GWC load file information is located by typing

```
# cd /var/opt/nortel/gwc
```

and pressing the Enter key.

2 List all the GWC load names by typing

```
# ls
```

and pressing the Enter key.

3 Select the new GWC software load from the list and display its content by typing

**# /opt/nortel/NTsesm/tools/gwc_tools/gwclfinfo /var/opt/nortel/gwc/<gwc_load_file>**

and pressing the Enter key.

where

**<gwc_load_file>**
is the name of the selected GWC load image file, for example pgc09bl_patched_03_04.imag

*Example response:*

```
Load information from pgc09bl_patched_03_04.imag

Load name: PGC09BL Image created: Fri Mar 5
7:0:21 2004

Patch-ID    Status    Activation

XBN63GZ9    Applied   NonAct

XED41GZ9    Applied   NonAct

XQA89GZ9    Applied   NonAct

.

.

.
```

4 This procedure is complete.

***Note:*** To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure on page 836.

***At the CS 2000 Management Tools terminal***

5 Access the temporary directory by typing

**# cd /tmp**

and pressing the Enter key.

6 Access the CBM server by typing

**# ftp <CBM_IP_address>**

and pressing the Enter key.

where

**<CBM_IP_address>**
is the IP address of the CBM server

**7** When prompted, enter the user name by typing

**`Name: gwcload`**

and pressing the Enter key.

**8** When prompted, enter the password by typing

**`Password: gwcload`**

and pressing the Enter key.

**9** Set up the ftp transfer process to binary by typing

**`ftp> bin`**

and pressing the Enter key.

**10** Transfer the GWC image load file by typing

**`ftp> get <gwc_image_name>`**

and pressing the Enter key.

where

**`<gwc_image_name>`**
is the name of the GWC load image file stored on the CBM server

*Example response:*

```
200 PORT command successful.
150 Opening data connection for pgt93ax.imag (binary
                                    mode) (10294018).
226 Transfer complete.
local: pgt93ax.imag remote: pgt93ax.imag
10294018 bytes received in 5.3 seconds (1908.92 Kbytes/s)
```

**11** Return to the /tmp directory on the CS 2000 Management Tools server by typing

**`ftp> quit`**

and pressing the Enter key.

12 Display the content of the GWC software load image by typing

**# /opt/nortel/NTsesm/tools/gwc_tools/gwclfinfo /tmp/<gwc_image_name>**

and pressing the Enter key.

where

**<gwc_image_name>**
is the name of the transferred GWC load image file

*Example response:*

```
Load information from pgt93ax.imag

Load name: PGT93AX Image created: Fri Mar 5
7:0:21 2004

Patch-ID    Status    Activation

XBN63GZ9    Applied   NonAct

XED41GZ9    Applied   NonAct

XQA89GZ9    Applied   NonAct

.

.

.
```

13 When you are finished reviewing the content of the file, remove the GWC load image from the /tmp directory by typing

**# rm /tmp/<gwc_image_name>**

and pressing the Enter key.

where

**<gwc_image_name>**
is the name of the transferred GWC load image file

14 This procedure is complete.

***Note:*** To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure on page 836.

# Upgrading a Media Server 2010

This procedure enables you to upgrade the Media Server 2010 as part of a network-wide upgrade to a new release.

## Office impact

Upgrading the Media Server 2010 as part of network-wide upgrade is dependent upon the upgrade of other network elements first being completed. Therefore, this procedure must be performed at the appropriate time within the network upgrade sequence.

When this procedure is performed in response to a network-wide upgrade, the Media Server 2010 is not operational. Therefore, this procedure should be performed during an offline network maintenance window or when sufficient additional servers are available to maintain normal network operations while this node is out of service.

In this procedure each Media Server 2010 node in the network is to be updated one at a time.

When this upgrade procedure is successfully completed, INI files retrieved from the Media Server 2010 nodes will be encrypted.



**CAUTION**

During the upgrade procedure, you will perform a hard reset on the Media Server. If you are upgrading a 240 port Media Server 2010, the hard reset will take both Media Servers out of service. Any active calls will be dropped!

## Material requirements

This is a software-only procedure and doesn't require special tools. The following files are provided either on compact disc or through electronic software distribution (ESD):

- CMP file (software executable load)
- INI file (configuration file)
- DAT files containing specific information (such as Conference tones, and information to deliver test trunk functionality)

The client workstation must be running the following programs:

- Microsoft Windows 98, NT, 2000, XP, or 2003
- Netscape 6, or higher, or Microsoft Internet Explorer (IE) 6.0, or higher

## Procedure to upgrade a Media Server 2010

Before starting this procedure, review any documentation included with the software. The documentation included with the software may override or supplement the procedure described below.

For increased security, the CS 2000 Management Tool and SDM logins, and the MS 2000 Series Configuration Tool (Media Server 2000 Series CLUI) are equipped with login timeouts. If at any point the procedure below the user interface or telnet session times out, follow the procedure for logging back in, and continue the procedure from the point at which the timeout occurred.

### Upgrading a Media Server 2010

#### *At the Windows desktop interface*

1 Open a DOS window and enter the following three commands:

```
ping <IP address of router>
ping <IP address of CS 2000 Management Tool>
ping <IP address of SDM>
```

If a response displays for all three commands, continue with the next step. If a response does not display for any one of the three commands, check connections and configuration of the network settings for the PC (or laptop). Do not continue with the procedure below until the ping commands all indicate successful connections.

2 Open a telnet connection to the CS 2000 Management Tool.

3 When prompted, enter **nortel** as the user name and **nortel** as the password.

4 Back up the files in the /data/load/ams directory by performing the following steps:

**a** Log in to the Media Server 2000 Series CLUI by entering the following commands:

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

**b** When prompted, enter **nortel** as the user name and **nortel** as the 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)
>
```

**c** Enter the number corresponding to “Backup INI file for all nodes”. This will retrieve a current copy of the INI file for each Media Server 2010 configured in the system.

***Note:*** The .ini files are backed up in a directory with the ams ip address as the directory name. Only the last five backed up .ini files are kept in this directory. Note the dates to determine which file is the most recent.

**d** Press “x” to exit the Media Server 2000 Series CLUI.

**e** Enter the following on the command line:

**cd /data/loads/ams**

**f** Create a backup directory with a descriptive name that includes today’s date and the current release version, 6.2:

**mkdir ams_bku_*<today’s date>*_*<release>***

**Example**
mkdir ams_bku_20031031_6.2

**g** Back up the files:

**cp -p *.cmp ams_bku_*<today’s date>*_*<release>***

**cp -p *.dat ams_bku_*<today’s date>*_*<release>***

***Note:*** If you receive an error such as “cp cannot access *.dat”, this indicates that there are no files of this type to back up.

**h** Each Media Server 2010 node has a directory containing a copy of its INI file. The directory name is the IP address of the Media Server 2010 node. Make a backup copy of each Media

Server 2010 directory by **repeating** the following command at the command line for each Media Server 2010 node:

**cp -pr *<MS 2010 ip address>* ams_bku_*<today's date>*_*<release>***

where *<release>* is the current release (6.2)

**Example**
cp -pr 172.17.40.230 ams_bku_20040501_6.2

**i** Change to the backup directory you created in step f above and verify that the files and directory are actually present.

**5** Determine the source for the software upgrade files.

| If | Do |
|---|---|
| the software upgrade files are on CD | step 6 |
| the software upgrade files have been delivered through ESD | step 7 |

**6** Copy the files from the CD.

**a** Insert the CD into the CS 2000 Management Tool CD drive.

**b** Enter the following command:

```
cd /cdrom/cdrom0
```

**c** Enter the following command:

```
ls
```

Verify the content of the CD that displays by referring to the patch or release installation instructions to determine the correct release content. You may see .ini, .dat, and .cmp files listed, as well as an installation script (*<filename>*.sh or *<filename>*.pl). The CD may also contain some documentation or a README.file.

**d** Copy the files to the ams directory on the CS 2000 Management Tool by entering the following command:

```
cp * /data/loads/ams
```

**e** Enter the following commands:

```
cd /data/loads/ams
```

```
ls -ltr
```

Ensure that the files you copied are present in the directory. The newer files will appear near the bottom of the listing.

***Note:*** Make a note of the full path name of the .cmp file for use later in this procedure.

**7** Prepare the .dat file and the .ini file.

**a** Refer to the release notes and consult with your network administration regarding the tones file to determine if a customized toneset .DAT file is appropriate for your network.

**b** Perform an upgrade to the .ini file by entering the following command:

**perl iniupgrade.pl AMS_DefaultConfig_IP_v109.ini <*SN06.2 ini file from step* 4c> <*SN07 .ini filename*>**

**8** Install the new software load on the Media Server 2010.

**a** Log in to the Media Server 2000 Series CLUI by entering the following commands:

**cd /opt/nortel/NTsesm/bin/**

**./ms2000.sh**

**b** When prompted, enter **nortel** as the user name and **nortel** as the password.

*The Media Server 2000 Series CLUI main menu displays.*

**c** Enter the number corresponding to “Node Maintenance and Configuration”.

**d** In response to the prompt, enter the IP address of the Media Server 2010 node that you are upgrading.

*The Main Menu for MS2010 at <ip_address> displays.*

```
***** Main Menu for MS2010 at <ip_address> *****
1) Maintenance Menu
2) Configuration Menu
x) EXIT
Enter selection (1-2, x)
>
```

**e** Enter the number corresponding to, “Configuration Menu”.

*The Main Configuration Menu for MS2010 at <ip_address> displays.*

```
*Main Configuration Menu for MS2010 at <ip_address>*
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)
>
```

**f** Enter the number corresponding to “Display this nodes current configuration”.

*The current configuration information for the node displays.*

Make a note of the existing configuration values for this node, especially the “Software Version”, for use later in this procedure.

***Note:*** If you encounter the error, “The MS 2000 node at xx.xxx.xxx.xx is either not in service or is not an MS 2000 node”, verify that you have entered the correct IP address. Use the “ping” command to ensure that the MS 2010 node can be accessed. If necessary, “hard” reset the server and repeat step d. Instructions for performing a hard reset can be found in steps 18a and 18b

**g** Press Enter to continue.

*The Main Configuration Menu for MS2010 at <ip_address> displays.*

**h** Press “x”, to exit this menu.

*The Main Menu for MS2010 at <ip_address> displays.*

**i** Enter the number corresponding to the “Maintenance Menu”.

*The Maintenance Menu for MS2010 at <ip_address> displays.*

```
**** Maintenance Menu for MS2010 at <ip_address> ****
1) Download load files to this node
2) Backup the INI file for this node
3) Perform a soft reset on this node
4) Lock or Unlock this node
x) EXIT
Enter selection (1-4, x)
>
```

**j** Enter the number corresponding to “Lock or Unlock this node”.

*The MS 2000 Lock Menu displays.*

**i** In response to the prompt, enter the number corresponding to “Perform Graceful Lock”.

***Note:*** Gracefully locking a node ensures that active calls on the node complete before the node is locked and removed from service.

**ii** In response to the prompt, enter “y” and press Enter. When prompted to continue, press Enter again.

*The MS 2000 Lock Menu displays.*

**iii** Press “x”, to exit this menu.

*The Maintenance Menu for MS2010 at <ip_address> displays.*

**k** Determine whether the node is locked.

| If | Do |
|---|---|
| the “Current state” in the Media Server 2010 Lock Menu displayed in the previous step indicates that the node is locked | step q |
| the “Current state” in the Media Server 2010 Lock Menu displayed in the previous step indicates that the node is not locked | step l |

**l** Press “x”, to exit the menu.

*The Main Menu for MS2010 at <ip_address> displays*

**m** Enter the number corresponding to “Configuration Menu”.

*The Main Configuration Menu for MS2010 at <ip_address> displays.*

**n** Wait for the calls on the node to complete. Enter the number corresponding to “Display this nodes current configuration”.

*The current configuration information for the node displays.*

In the configuration display, look for the “Lock State” parameter. If the node is not locked, press Enter and perform this step again. If the node is locked, press Enter and go on to the next step.

**o** Press “x” to exit the menu.

*The Main Menu for MS2010 at <ip_address> displays.*

**p** Enter the number corresponding to “Maintenance Menu”.

*The Maintenance Menu for MS2010 at <ip_address> displays.*

**q** Enter the number corresponding to “Download load files to this node”.

*The MS 2000 Restore Loads Menu displays.*

**r** The Toneset and TestTrunk .dat files must be copied to the SDM. The .dat files only need to be copied once.

**i**

| If | Do |
|---|---|
| this is the first node you are upgrading using this procedure | continue this step |
| this is not the first node you are upgrading using this procedure | step v |

**ii** Enter the number corresponding to “Download call progress tones (.dat) file”.

*A list of .dat files displays.*

**iii** Enter the number corresponding to the appropriate toneset .dat file to upload. In response to the prompt to do a soft reset, enter “n”.

**iv** In response to the prompt to save the files to the SDM, enter “y”.

*When the file has been successfully copied to the SDM, as indicated by a message display at the console, the MS 2000 Restore Loads Menu displays.*

**v** Enter the number corresponding to “Download load files to this node”.

*The MS 2000 Restore Loads Menu displays.*

**vi** Enter the number corresponding to “Download call progress tones (.dat) file”.

*A list of .dat files displays.*

**vii** Enter the number corresponding to the appropriate TestTrunk .dat file to upload. In response to the prompt to do a soft reset, enter “n”.

**viii** When the download completes, as indicated by a message display on the console, you will be prompted to transfer the file to the SDM. Enter “y” in response to the prompt to save the file to the SDM.

*When the file has been successfully copied to the SDM, as indicated by the message display at the console, the MS 2000 Restore Loads Menu displays.*

**s** Enter the number corresponding to “Download load image (.cmp) file”.

*A list of .cmp files displays.*

**t** Enter the number corresponding to the correct file copied off of the upgrade software CD. In response to the prompt to continue, enter “y”.

The download begins. The Media Server 2000 Series CLUI will not respond for up to five minutes while the download is in progress.

**u** When the download completes, as indicated by a message display on the console, you will be prompted to transfer the file to the SDM. Enter “y” in response to the prompt to save the .cmp file to the SDM.

*When the file has been successfully copied to the SDM, as indicated by a message display at the console, the MS 2000 Restore Loads Menu displays.*

**v** The INI file associated with the new software load must be installed on the Media Server 2010 nodes.

***Note:*** This is the SN07 .ini file that was created in step 7.

**i** Enter the number corresponding to for “Download configuration (.ini) file”.

*A list of .ini files displays.*

**ii** Enter the number corresponding to the INI file to upload. This file was created in step 7. In response to the prompt to continue, enter “y”.

The download begins. The Media Server 2000 Series CLUI will not respond for up to five minutes while the download is in progress.

**iii** When the download completes, as indicated by a message display on the console, you will be prompted to transfer the file to the SDM. Enter “y” in response to the prompt to save the INI file to the SDM.

*When the file has been successfully copied to the SDM, as indicated by the message display at the console, the MS 2000 Restore Loads Menu displays.*

**w** Press “x” to exit this menu.

*The Maintenance Menu for MS2010 at <ip_address> displays.*

**x** Enter the number corresponding to “Perform a soft reset on this node”. In response to the prompt, “Perform Soft Reset?”, enter “y”. In response to the prompt to continue, press Enter.

*The Maintenance Menu for MS2010 at <ip_address> displays.*

**y** Press “x” to exit this menu.

*The Main Menu for MS2010 at <ip_address> displays.*

**z** After waiting approximately 2 minutes for the soft reset to complete, enter the number corresponding to “Configuration Menu”.

*The Main Configuration Menu for MS2010 at <ip_address> displays.*

**aa** Enter the number corresponding to “Display this nodes current configuration”.

*The current configuration information for the node displays.*

**ab** In the configuration display, look for the “Software Version” parameter. Verify that the expected version of the software has been downloaded (check the release notes for the software upgrade label). Press Enter.

*The Main Configuration Menu for MS2010 at <ip_address> displays.*

**ac** At this point in the upgrade it may be necessary to configure any new functionality. Refer to the release notes to determine if there are any special configuration requirements for the new release.

**ad** Press “x” to exit this menu.

*The Main Menu for MS2010 at <ip_address> displays.*

**ae** Press “x” to exit this menu.

*The Media Server 2000 Series CLUI main menu displays.*

**9** Press “x”, to exit from the MS 2000 Series CLUI.

**10** Minimize the window containing the telnet connection with the CS 2000 Management Tool.

| If | Do |
|---|---|
| this is the first node you are downgrading using this procedure | step 11 |

| If | Do |
|---|---|
| this is not the first node you downgrading using this procedure | step 17 |

11 Open a telnet connection to the SDM server in order to redirect links to the new file versions.

12 Log in with the “root” user name and password.

13 Enter the following commands at the command line:

```
cd /swd/ams
ls -ltr *.cmp
```

*The “.cmp” files in the “ams” directory display.*

**Example**
-rwxr-xr-x 2 swld swld 1024 date **:** ams_420108255.cmp

-lrwxr-xr-x 2 swld swld 1024 date **:** ams.cmp -> ams_420108255.cmp

-rwxr-xr-x 2 swld swld 1024 todaysdate **:** ams_<newrel>.cmp

14 Enter the following command:

```
ln -sf <new filename> <linkname>
```

**Example**
ln -sf AMS_420109378.cmp ams.cmp

***Note:*** The linkname is the name to the left of the pointer (->) in the listing output lines beginning with “l” (lower-case L). (Refer to the example in step 13.) Record the value of the linked file displayed in step 13 for possible use in a downgrade procedure should a severe problem requiring a downgrade to the current release occur.

15 Enter the following command:

```
sum *.cmp | sort
```

*A list of the “.cmp” files, with checksums for each of the files, displays.*

**Example**
17124 ams.cmp

54723 AMS_420108255.cmp

17124 AMS_420109378.cmp

Verify that the checksums for the symbolic link matches the checksum for the new .cmp file. Thus, in the example above, the files “ams.cmp” and “AMS_42109378.cmp” both have the same checksum, “17124”.

***Note:*** If the message, “sum: ams.cmp No such file or directory” displays, this indicates an invalid link. Steps 13 through 15 must, in that case, be repeated.

**16** Minimize the window containing the telnet connection with the SDM.

**17** Enter the following command on the command line in the window containing the telnet session with the CS 2000 Management Tool:

```
ping -s <IP address of MS 2010>
```

**Example**
ping -s 10.10.10.10

*A ping display starts.*

**Example**
Reply from 10.10.10.10: bytes=32 time<10ms TTL=252
Reply from 10.10.10.10: bytes=32 time<10ms TTL=252
.
.

### *At an Media Server 2010 unit*

**18** Perform a “hard” reset of the Media Server 2010:



**CAUTION**

Performing a hard reset on a 240 port Media Server 2010, takes both Media Servers out of service.

**a** At the Breaker Interface Panel located at the top of the frame, turn off the breaker associated with the Media Server 2010 that you are upgrading and then turn the breaker on again.

*In the ping command window, check that the Media Server 2010 is again responding. Wait up to three minutes*

*for the reply. The normal response is a short down time with a return to service of the Media Server 2010.*

**b** Check the activity lights on the front of the Media Server 2010 card:

- the blue hot swap ready LED should not be illuminated
- the green power LED should be lit
- the dual ethernet LEDs should indicate a connection (solid green) with activity (blinking orange)
- the yellow activity LED should light after about one minute
- the red Fail LED should not be lit

***Note:*** A problem with the yellow LED indicates a problem with the bootp server download of the software. Check the output from steps 13 through 15 for a possible problem with the .cmp file configuration.

***At the Windows desktop interface***

**19** Press the “Ctrl” key and hold while pressing the “C” key. This will terminate the “ping” command.

**20** Verify that the upgrade has been completed.

**a** Log in to the Media Server 2000 Series CLUI by entering the following commands:

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

**b** When prompted, enter **nortel** as the user name and **nortel** as the password.

*The Media Server 2000 Series CLUI main menu displays.*

**c** Enter the number corresponding to “Node Maintenance and Configuration”.

**d** In response to the prompt, enter the IP address of the Media Server 2010 node that you are upgrading.

*The Main Menu for MS2010 at <ip_address> displays.*

**e** Enter the number corresponding to “Configuration Menu”.

*The Main Configuration Menu for MS2010 at <ip_address> displays.*

**f** Enter the number corresponding to “Display this nodes current configuration”.

*The current configuration information for the node displays.*

Verify that the configuration information displayed matches the expected configuration values in the release notes. Pay particular attention to the software version and compare it to the expected value making sure it has changed since performing step 8e. Ensure that the port allocation and language settings are correct. This verifies that the upgrade was done successfully.

**g** Press Enter to continue.

*The Main Configuration Menu for MS2010 at <ip_address> displays.*

**21** Press “x” to exit this menu.

*The Main Menu for MS2010 at <ip_address> displays.*

**22** Press “x” to exit the menu.

*The Main Menu for MS2010 at <ip_address> displays.*

**23** Enter the number corresponding to “Maintenance Menu for MS2010 at <ip_address>”.

*The Maintenance Menu for MS2010 at <ip_address> displays.*

**24** Enter the number corresponding to the “MS2000 Lock Menu”.

*The MS 2000 Lock menu displays.*

**a** In response to the prompt, enter the number corresponding to “Unlock this node”.

*The MS2000 Lock Menu displays.*

**b** Press “x” to exit this menu.

*The Maintenance Menu for MS2010 at <ip_address> displays.*

**25** Press “x” twice to return to the Media Server 2000 Series Main menu.

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

**26** At this point in the procedure, you have completed upgrading a node. The functionality of the node can be verified by directing calls to it. After this verification is complete, determine whether additional nodes are to be upgraded.

| If | Do |
|---|---|
| another node is to be upgraded | step 8c |
| no other node is to be upgraded | step 27 |

27 Log off from all Media Server 2010 nodes and close all windows.

***Note:*** It is recommended that you perform a full backup of the SESM.

28 Add the Media Server 2010 devices to the Integrated EMS for alarm handling. Refer to the Adding a Media Server MS2000 NE) in the *Integrated EMS Configuration Management* document, *NN10330-511*.

29 Delete the Media Server 2010 devices from the SESM inventory. Refer to the Adding a Media Server MS2000 NE) in the *Integrated EMS Configuration Management* document, *NN10330-511*.og off from all Media Server 2010 nodes and close all windows.

30 You have completed this procedure.

# Upgrading the MG 9000

This section provides a description of the upgrade process and the software upgrade tool in the MG 9000 Manager used to upgrade software in the cards in the MG 9000. The following procedures for upgrading the MG 9000 are included in this section:

- Installing MG 9000 loads into the CS 2000 Core Manager from DAT tape on page 909
- Installing MG 9000 loads into the CS 2000 Management Tools Manager from CDROM on page 916
- Provisioning a floating IP address on page 918
- information on the process and tools used to upgrade software in the MG 9000 cards
  - Upgrading software in MG 9000 cards on page 921
  - "Software Upgrade View" in Upgrading the MG 9000, NN10048-461
  - "Software upgrade errors and problem resolution" in Upgrading the MG 9000, NN10048-461
  - "Upgrade Wizard Overview" in Upgrading the MG 9000, NN10048-461
- upgrade procedures by type
  - "Card upgrade with user intervention" in Upgrading the MG 9000, NN10048-461
  - Card upgrade without user intervention" in Upgrading the MG 9000, NN10048-461
  - "MG Upgrades" in Upgrading the MG 9000, NN10048-461
  - Upgrading the MG 9000 from SN06.x to SN07 on page 923
- "Downgrading the MG 9000 Manager from SN07 to SN06.x" in Upgrading the MG 9000, NN10048-461
- Downloading software into the MTA card on page 926
- Downloading software into the xDSL card on page 928
- "Upgrade History" in Upgrading the MG 9000, NN10048-461
- Patching the MG 9000 on page 1777

# Installing MG 9000 loads into CS 2000 Core Mgr from DAT tape

## Purpose of this procedure

This procedure describes how to install the MG 9000 software loads onto the CS 2000 Core Manager (SDM) from Digital Audio Tape (DAT) tape.

## When to use this procedure

This procedure is to be used when a Maintenance Non-computing Load (MNCL) software release or standard NCL is delivered to the customer site.

## Prerequisites

When supporting an upgrade from SN06.x to SN07, ensure the SN06.x loads are currently in the SDM in the event there is a need to perform a software downgrade from SN07 to SN06.x.

## Action

**Installing MG 9000 loads into the CS 2000 Core Manager from DAT tape**

***At the CS 2000 Core Manager frame***

**1** Insert the DAT tape in slot 2 or slot 13 on the CS 2000 Core Manager.

***At the CS 2000 Core Manager console or terminal window***

**2** Log in to the CS 2000 Core Manager as the root user.

```
AIX Version 4
(C)Copyrights by IBM and by others 1982, 1996.
login: root
root's password: <password>
```

**3** Enter the SDM maintenance level by typing

```
#sdmmtc
```

**4** Enter the Software Installation Menu level by typing

```
>swim
```

The system responds with the SWIM level.

**5** Enter the Apply level by typing

```
>apply
```

**6** Retrieve the fileset from tape by typing

```
>source <dat_no>
```

*where* dat_no is 0 or 1. Use 0 if the DAT is in slot 2 or 1 if the DAT tape is in slot 13.

**7** Select the new MG 9000 software from the Apply menu by typing

```
>select <fileset_no>
```

*where* fileset_no is an integer value and represents the new MG 9000 software file set such as “4”

To select multiple or all file sets, the Select command should be executed for each file set before the Apply command is executed. As each file set is selected, its file set is highlighted on the MAP terminal screen.

***Note:*** The load will be placed in the following directory: /swd/mg9k/.

**8** Apply the file set to the CS 2000 Core Manager (SDM) by typing

```
>apply
```

**9** The MG 9000 software is now available to support software upgrades from the MG 9000 Manager.

**10** Remove the DAT tape.

**11** This procedure is complete.

# Setting the CS 2000 CLLI on an SSPFS-based server

## Application

Use this procedure to set the CLLI of the Communication Server 2000 (CS 2000) on a Succession Server Platform Foundation Software (SSPFS)-based server. You can also use this procedure to remove the CS 2000 CLLI from the server.

**ATTENTION**
Ensure your system is patch-current before performing this procedure. If the system is not patch-current, changing or unconfiguring the CM CLLI may cause loss of configuration data on the system. If you are unsure whether the patch that corrects this issue has been applied, contact your next level of support before proceeding.

## Prerequisites

You must have the CLLI for the CS 2000 that is associated with the SSPFS-based server on which you are setting the CLLI. The CS 2000 CLLI is listed in table OFCENG.

## 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 are setting the CS 2000 CLLI

**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 “OAMP Application Configuration” option in the menu.

*Example response*

```
OAMP Application Configuration
 1 - sdm_conf (Configure SDM IP Address and
     User)
 2 - sdm_unconf (Unconfigure SDM IP Address and
     User)
 3 - cmClli_conf (Configure CM_CLLI Address)
 4 - cmClli_unconf (Unconfigure CM_CLLI IP
     Address)
 5 - cm_conf (Configure CM IP Address)
 6 - cm_unconf (Unconfigure CM IP Address)

 X - exit

select -
```

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

| If you are | Do |
|---|---|
| setting the CS 2000 CLLI on the Sun server | step 9 |
| removing the CS 2000 CLLI from the Sun server | step 10 |

**9** Set the CS 2000 CLLI as follows:

**a** Enter the number next to the “cmClli_conf” option in the menu.

*Example response*

```
===Executing “cmClli_conf”

Enter CM_CLLI:
```

**b** When prompted, enter the CLLI for the CS 2000.

*Example response*

```
CM CLLI:      CLLITEST

Enter “ok” to accept current settings
```

**c** When prompted, confirm the setting by typing

**ok**

and pressing the Enter key.

*Example response*

```
Processing values...

CM_CLLI Configured
Please perform a logout and login so your
shell will reflect CLLI environment settings

===”cmClli_conf” completed successfully
```

**d** Proceed to step 11.

**10** Remove the CS 2000 CLLI as follows:

**a** Enter the number that corresponds to the “cmClli_unconf” option in the menu.

*Example response*

```
===Executing “cmClli_unconf”

Please perform a logout and login so your
shell will no longer contain the CLLI
environment settings

===”cmClli_unconf” completed successfully
```

**b** When prompted, enter the CLLI for the CS 2000.

*Example response*

```
CM CLLI:      CLLITEST

Enter “ok” to accept current settings
```

**c** When prompted, confirm the setting by typing

**ok**

and pressing the Enter key.

*Example response*

```
CM CLLI:      CLLITEST

Enter “ok” to accept current settings
```

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

```
select - x
```

and pressing the Enter key.

**12** Log out and log back in to the Sun server to reflect the CLLI environment changes.

**13** You have completed this procedure.

# Installing MG 9000 loads into CS 2000 Core Mgr from CDROM

## Purpose of this procedure

This procedure describes how to install the MG 9000 software loads onto the CS 2000 Core Manager (SDM) from CDROM.

## When to use this procedure

This procedure is to be used when a Maintenance Non-computing Load (MNCL) software release or standard NCL is delivered to the customer site.

## Prerequisites

When supporting an upgrade from SN06.x to SN07, ensure the SN06.x loads are currently in the SDM in the event there is a need to perform a software downgrade from SN07 to SN06.x.

## Action

### Installing MG 9000 loads into the CS 2000 Management Tools Manager from CDROM

***At the CS 2000 Management Tools Manager***

**1** Insert the CDROM into the CDROM tray. If the unit is a Netra 240 in a cluster configuration, use the active Netra 240 unit. The active unit is identified by a lit USER LED on the front of the unit.

The CDROM label for the SAM21 Shelf Controller software includes the product code, MG9K0007, on the lower half of the label.

***At the CS 2000 Management Tools console or terminal window***

**2** Log in and then use the su command to gain root privilege.

```
login: username
Password: <password>
Last login: Fri Jun 30 12:48:18 from <otherhost>
su - root
Password: <password>
```

**3** Execute the platform_load_install.sh script by typing

```
# /opt/nortel/sspfs/Scripts/platform_load_install.sh
```

The system responds with the following.

```
Welcome to the Platform Installation Tool
Version 3.2

================================================
RPM INSTALLATION/REMOVAL
============================
1) Install RPM from CDROM 2) Install RPM from
                             Disk
3) Uninstall RPM          4) Query all RPMs

OTHER
=========
C) Change Rotation Parameters P) View Rotation
                                 Parameters
V) MG9K Platform Version      X) Exit
Installed

Please choose one of the following:
```

**4** To install the software type **1** and press the Return key.

The screen clears and the contents of the .rpm package are displayed.

***Note:*** If the message `There is no cd in the CDROM drive, please check drive` is displayed, ensure that the CDROM is inserted in the tray for this unit.

**5** To proceed with the software installation, type Y.

The software is extracted from the .rpm package. The .rpm package is transferred to the CS 2000 Core Manager.

**6** Enter the root password for the CS 2000 Core Manager. The software is installed on the CS 2000 Core Manager.

**7** Enter the Eject command to eject the CD from the CDROM drive.

```
# eject
```

**8** Log out of the CS 2000 Management Tools server.

**9** Remove the CDROM.

**10** This procedure is complete.

# Provisioning a floating IP address

## Purpose of this procedure

The MG 9000 Manager assigns the floating IP address to the card being upgraded dynamically. The floating IP address is provisioned from the MG 9000 Manager as described in the following procedure. Provisioning a floating IP address should be performed during initial installation and commissioning. The floating IP address is persisted in the MG 9000 Manager data.

***Note:*** Before beginning, ensure you have the correct privileges to perform this procedure.

Contact your network administrator to obtain a new IP address when a new floating IP address must be provisioned.

## When to use this procedure

This procedure is provided only if the need arises to change, correct, or add the floating IP address.

## Prerequisites

There are no prerequisites.

## Action

**Provisioning a floating IP address**

***At the MG 9000 Manager***

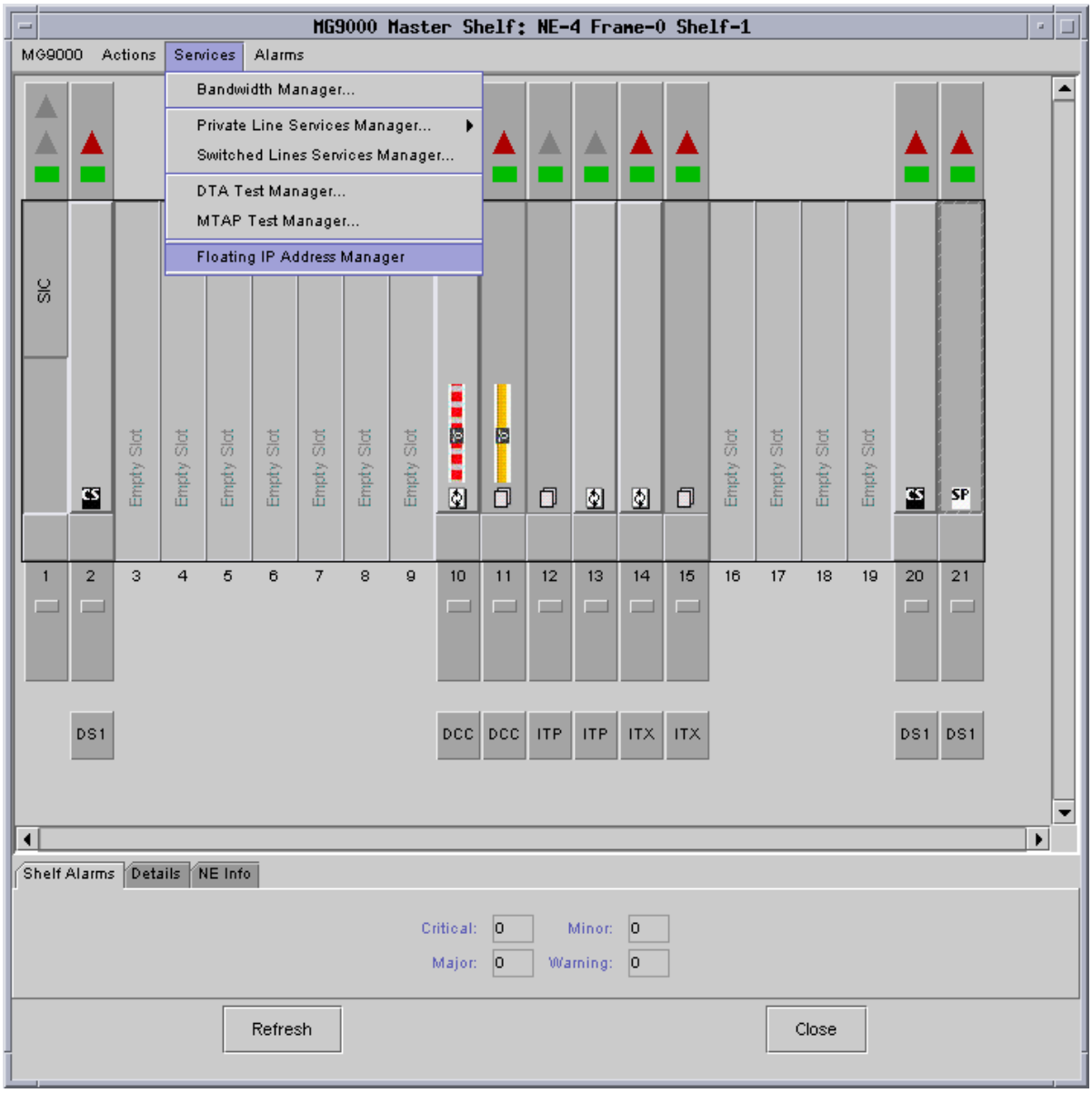
**1** Verify whether a floating IP address has already been provisioned at the MG 9000 Manager by selecting Services->Floating IP Address Manager from the menu bar of any Frame, Shelf, or Card View. This address must be in the same subnet as the MG 9000.

***Note:*** If performing an upgrade from SN06.x to SN07, perform this step from the SN06.x MG 9000 Manager.

**2** To provision a floating IP address in the MG 9000 Manager if necessary, perform the following steps:

**a** From any Frame, Shelf, or Card view select the menu Services. From within Services select Floating IP Address Manager, as shown in the following figure.

## Floating IP Address Manager accessed from Shelf View



**b** Enter the IP address in the Floating IP Address Manager and select Apply. The address will be displayed under existing IP addresses. When finished, select Close.

### Floating IP Address Manager View




**c** If the floating IP address must be replaced, delete the entry first. To delete an entry select the entry, select the Delete check box, then press Apply. When finished select Close.

**d** If the floating IP address is correct, select Close.

**3** This procedure is complete. If this is part of an upgrade, return to the upgrade checklist to continue with the upgrade process.

# Upgrading software in MG 9000 cards

This section provides an overview of upgrading software in MG 9000 cards.

The MG 9000 Manager provides tools for upgrading software in MG 9000 cards to upgrade the software in the following intelligent cards in the MG 9000:

- data control card (DCC)
  - — OC-3
  - — DS1-IMA
- Internet telephony extender (ITX) card
- Internet telephony processor (ITP) card
- DS-512 Access Bridging Interface (ABI) card
- DS1 card (not used in UA-IP solution)

The following cards do not use the Software Upgrade Wizard. Instead, each card must have the software downloaded into it individually using the Software Download tool accessed from the card view for each card. There are software download procedures provided for these cards later in this document.

- metallic test access (MTA) card
- x digital subscriber line (xDSL) card

The software upgrade consists of the following four steps:

1. Configure - The configuration parameters are entered in a Card Upgrade Wizard or MG Upgrade Wizard described later.
2. Download - The MG 9000 is requested to download the software load to a card or cards based in the parameters configured in the previous step. The load is downloaded and stored in flash memory.
3. Apply - The software load is installed. A restart is performed in the card.
4. Accept - The new installed load is made the primary load. The user can no longer revert to the old load unless a complete downgrade is performed.

An additional Abort step can be used to abort an upgrade in progress, an revert back to the old load.

***Note:*** Software upgrade of cards in the MG 9000 must be performed in the following order DS1, ABI, ITP, ITX, DCC.

There are two ways to perform a software upgrade.

- with user interaction - The user must enter separate commands to perform the download, apply, and accept steps.
- without user interaction - The user enters a single command to perform the download, apply, and accept steps.

**Upgrade version rules**

The software upgrade application requires the following version order when an upgrade is performed to a load with the same version or to higher version load.

- DS1 or ABI
- ITP
- ITX
- DCC

***Note 1:*** The MG 9000 supports in-service upgrades from SN06.x to SN07. The Silence Suppression variables (used in the UA-IP solution only) will be set to default when the upgrade occurs. To reset the Silence Suppression variables, go to “Provisioning switched lines services” in *MG 9000 Configuration Management*, NN10096-511.

***Note 2:*** When it is necessary to downgrade to SN06.x, perform the “Downgrading the MG 9000 Manager from SN07 to SN06.x” in *Upgrading the MG 9000*, NN10048-461 .

***Note 3:*** During a downgrade, attempting to upgrade cards to a version lower than the DCC card is not supported.

Upgrades - the supported upgrade path for the MG 9000 is from SN06 to SN07 for the UA-IP solution and from SN06.2 to SN07 for the UA-AAL1 solution.

Downgrades - the supported downgrade path for the MG 9000 is from SN07 to SN06.2 for UA-AAL1 and SN07 to SN06 for UA-IP.

# Upgrading the MG 9000 from SN06.x to SN07

## When to use this procedure

Use the following procedure when it is necessary to upgrade the MG 9000 from SN06.x to SN07 using MG 9000 Patch Image load files.

***Note:*** The MG 9000 cards are upgraded in the following order: DS1, ABI (DS-512), ITP, ITX, and DCC.

### What is an MG 9000 Patch Image (9PI) load file?

A 9PI is a pre-patched MG 9000 load image file and is identified by the .tar extension on the filename. The patches contained in the image are not required to be applied following the upgrade. However, patches for the MG 9000 are administered using the Network Patching Manager (NPM) patching system so the NPM needs to be taught about the applied patches. Any device that has been upgraded to a pre-patched load must be audited (by the NPM) following the upgrade for the NPM to determine the patch content. Any pre-applied patches need to be placed in the NPM database (using the getpatch command). Also, any additional patches required but not included in the image will need to be applied. For information and procedures for patching the MG 9000 software using the NPM, refer to *ATM Solutions Upgrade*, NN10261-450 or *IP Solutions Upgrade*, NN10344-450.

To display the content of an SN07 patched image without having to load the file into a card and have the NPM perform an audit, login to the machine where the load files are located, change to the directory where the load file resides and enter the following at the command line on one line:

```
> strings SC0A07BB_GZ.tar | awk
'/patchlist_begin/'/patchlist_end/'
```

where SCOA07BB_GZ.tar is an example of a patched image file name

The following is an example of the output in response to the previous command:

```
patchlist_begin
SCO01UBB
SCO02UBB
SCO03UBB
SCO04UBB
SCO05UBB
SCO06UBB
SCO07UBB
SCO10UBB
SCO12UBB
SCO13UBB
SCO17UBB
patchlist_end
```

## Prerequisites

Perform the upgrade in the SN06.x Subnet View.

Ensure the NE has been exported and the floating IP address has already been provisioned.

## Action

### Upgrading the MG 9000 from SN06.x to SN07

#### *At the MG 9000 Manager*

1. At the Frame View of the MG 9000 selected for upgrade click the Actions menu.
2. At the Actions menu select Software Upgrade... The MG 9000 Software Upgrade view is created as described in “Softwareupgrade view” in *Upgrading the MG 9000*, NN10048-461.
3. Check the Upgrade Originator pane in the MG 9000 Software Upgrade View to ensure the MG 9000 Name and Originating View (NE number) represent the MG 9000 to be upgraded.
4. Press the Configure button to start the MG Upgrade wizard. The MG Upgrade Wizard, Card Type Selection, Step 1 appears.
5. Select “All Card Types” to upgrade all cards. A check appears in the box next to the selection.
6. Select “Use one load server only” to use the same load server. Click the Next button.

**7** In the MG Upgrade Wizard, Select a load server, enter the server address, user identifier, and password for the load server where the SN07 load for the selected card type is contained. Click Next.

**8** In the MG Upgrade Wizard, for each card specify an SN07 load, the directory and load name are provided. Respond to each step requesting the load name for the card. Ensure you use the latest pre-patched image load file provided by Nortel located on the SDM in directory /swd/mg9k/. The following represent SN07 load names, though the ones listed here may not be the latest available:

- DS1G07AZ_GZ
- ABIG07AZ_GZ
- ITPA07AZ_GZ
- ITXA07AZ_GZ
- SCOA07AZ_GZ (DCC-OC3) or SCIA07AZ_GZ (DCC DS1-IMA)

Click on Next and repeat this step for each card type. Click on Finish.

**9** At the Software Upgrade View, click on Upgrade to start the upgrade process.

***Note:*** All upgraded nodes (cards) display a major alarm which remains until the NE is controlled by an upgraded MG 9000 Manager.

**10** This procedure is complete.

If the MG 9000 Manager is a one-server configuration, go to step 8 on page 780 of the MG 9000 Manager and MG 9000 SN06.x to SN07 upgrade checklist (one-server) and continue with the upgrade process.

If the MG 9000 Manager is a two-server configuration, go to step 13 on page 794 of the MG 9000 Manager and MG 9000 SN06.2 to SN07 upgrade checklist (two-server) and continue with the upgrade process.

# Downloading software into the MTA card

## When to use this procedure

Use this procedure when it is necessary to update software onto an MTA card. The Software Download Manager menu option provides access to a Software Download Manager window.

## Prerequisites

If the software download is part of the SN06.x to SN07 upgrade, ensure the floating IP address has already been provisioned.

## Action

### Downloading software into the MTA card

***At the SN06.x MG 9000 Manager***

1. At the Subnet View, double click on the MG 9000 that has the MTA card to which software is to be downloaded. The Frame View appears.
2. At the Frame View, double click on the shelf in which the MTA card resides. The Shelf View appears.
3. At the Shelf View, double click on the slot in which the MTA card resides. The card view appears.
4. To request a download, select the Locked option for the Administrative Status in the Status box. The card must be Locked prior to requesting a download.
5. From the MTA Card View menu level, select Actions->Software Download Manager
6. Enter data in the fields as follows:
   - File Path - the path and name of the file on the SDM to be downloaded to the card (/mg9k/<loadname>)
   - IP address - the file location (IP address)
   - Server userName - the login name for the server where load resides
   - Server password - the password for the server where load resides
   - select Force Download if forced download is required
7. Select the Download button at the bottom of the Software Download Manager window.

Once the download is complete, the Load Status field indicates if the download was successful, and the software load being used by the card is displayed under Restart Current in the Software Load pane.

***Note:*** After the software download is performed, a message appears stating that the MTA card is restarted.

Perform the download again, since the MTA card has a Primary and Backup load. When a download is performed, the Primary load becomes the Backup load and the new load becomes the Primary load. Performing the download twice makes the new load the Primary and the Backup load and guarantees the current load is the new load.

**8** After the second download is complete, from the MTA Card View set the Administrative Status of the MTA card to Unlocked by selecting the Unlocked option in the Status box.

**9** This procedure is complete. If this action is part of an MG 9000 upgrade, return to the upgrade checklist to continue with the upgrade process.

# Downloading software into the xDSL card

## When to use this procedure

Use this procedure when it is necessary to download updated software onto an xDSL card. The Software Download Manager menu option provides access to a Software Download Manager window.

## Prerequisites

Perform this activity during periods of low traffic.

If the software download is part of the SN06.x to SN07 upgrade, ensure the floating IP address has already been provisioned.

## Action

**Downloading software into the xDSL card**

***At the SN06.x MG 9000 Manager***

1. At the Subnet View, double click on the MG 9000 that has the xDSL card to which software is to be downloaded. The Frame View appears.
2. At the Frame View, double click on the shelf in which the xDSL card resides. The Shelf View appears.
3. At the Shelf View, double click on the slot in which the xDSL card resides. The card view appears.
4. To request a download, select the Locked option for the Administrative Status in the Status box. The card must be Locked prior to requesting a download.
5. From the xDSL Card View menu level, select Actions->Software Download Manager
6. Enter data in the fields as follows:
   - File Path - the path and name of the file to be downloaded to the card (/mg9k/<loadname>)

     ***Note 1:*** For cards with no patchables (no .tar file), include the .bin extension (such as, DSLA07BW.bin) as /mg9k/DSLA07BW.bin.

     ***Note 2:*** In certain offices, the file path may be /swd/mg9k/

   - IP address - the file location (IP address)

- Server userName - the login name for the server where load resides
- Server password - the password for the server where load resides
- select Force Download if forced download is required. The force option is needed only when the card must be reloaded with the same load that already exists on the card.

**7** Select the Download button at the bottom of the Software Download Manager window. When the download begins the download icon appears on the card.

Once the download is complete, the download icon disappears and the initialization icon appears. Once initialization is complete, the icon disappears and the software load used in the card is displayed in the Software Load section of the Card View.

**8** If necessary, repeat steps 3 through 7 for all xDSL cards in the MG 9000 network element that must be upgraded. Otherwise skip this step.

**9** Unlock the cards that were locked in step 4.

**10** This procedure is complete. If this action is part of an MG 9000 upgrade, return to the upgrade checklist to continue with the upgrade process.

# Upgrading the UAS

## UAS06 or UAS07 to UAS08 (SN06) software upgrade procedure

This procedure enables you to perform an upgrade from release UAS06 or UAS07 to release UAS08. Steps 1 through 15 of this procedure must be performed for each domain that you are upgrading.

***Note:*** The UAS is normally deployed on the network in pairs of systems, with two separate systems per chassis. The left-hand side of the chassis is designated as domain A. The right-hand side of the chassis is designated as domain B. If you are upgrading two domains on a chassis from release UAS06 to release UAS08, you must perform the upgrade on domain B first. If you are upgrading from UAS07 to UAS08, upgrade domain A first and then domain B.



**CAUTION**

No remote access sessions (telnet, ftp) should be in progress on a unit that is being upgraded.

### Procedure 1 UAS06 or UAS07 to UAS08 software upgrade procedure

***At your console***

1 Using the APS Administration GUI procedure “Disabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” disable audio provisioning for this UAS unit.

2 Using the Universal Audio Server Manager, look in the States window of the Network Element Status panel at the Usage category to determine whether the UAS is active and is processing calls. If the UAS is idle, proceed to step 3 of this procedure. If the UAS is active, determine whether any conferences are in progress by pulling down the Component menu in the System Identification window of the Network Element Status panel and selecting “conferencing service.” From the “conferences in progress” value in the component-specific panel of the Performance tab screen, determine whether to proceed to step 3 of this procedure: if conferences are in progress, wait until they complete; if conferences are not in progress, proceed with this procedure.

3 Using the procedure “Changing the Admin state,” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state for this UAS unit being upgraded to “graceful lock.”

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

4 Uninstall (remove) the release UAS06 or UAS07 software by performing the procedure, UAS06/UAS07 application software removal on page 1601. Removing the software creates the proper archive files for the following steps.

5 Archive the UAS06 and/or UAS07 configuration files by performing the following steps:

***Note:*** This step is performed to ensure that you have the latest version of the configuration files backed up in the event that you need to perform a downgrade back to an earlier release later on.

**a** Open a command line interface at the UAS:

**i** select **Start -> Run**

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

**iii** press Enter

**b** If you wish to archive UAS06 configuration files, enter the following commands:

```
mkdir D:\UAS06restore
```

```
xcopy C:\Winnt\Temp\*.archive
D:\UAS06restore /Y
```

Messages showing the files being copied display.

Go to step d

**c** If you wish to archive UAS07 configuration files, enter the following commands:

```
mkdir D:\UAS07restore
```

```
xcopy C:\Winnt\Temp\*.archive
D:\UAS07restore /Y
```

Messages showing the files being copied display.

**d** Close the command line interface.

6 If you are upgrading from release UAS06 and if the fabric type of your system is ATM-AAL2, remove the BX4000c (S007) card and replace it with a PA200 card by performing the procedure,

Replacing a BX4000c (S007) card with a PA200 card on page 934.

***Note:*** Before replacing the BX4000c (S007) card with a PA200 card, you must have completed replacing the CPV5350 processor card with a CPV5370 processor card. For assistance, contact your Nortel Networks service representative.

**7** Upgrade the Global Server (GS) base platform software by performing the procedure, Upgrading Global Server base platform software on page 937.

**8** If you are upgrading from UAS06 to UAS08, perform the procedure, Configuring NetMeeting on a Win2K AS on page 939. NetMeeting can be used for accessing the UAS from a remote location in the event that any additional configuration or troubleshooting is required after the installation.

**9** Install the UAS08 software by performing the procedure, UAS08 application software installation on page 941.

**10** If the CG6000 card configuration is to be changed, perform the procedure, “Adding a CG6000 card to a UAS node,” or the procedure, “Removing a CG6000 card from a UAS” in the NTP NN10073-911, entitled “UAS Fault Management.”

**11** Enable audio distribution at the APS for this UAS unit by performing the procedure “Enabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management.”

**12** Perform the procedure “Provisioning a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” to force immediate provisioning of any files created before the start of the upgrade.

**13** Update any remaining UAS units by performing this procedure for each unit.

**14** Using the procedure “Viewing UAS performance measurements,” in the document, NN10139-711, entitled “UAS Performance Management,” verify that the UAS unit is enabled and is processing calls. In the procedure view, specifically, the performance measurements for the “Conferencing Service” and “IVR Service” components.

**15** Reactivate audio provisioning capability for system users by performing the procedure “Editing user profiles,” in the document, NN10095-511, entitled “UAS Configuration Management,” changing the user status of all system users to “activated.”

16 If you wish to limit access to the “regedit.exe” and “regedt32.exe” utilities, perform the procedure, Limiting access to the “regedit.exe” and “regedt32.exe” utilities on page 1605.

17 If you wish to limit access to the shared network folders, perform the procedure, Limiting access to shared network folders on page 1607.

18 If you wish to limit access to the “hh.exe”, “winhelp.exe”, or “winhlp32.exe” utilities, perform the procedure, Limiting access to the “hh.exe”, “winhelp.exe”, and “winhlp32.exe” utilities on page 1608.

19 If you wish to configure IP Security on the UAS, perform the procedure, Configuring IPSec and IKE on page 1610.

20 You have completed this procedure.

# Replacing a BX4000c (S007) card with a PA200 card

This procedure enables you to upgrade from a BX4000c (S007) card to a PA200 card in ATM-AAL2 systems. Before you start performing this procedure, ensure that you have a complete PA200 card set, that is, a PA200 card and an R200 rear transition module.

## Replacing a BX4000c (S007) card with a PA200 card



**WARNING**
**Static electricity damage**
While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.



**DANGER**
**Laser radiation exposure**
The exposed ends of fiber optic cables can emit harmful laser radiation. Do not look at the ends of fiber optic cables unless protector caps are in place. Disconnect all laser sources when personnel are working with fiber-optic cables.



**CAUTION**
**Possible equipment damage**
Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

***At the system console (Windows desktop interface) connected to the domain containing the card being replaced:***

**1** Stop any applications that may be 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.

**2** Shut down the system:

select **Start -> Shut Down**

**a** On the Shut Down Windows screen, select “Shut down this computer.” When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do not turn off power to the computer.

**3** Locate the BX4000c card. If the UAS node is located on the left side of the shelf, the card will be in slot 5; if the node is located on the right side of the shelf, the card will be in slot 12. Remove the BX4000c card by performing the following steps:

**a** Disconnect the OC3c interface cable from the BX4000c card. After the cable has been removed, cap the connectors on the card and on the fiber cable.

**b** Remove the BX4000c card. (The screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed.)

***Note:*** There is no rear transition module for this card.

**c** Install a filler plate over the slot from which the BX4000c card was removed.

**4** Install the PA200 card set by performing the following steps:

**a** Remove the filler plate either from slot 6 or from slot 11 on the back of the chassis, depending on where you will install the R200 rear transition module of the PA200 card set, and then remove the corresponding filler plate from slot 6 or 11 on the front of the chassis, where you will install the PA200 card.

**b** Insert the new R200 rear transition module in the back of the chassis. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.

**c** Insert the new PA200 card in the front of the chassis. Lock the lock latches on the card and tighten the screws that secure the card in the shelf.

**d** Remove the protective caps from the connectors on the new R200 rear transition module and from the connectors on the fiber cable. Connect the OC3c interface cable to the module.

**5** With an appropriate device, press the guarded reset switch located on the front panel of the CPV5370 Processor card that is associated with the domain in which the PA200 card is being installed. The CPV5370 card is located in slot 7 for the left domain and in slot 9 for the right domain.

**6** You have completed this procedure.

# Upgrading Global Server base platform software

This procedure enables you to remove existing Global Server base platform software and upgrade to release Global Server 3.3.

## Upgrading Global Server base platform software

***At your console***

**1** Insert the CD-ROM, “Global Server Platform Software, GS v3.3” into the CD-ROM drive of the domain (A or B) of the application server on which you are installing operating system software.

**2** Select **Start -> Programs -> Accessories -> Command Prompt**

**3** Upgrade from the previous version of the platform software by entering the following command at the command prompt:

```
<cdrom>:\upgrade <cdrom>:\
```

where *<cdrom>* is the letter of the CD-ROM drive on the application server. For example: **E:\upgrade E:**

***Note 1:*** Software upgrade will take several minutes to complete; if a security lock screen appears before the upgrade completes, log back in.

***Note 2:*** A message will appear in the MS-DOS window that indicates when the upgrade has completed.

**4** The upgrade of the platform reverts the Global Server Program Manager service password to its default value. It may be necessary at this point to synchronize passwords in order for the service to start properly.

| If | Do |
|---|---|
| you have the default system password, “superuser” | step 8 |
| you have changed the password | step 5 |

**5** Perform the following steps to synchronize the Global Server Program Manager service, PMGR, with the system password:

**a** select **Start -> Run**

**b** Enter the following:

```
Services.msc
```

*The Services window displays.*

6 In the Services window, right-click pmgrDaemon and select Properties.

*The PMGRdaemon Properties (Local Computer) window displays.*

7 In the PMGRdaemon Properties (Local Computer) window, select the Log On tab.

**a** Select “This account.”

**b** In the “account name” field, verify the entry or enter:

```
.\Administrator
```

**c** In the “password” and “confirm password” fields, enter the new password.

**d** Click OK.

*The Microsoft Management Console dialog box displays.*

8 Remove the CD-ROM from the CD-ROM drive.

9 You have completed this procedure.

This procedure enables you to configure NetMeeting software on a single Win2K application server. This procedure is required only when you are upgrading from UAS06.

***Note:*** In order to prevent possible access problems, you should install NetMeeting on your desktop only when logged in as "administrator".

### Configuring NetMeeting on a Win2K AS

***At your console***

**1** Perform the following steps:

**a** select **Start -> Programs -> Accessories -> Communications -> NetMeeting**

*The NetMeeting Setup Wizard window displays.*

**b** Click Next.

**c** In the subsequent NetMeeting Setup Wizard window, enter the requested information about your system and then click Next.

**d** In the subsequent NetMeeting Setup Wizard window, deselect the "Log into a directory server when NetMeeting starts" check box and then click Next.

**e** In the subsequent NetMeeting Setup Wizard window, select the "Local Area Network" check box for the speed of your network connection and then click Next.

**f** In the subsequent NetMeeting Setup Wizard window, deselect all check boxes for the desktop shortcuts and then click Next.

**g** In the final NetMeeting Setup Wizard window, ignore the Sound Card hardware warning message and click Finish.

*The NetMeeting application starts*.

**2** In the NetMeeting application main window, perform the following steps:

**a** select **Tools -> Remote Desktop Sharing**

**b** In the Remote Desktop Sharing Settings window that displays, click the "WIZARD ..." box.

*The Remote Desktop Sharing Wizard window displays.*

**c** Click Next.

**d** In the subsequent Remote Desktop Sharing Wizard window, click Next.

**e** In the subsequent Remote Desktop Sharing window, select the “No, I will do this later” and then click Next.

**f** In the final Remote Desktop Sharing Wizard window, click Finish.

**g** In the Remote Desktop Sharing Settings window, click OK.

**3** In the NetMeeting application main window, select **Call -> Automatically Accept Calls**

**4** In the NetMeeting application main window, select **Call -> Exit and Activate Remote Desktop Sharing**

**5** You have completed this procedure.

# UAS08 application software installation

This procedure enables you to install the UAS08 application software.

### UAS08 application software installation

***At your console***

**1** Close all applications.

**2** Insert the UAS08 installation CD into the CD-ROM drive.

**3** Launch the InstallShield Wizard for Universal Audio Server program by performing the following steps:

**a** select **Start -> Run**

**b** In the Run window, click Browse.

**c** In the Browse window, navigate to the file, *<cd-rom>*: \winnt\setup.exe, select the file, and click Open.

***Note:*** *<cd-rom>* is the “drive letter” assigned to the CD-ROM device.

**d** Click OK.

*The Welcome window for the InstallShield Wizard for Universal Audio Server displays.*

**4** In the Welcome window for the InstallShield, click Next.

*The Choose Node Type screen displays.*

**5** Select the appropriate gateway type, Gateway or Universal Audio Server (audio server).

| If | Do |
|---|---|
| you chose Gateway (in support of an IMS release) | step 6 |
| you chose Universal Audio Server | step 8 |

**6** Click Next.

**7** In the screen that displays, select “PRI” and then click Next.

**a** Go to step 12.

**8** Select the bearer fabric type of your system, either IP or ATM.

| If | Do |
|---|---|
| you chose IP | step 12 |
| you chose ATM | step 9 |

**9** In the InstallShield Wizard Complete screen, click Finish.

***Note 1:*** In some cases, an application error will display immediately after the information message, “Stopping Program Manager.” This is a known platform problem that is patched by the UAS installation. If an error dialog appears with an “AM.EXE Application error” pop-up indicating a problem with an instruction at a referenced memory location, dismiss the error dialog by clicking the “OK” button.

***Note 2:*** Up to 60 seconds may pass before the InstallShield Wizard Complete screen first appears.

***Note 3:*** If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

**10** Perform the following steps.

**a** Perform the following steps to install the PCI drivers:

**i** Right-click My computer, and then select “Properties.”

**ii** In the pop-up window that displays, select the Hardware tab and click Device Manager (located in the middle of the window).

**iii** In the Device Manager window that displays, right-click PCI Memory Controller (located under “TDM/ATM bridge 2” on the window) and select “Properties.”

***Note:*** For ground-up installations and for UAS06 AAL2 upgrades, PCI Memory Controller will appear under “Other devices” on the window.

**iv** In the PCI Memory Controller Properties window that displays, select the Driver tab and then click the Update Driver button.

**v** In the Upgrade Device Driver Wizard window that displays, click Next.

vi In the Install Hardware Device Drivers subscreen (of the Upgrade Device Driver Wizard window), the radio button, “Search for a suitable driver for my device” is selected by default. Click Next.

vii In the Locate Driver Files subscreen (of the Upgrade Device Driver Wizard window), deselect “Floppy disk driver” and “CD-ROM driver”, then select “Specify a location” box, and, finally, click Next.

viii In the Upgrade Device Driver Wizard pop-up window (subtitled, “Insert the manufacturer’s installation disk into the drive selected and then click OK”), type (or browse for) “c:\NMS_pa200\Pa200\system” and then click OK.

ix In the Driver Files Search Results window, click Next.

x In the Completing the Upgrade Device Driver Wizard subscreen (of the Upgrade Device Driver Wizard window), click Finish.

xi In the PA200 Base Board WDM Properties window, click Close.

xii Close the Device Manager window (click X, located in the upper right-hand corner of the window).

xiii Close the System Properties window (click OK).

**b** Re-boot the system by performing the following steps:

i select **Start -> Shutdown**

ii select “restart the computer” in the Shutdown Windows screen.

**c** After the system re-boots, log back into the system as “administrator” (user name), and enter either “superuser” as the password or the password supplied by your network administrator.

**d** Open a command line interface at the UAS:

i select **Start -> Run**

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

iii press Enter

iv type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

v press Enter

**e** Launch the Local Configuration Interface GUI by performing the following steps:

i select **Start -> Run**

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

iii press Enter

iv type **lci** on the command line

***Note:*** The first letter in the lci command is an “l”, as in “local.”

v press Enter

*The main Local Configuration Interface GUI screen displays.*

vi select the “node” folder in the Network Element Tree pane.

*The Bearer Type ATM Local Configuration Interface GUI screen displays. Three tabs display in the “Details of selected tree node” window. Each tab selects a separate screen used for data filling.*

vii You may see a pop-up window explaining that the configuration is not consistent with ATM. The system will ask you whether you want to update. Click OK.

viii You may see a pop-up message window that indicates the configuration data has been updated. Click OK.

**f** Examine the Adaptation Layer heading on the screen and ensure that the appropriate screen for the ATM bearer fabric type of your system displays.

***Note:*** If you are performing a ground-up installation, the Adaptation Layer heading on the screen will be blank. If you are, instead, upgrading an existing ATM system, the Adaptation Layer heading will contain the appropriate ATM bearer fabric type for your system.

| If | Do |
|---|---|
| the appropriate screen for the bearer fabric type displays | step h |
| the appropriate screen for the bearer fabric type does not display | step g |

**g** Pull down the Adaptation Layer menu and select the appropriate bearer fabric type. The following rules dictate the system reaction to your selection:

- When you select a bearer fabric type for the first time during a ground-up installation, the pop-up message

"Setting the default ATM mode ..." displays; click OK in the message pop-up.

- When you select ATM-AAL1, the system checks to ensure that IVR is disabled and BCT is enabled, as required, for the ATM-AAL1 system. If the system detects that IVR is enabled or BCT is disabled, it will react in the following manner:
  - — A pop-up window explaining that the configuration is not consistent with ATM displays. The system will ask you whether you want to update; click OK in the message pop-up.
  - — Another pop-up message window that indicates the configuration has been updated will then display; click OK in the message pop-up.

*The Bearer Type ATM Local Configuration Interface GUI screen that you selected displays.*

***Note:*** In each of the screens that display when you manipulate the ATM fabric version of the LCI GUI in the following steps, fields containing default data that cannot be changed appear in the color grey. In addition, when data is entered in an incorrect format in some of the fields that can be changed, the field label changes to a red color. When the data is then corrected in the field, the field label changes back to black. None of the screen changes can be validated and saved until all fields in all of the screens associated with the bearer fabric contain correct information.

**h** Determine whether the fabric type of your system is ATM-AAL1 or ATM-AAL2.

| If | Do |
|---|---|
| your UAS bearer fabric type is ATM-AAL1 | step i |
| your UAS bearer fabric type is ATM-AAL2 | step m |

i In the General tab screen, verify and/or enter information for the following fields:

- **Atm Companding Mode**

  *This is the companding mode, either A-Law or Mu-Law.*

- **Optical Carrier Mode**

  *This field allows selection of the appropriate optical carrier standard for your ATM card, either SONET (a North American standard for optical carriers) or SDH (a European standard for optical carriers). The default for AAL1 systems is SONET.*

- **NTP Server IP**

  *This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.*

  ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

- **Backup Storage IP**

  *This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.*

- **ATM CTone Support**

  *This field, which must be datafilled when ATM BCT Support is ENABLED (ATM BCT Support is always ENABLED for an AAL1 system), determines how the audio endpoints for the ATM AG4000 card are defined. The possible responses are: ENABLED or DISABLED. If an AG4000 card is not provisioned in the system, this field should be set to DISABLED.*

j Select the “Call Agent” tab.

*The Call Agent tab screen displays in the “Details of selected tree node” window.*

**k** In the Call Agent tab screen, verify and/or enter information for the following fields:

- **Primary Call Agent Name**

  *This is the computer name associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent IP Address**

  *This is the IP address associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent Port**

  *This is the port of the Call Agent application (default is 2944).*

- **UAS Call Control Port**

  *This is the port associated with receiving the call control message stream (default is 2944).*

**l** Go to step 13.

**m** Ensure that the General tab screen is selected.

**n** In the General tab screen, verify and/or enter information for the following fields:

- **Atm Companding Mode**

  *This is the companding mode, either A-Law or Mu-Law.*

- **Optical Carrier Mode**

  *This field allows selection of the appropriate optical carrier standard for your ATM card, either SONET (a North American standard for optical carriers) or SDH (a European standard for optical carriers). The default for AAL2 systems (including wireless systems) is SDH; if a*

*North American AAL2 system is being configured, this field must be changed to SONET.*

- **Gateway Control Protocol**

  *This is the control protocol for the UAS, either H.248 or MGCP.*

- **IVR Support**

  *This indicates whether IVR support is enabled on this system.*

- **NTP Server IP**

  *This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.*

  ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

- **Primary DBServer Host**

  *This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, when IVR Support is enabled, an entry must still be made in this field.*

- **Primary DBServer IP**

  *This is the IP address of the APS that is hosting the database server used by this UAS node.*

- **Backup Storage IP**

  *This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.*

- **Audio Synch on Restart**

  *For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled,*

*hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.*

- **ATM BCT Support**

  *This indicates whether Bearer Channel Tandeming is supported on this system*

- **ATM CTone Support**

  *This field, which must be datafilled when ATM BCT Support is ENABLED, determines how the audio endpoints for the ATM AG4000 card are defined. The possible responses are: ENABLED or DISABLED. If an AG4000 dedicated to CTone is not provisioned, this field should be set to DISABLED.*

**o** Select the “Call Agent” tab.

*The Call Agent tab screen displays in the “Details of selected tree node” window.*

**p** In the Call Agent tab screen, verify and/or enter information for the following fields:

- **Primary Call Agent Name**

  *This is the computer name associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent IP Address**

  *This is the IP address associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent Port**

  *This is the port of the Call Agent application (default is 2944).*

- **UAS Call Control Port**

  *This is the port associated with receiving the call control message stream.*

- **Legacy Announcements**

  *This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.*

  ***Note:*** If Legacy Announcements is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Announcements is

Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **Primary Language**

  *This is the primary language associated with the node.*

  ***Note:*** A Primary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  *This is the secondary language associated with the node.*

  ***Note:*** A Secondary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Secondary Language field will also be Disabled.

**11** Double click the “Cards Folder”, which is located in the Nodes folder in the Network element Tree pane.

*A list of the cards that are installed in the system displays below the “Cards Folder”.*

**a** Review the card list. In the list, click the bullet associated with a card for which information is to be examined or changed.

*A card detail window displays in the “Details of selected tree node” screen.*

| If | Do |
|---|---|
| card information is to be changed | step b |
| card information is not to be changed | step 13 |

**b** Enter information in the following fields in the dedicated card details window:

- Test Trunk Support; select either Enabled or Disabled
- Test Trunk Config Size; select the appropriate size (small - 50k trunks; medium - 100k trunks; large - 200k trunks), when Test Trunk Support is Enabled. This determines the number of channels available for tests.

- Sage Box 1 IP (address); enter when Test Trunk Support is Enabled. One Sage test box is use for small and medium test trunk configurations.
- Sage Box 2 IP (address); enter if a second Sage test box is required, when Test Trunk Support is Enabled. Two Sage test boxes are used for large configurations.

**c** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step d |
| you do not want to save the information | step g |

**d** Click Validate.

**e** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI card detail screen) and select “Save”. Click OK when the confirmation screen displays.

**f** Go to step 13.

**g** Click Cancel.

**h** Either return to step a and select another card, or go to step 13.

**12** In the InstallShield Wizard Complete screen, which displays after a slight delay, select “Yes, I want to restart my computer now.” Click Finish.

***Note 1:*** The system re-boot (restart) is required in order for the installation program to complete registry updates.

***Note 2:*** If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

**a** After the system re-boots, log back into the system as “administrator” (user name), and enter either “superuser” as the password or the password supplied by your network administrator.

**b** Open a command line interface at the UAS:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

**v** press Enter

**c** Launch the Local Configuration Interface GUI by performing the following steps:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **lci** on the command line

***Note:*** The first letter in the lci command is an “l”, as in “local.”

**v** press Enter

*The main Local Configuration Interface GUI screen displays.*

***Note:*** In each of the screens that display when you manipulate the IP fabric version of the LCI GUI in the following steps, fields containing default data that cannot be changed appear in the color grey. In addition, when data is entered in an incorrect format in some of the fields that can be changed, the field label changes to a red color. When the data is then corrected in the field, the field label changes back to black. None of the screen changes can be validated and saved until all fields in all of the screens associated with the bearer fabric contain correct information.

**vi** select the “node” folder in the Network Element Tree pane.

*The Bearer Type IP Local Configuration Interface GUI screen displays. Four tabs display in the “Details of selected tree node” window. Each tab selects a separate screen used for data filling.*

**d** In the General tab screen, verify and/or enter information for the following fields:

- **Gateway Control Protocol**

  *This is the control protocol for the UAS, either H.248 or MGCP.* Ensure that the Gateway Control Protocol is set to H.248.

- **IVR Support**

  *This field determines whether IVR support is enabled in this system.*

- **Conferencing State:**

  *This field determines whether Conferencing is enabled in this node.*

  ***Note:*** If Conferencing State is Disabled, then the Conference Spanning field is also Disabled.

- **Conference Spanning**

  *This field determines whether Conference Spanning is supported by the node. Conference Spanning allows conferences with up to 128 participants.*

  ***Note:*** If “Conferencing State” is Disabled, then the Conference Spanning field is also Disabled.

- **Conference Expansion Ports**

  *This field indicates the number of reserved conference ports that can be used to grow existing conferences, but that cannot be used in reservations for new conferences. This prevents existing conferences from running out of resources. Once a port from this buffer is used, it is restored to the pool of resources after any member of the conference in the pool drops out of the conference.*

  W*hen you increase this number, fewer ports are available for general use. For example, if you reserve four ports, a 32-port pool will have only 28 ports available for new conferences. If you decrease this number, fewer ports are*

*available to grow existing conferences when the pool is full.*

- **NTP Server IP**

  *This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.*

  ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

- **Primary DBServer Host**

  *This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, accept the default settings.*

- **Primary DBServer IP**

  *This is the IP address of the APS that is hosting the database server used by this UAS node.*

- **Backup Storage IP**

  *This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.*

- **Audio Synch on Restart**

  *For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled, hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.*

- **Tone set**

  *This is the default tone set provided for the country that you select from the pull-down menu associated with this field.*

**e** Select the “Bearer” tab.

*The Bearer tab screen displays in the “Details of selected tree node” window.*

**f** In the Bearer tab screen, verify and/or enter information for the following fields:

- **Rtp Base Port**

  *This is the first port number used for real-time protocol streams on VoIP cards.*

  ***Note:*** This must be an even number. In addition, commas must not be entered in the number.

- **Annc Circuits per Card**

  *This is the number of circuits available for announcements on each bearer card in the system. This number is taken from the engineering data for the system. If IVR is enabled, this number should be greater than zero. The allowable values are one through the value of Max. Annc Circuits per Card.*

- **Conference Circuits per Card**

  *This is the number of circuits available for conferencing on each bearer card in the system. This number is taken from the engineering data for the system. If conferencing is enabled, this number should be greater than zero. The allowable values are one through the value of Max. Conf. Circuits per Card.*

- **Max. Annc Circuits per Card**

  *This is the maximum value for Annc Circuits per Card, for the network element. This number can vary depending on the software release of the network element and also depending on whether the network element is configured for IP or for ATM. The element manager uses this value to perform error checking on the user's input for Annc Circuits per Card.*

- **Max. Conf. Circuits per Card**

  *This is the maximum value for Conference Circuits per Card for the network element. This number can vary depending on the software release of the network element. The element manager uses this value to perform error checking on the user's input for Conference Circuits per Card.*

- **Transmit Gain**

  *This is the strength of a signal going out from the vocoder of an rtp endpoint as compared with the strength of a*

*signal going into the vocoder. Transmit Gain does not apply to conferencing service.*

- **Receive Gain**

  *This is the strength of a signal coming into an rtp endpoint from the decoder as compared with the strength of a signal coming into the decoder.*

- **Default TOS**

  *This field determines the Type of Service bit usage for this UAS, 0-255. The default is 0, which indicates “normal” delay, throughput, and reliability, with “routine” precedence.*

- **RFC2833 DTMF**

  *This field indicates how the UAS will determine whether RFC2833 is enabled for each RTP connection. RFC2833 defines a method for passing DTMF digits “out-of-band” in special RTP packets, in order to provide more reliable*

*DTMF recognition than is possible with low-bandwidth codecs. The possible selections include:*

— *AlwaysOff (RFC2833 support is always disabled, regardless of call control)*

— *Negotiated (RFC2833 support is enabled per call control messaging, that is, SDP and/or LCO negotiation)*

***Note:*** The setting should be AlwaysOff when announcements or conferencing are supported.

- **RFC2833 DTMF Squelch**

  *Not applicable*

- **G729B**

  *This field indicates G.729B audio codec support.*

- **Clock Sync Mode**

  *Not applicable*

- **Primary Clock Source**

  *Not applicable*

- **Secondary Clock Source**

  *Not applicable*

- **Clock Source Carrier Type**

  *Not applicable*

- **Supported Codec**

  *These check boxes determine which codecs, G711, G723, G726, G729, and T.38 are supported. The following guidelines should be followed when you are selecting the codecs:*

  — *T.38 is selectable only when at least one CG6000 card with BCT capability is installed in the system.*

  — *In an all-BCT system, all voice codecs should be disabled.*

  — *In a non-BCT system, up to a maximum of four voice codecs can be selected; the T.38 codec cannot be selected.*

  — *In a mixed system (BCT + IVR, BCT + Conf, BCT + IVR + Conf), up to a maximum of four of the codecs*

*can be selected; one of the four codecs selected must be a voice codec.*

— *In a non-BCT system supporting only conferencing service, G.729 must not be selected.*

— *It is recommended that you select G.711 for systems supporting conferencing service, to avoid any possible deterioration of voice quality.*

**g** Select the “Call Agent” tab.

*The Call Agent tab screen displays in the “Details of selected tree node” window.*

**h** In the Call Agent tab screen, verify and/or enter information for the following fields:

- **Primary Call Agent Name**

  *This is the computer name associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent IP Address**

  *This is the IP address associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent Port**

  *This is the port of the Call Agent application (default is 2944).*

- **UAS Call Control Port**

  *This is the port associated with receiving the call control message stream (default is 2944).*

- **Legacy Announcements**

  *This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.*

  ***Note:*** If Legacy Announcements is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Announcements is Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **Primary Languag**e

  *This is the primary language associated with the node.*

  ***Note:*** A Primary Language is required only if the Legacy Announcements field is Enabled. If Legacy

Announcements is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  *This is the secondary language associated with the node.*

  ***Note:*** A Secondary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Secondary Language field will also be Disabled.

**13** Select the “Log Levels” tab.

*The Log Levels tab screen displays in the “Details of selected tree node” window.*

**14** In the Log Levels tab screen, verify and/or enter information for the following fields:

- **System Log Level**

  *System logs are information, warning, or error events. This field specifies that the Main Subagent is to send either all logs for that source, only warning and error logs for that source, only error logs for that source, or no logs for that source to the element management station.*

- **UAS Log Level**

  *Audio Server logs include information, warning, or error events. This field specifies that the Main Subagent is to send either all logs for that source, only warning and error logs for that source, only error logs for that source, or no logs for that source to the element management station.*

- **Application Log Level**

  *Application logs include information, warning, or error events. This field specifies that the Main Subagent is to send either all logs for that source, only warning and error logs for that source, only error logs for that source, or no logs for that source to the element management station.*

- **Security Log Level**

  *Logs are either audit-succeed or audit-fail. This field specifies that the Main Subagent is to send either all security*

*logs, only audit-fail logs, or no logs for that source to the element management station.*

**15** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step 16 |
| you do not want to save the information | step 19 |

**16** Click Validate.

**17** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK in the confirmation screen and then click OK in the acknowledgement screen.

**18** Go to step 20.

**19** Click Cancel.

*The entries in the screen fields revert to the default values.*

**20** Determine whether SNMP management configuration parameters need to be changed.

| If | Do |
|---|---|
| SNMP management configuration parameters need to be changed | step 21 |
| SNMP management configuration parameters do not need to be changed | step 22 |

**21** Click the “Reconfigure SNMP” button, located at the bottom of the Local Configuration Interface GUI screen.

*An SNMP re-configuration warning pop-up window displays. When you click OK in response to the message in the pop-up window, the Local Configuration Interface GUI SNMP window displays, showing default values delivered with the UAS system.*

**a** Enter information for the following fields in the screen:

- **v2c read/write community**

  This is the SNMPv2c community name for read/write access through the SNMP-based management station.

- **v2c read only community**

  This is the SNMPv2c community name for read-only access through the SNMP-based management station.

- **v3 read/write user**

  This is the SNMPv3 community name for read/write access through the SNMP-based management station.

- **v3 read only user**

  This is the SNMPv3 community name for read-only access through the SNMP-based management station.

- **trap version**

  This is the SNMP version of the SNMP traps sent by the UAS.

- **trap destination**

  This is the destination IP address associated with the remote SNMP management station. This is the address to which SNMP traps are sent.

- **trap port**

  This is the UDP port associated with the remote SNMP management station.

**b** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step c |
| you do not want to save the information | step f |

**c** Click OK.

**d** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK in the confirmation screen and then click OK in the acknowledgement screen.

**e** Go to step 22.

**f** Click Cancel.

*The entries in the screen fields revert to the default values.*

**22** Determine whether the bearer fabric of the UAS you are installing is ATM or IP.

| If | Do |
|---|---|
| the bearer fabric type is IP | step 24 |
| the bearer fabric type is ATM | step 23 |

**23** Close the Local Configuration Interface GUI screens by pulling down the menu under File and selecting “Exit”.

**a** Go to step 26.

**24** In the Network element Tree pane, select the “Cards” folder, which is located in the Nodes folder.

*The “Details of selected tree node” card screen displays.*

**a** Review the card list. The Card Type field will be set automatically to “CG6000C” if a card is present. The Card Type field will be set to “none” and the information detail field labels will be colored grey, if no card is present. Note the current configuration.

| If | Do |
|---|---|
| card information is not to be changed | step j |
| card information is to be changed, | step b |

**b** Double click the “Cards” folder, located in the Network element Tree pane and, from the list of cards that displays below the “Cards Folder”, click the bullet associated with a card to be changed.

*A card detail window displays in the “Details of selected tree node” screen.*

**c** Enter information in the following fields in the dedicated card details window:

- IP address associated with each CG6000C card
- default router associated with each CG6000C card
- network mask associated with each CG6000C card
- Bearer Channel Tandeming (BCT) support capability for each CG6000C card, either Enabled or Disabled.
- Test Trunk Support; select either Enabled or Disabled
- Test Trunk Config Size; select the appropriate size (small - 50k trunks; medium - 100k trunks; large - 200k trunks), when Test Trunk Support is Enabled. This determines the number of channels available for tests.

- Sage Box 1 IP (address); enter when Test Trunk Support is Enabled. One Sage test box is use for small and medium test trunk configurations.
- Sage Box 2 IP (address); enter if a second Sage test box is required, when Test Trunk Support is Enabled. Two Sage test boxes are used for large configurations.

**d** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step e |
| you do not want to save the information | step h |

**e** Click Validate.

**f** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

**g** Go to step i.

**h** Click Cancel.

**i** Either return to step a and enter information for another card, or go to step j.

**j** Close the Local Configuration Interface GUI screens by pulling down the menu under File and selecting “Exit”.

**25** If you are installing a PRI gateway, and if you are performing an upgrade, you should already have a valid “ugw.conf” file; go to step 26. If you are installing a PRI gateway, and if you are performing a ground-up installation, ftp a new ugw.conf file to c:\uas\etc. Contact UAS Product Design if you need a new ugw.conf file, then go to step 26.

**26** This optional step validates configuration files and updates other configuration files. Any problems encountered will cause error messages to display in the command window. Note that this same action is performed upon the next application start-up.

**a** select **Start -> Run**

**b** type **cmd** in the window that displays

**c** press Enter

**d** Enter the following command in the window that displays:

```
configmgr -update -v
```

**e** press Enter

**27** This optional step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server. For additional information about this capability, see the "UAS system configuration backup/restore strategy" in the "Tools and Utilities" section of this document. The following steps are performed on a remote Unix system.

**a** Open a telnet session with 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
```

**b** Configure NFS to share the "/opt/uas" file system 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
```

**c** 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
```

**d** At your local 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" of the UAS07 document, NN10095-511, entitled "UAS Configuration Management."

**28** Start the application by performing the following steps:

a select **Start -> Run**

b enter **net start pmgrdaemon** in the window that displays

c press Enter

29 If you installed the software from a CD, remove the installation CD from the CD-ROM drive.

30 Inspect the UAS installation log file (UASinstLog.txt) for indications of any errors that may have occurred during the application software installation. The file is located in the c:\winnt\temp directory. If you find errors, contact your next level of support or your Nortel Networks service representative for assistance.

31 For ATM bearer fabric systems, this step ensures that the ATM cards have been upgraded with the latest firmware.

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d Enter the following command in the window that displays:

```
atmfirmware -upgrade
```

e press Enter

f select **Start -> Shutdown**

g select “restart the computer” in the Shutdown Windows screen.

32 Contact your Nortel Networks service representative to determine whether any patches need to be applied to the newly-installed UAS08 software.

33 To adjust the system time to your time zone, perform the following steps:

a select **Start -> Settings -> Control Panel -> Date/Time Window**

b select the Time Zone tab, adjust the time in the window that displays, and then click OK

34 You have completed this procedure.

# UAS08 to UAS08 upgrade

The following procedure enables you to perform a release UAS08 to UAS08 upgrade.



**CAUTION**

No remote access sessions (telnet, ftp) should be in progress on a unit that is being upgraded.

## UAS08 to UAS08 Upgrade

***At your console***

**1** Using the APS Administration GUI procedure “Disabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” disable audio provisioning for this UAS unit.

**2** Using the Universal Audio Server Manager, look in the States window of the Network Element Status panel at the Usage category to determine whether the UAS is active and is processing calls. If the UAS is idle, proceed to step 3 of this procedure. If the UAS is active, determine whether any conferences are in progress by pulling down the Component menu in the System Identification window of the Network Element Status panel and selecting “conferencing service.” From the “conferences in progress” value in the component-specific panel of the Performance tab screen, determine whether to proceed to step 3 of this procedure: if conferences are in progress, wait until they complete; if conferences are not in progress, proceed with this procedure.

**3** Using the procedure “Changing the Admin state,” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state for this UAS unit being upgraded to “lock graceful.”

*The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.*

4 Uninstall (remove) the release UAS08 software by performing the procedure, “UAS08 application software removal” in *Upgrading the UAS*, NN10047-461.

***Note:*** You must remove any patches applied to the software, in addition to the software.

5 Install the UAS08 software by performing the procedure, UAS08 application software installation on page 941.

6 Determine whether audio distribution is to be enabled on the node you are upgrading.

| If | Do |
|---|---|
| you are upgrading an ATM-AAL1, SIP conference-only, or PRI node | step 9 |
| you are not upgrading an ATM-AAL1, SIP conference-only, or PRI node | step 7 |

7 Enable audio distribution at the APS for this UAS unit by performing the procedure “Enabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management.”

8 Perform the procedure entitled “Provisioning a UAS node,” in the document, NN10095-511, entitled, “UAS Configuration Management,” to force immediate provisioning of any files created before the start of the upgrade.

9 Using the procedure “Changing the Admin state,” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state for this UAS unit to “unlocked.”

*The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.*

10 Using the procedure “Viewing UAS performance measurements,” in the document, NN10139-711, entitled “UAS Performance Management,” verify that the UAS unit is enabled and is processing calls. In the procedure view, specifically, the performance measurements for the “Conferencing Service” and “IVR Service” components.

11 Update any remaining UAS units by performing this procedure for each unit.

12 Reactivate audio provisioning capability for system users by performing the procedure “Editing user profiles,” in the document, NN10095-511, entitled “UAS Configuration Management,” changing the user status of all system users to “activated.”

13 You have completed this procedure.

# Installing OS and system software on a Win2K AS

This procedure enables you to install Win2K OS and system software on a single Win2K application server host processor.

Before you start performing this procedure, it is important that you have satisfied the following requirements:

- the UAS SAM16 application server hardware has been properly configured. Refer to NTP 203-7009-201, *Hardware Installation Guide* for information about configuring SAM16 hardware.
- the CD-ROM entitled “Win2K: Win2K OS and System Software for CPV 5350, GS v3.3” or “Win2K: Win2K OS and System Software for CPV 5370, GS v3.3” is available
- you have identified the type SCSI adapter(s) PMC configured in your system

## Installing OS and system software on a Win2K AS

***At your console:***

**1** Prepare the SAM16 for the Win2K installation by turning the machine on.

***Note:*** This step needs to be performed only during a ground-up installation.

**2** Restart the system by performing the following steps:

**a** select **Start -> Shutdown**

**b** Select “restart” in the Shutdown Windows screen.

***Note:*** This step is applicable only if you are upgrading the system.

3 During the boot process, break into the BIOS menu using function key (F2) and change the BIOS settings for the processor card your system is equipped with.

***Note:*** Ensure that a CD is not present in the CD-ROM drive while you are checking the BIOS settings.

| If your system is configured with | Refer to |
|---|---|
| CPV5350 card | "BIOS Settings for CPV5350 SCSI" in the document, NN10073-911, entitled "UAS Fault Management" in your UAS document suite |
| CPV5370 card | "BIOS Settings for CPV5370 SCSI" in the document, NN10073-911, entitled "UAS Fault Management " in your UAS document suite |

4 Insert the bootable CD-ROM, "Win2K: Win2K OS and System Software for CPV5350, GS v3.3" or "Win2K: Win2K OS and System Software for CPV5370, GS v3.3" into the CD-ROM drive of the domain (A or B) of the application server on which you are installing operating system software.

5 Exit the BIOS settings menu, saving changes by using the function key (F10).

6 Select "Yes" in the Setup Confirmation window that displays.

*The system responds by automatically restarting and displaying the MS-DOS 6.2 Startup Menu.*

***Note:*** If the MS-DOS 6.2 Startup Menu does not display, contact your next level of support.

7 At this point, the installation CD can continue unattended. Part or all of the hard drive will need to be reformatted, depending on the previous configuration. The system may reboot one or more times and continue automatically through the MS-DOS menu and, eventually, into the Ghost installation applications that install the Global Server OS and System Software.

***Note:*** If the hard drive has been used previously in a system that could not be shut down cleanly, as described in step 2, error messages may display. These messages should be ignored. Perform the following steps in response to the

messages, but do not QUIT or restart the system until the Ghost installation has completed.

- Select “OK” if the message, “NTFS ERROR: NTFS log file has not been flushed(fl=1). Restart NT then try again,” displays.
- Use the Tab and Enter keys to select “Continue” in the resulting pop-up window that displays, “NTFS Problem Detected: Ghost has detected problems with an NTFS partition. Recommend that you quit ghost and correct the problem by rebooting NT and running chkdsk. May also choose to continue normally, or perform a sector by sector copy of partition. QUIT; CONTINUE; SECTOR COPY.”

*The installation will continue and install successfully.*

**8** The installation will take about 30 minutes, during which various status and progress messages will be issued to the console. At the end of the installation, the message, “Loading of system partition complete ...” will display. Remove the CD from the CD-ROM drive and then press the **Ctrl** - **Alt** - **Delete** key combination.

***Note:*** The initial reboot of the Windows operating system will take slightly longer than usual; do not be concerned. After the system reboots, several status windows display as the installation proceeds. The installation will complete in approximately 5 minutes. Wait until all installation activity completes before making any keystrokes or mouse activity. Then, dismiss any new hardware wizard-related windows that display by clicking the “Cancel” button. DO NOT reboot the system at any point in this procedure. Dismiss any reboot pop-up windows by selecting “No”.

**9** You have completed this procedure.

# UAS06 application software installation

This procedure enables you to install the UAS06 application software.

### UAS06 application software installation

***At your console***

**1** Close all applications.

**2** Insert the UAS06 installation CD into the CD-ROM drive.

**3** Launch the InstallShield Wizard for Universal Audio Server program by performing the following steps:

**a** select **Start -> Run**

**b** In the Run window, click Browse.

**c** In the Browse window, navigate to the file, *<cd-rom>*: \winnt\setup.exe, and click Open.

***Note:*** *<cd-rom>* is the “drive letter” assigned to the CD-ROM device.

*The Welcome window for the InstallShield Wizard for Universal Audio Server displays.*

**d** Click OK.

**4** In the Welcome window for the InstallShield, click Next.

*The Choose Node Type screen displays.*

**5** Select the appropriate gateway type, Gateway or Universal Audio Server (audio server).

| If | Do |
|---|---|
| you chose Gateway | step 6 |
| you chose Universal Audio Server | step 7 |

**6** In the screen that displays, select “PRI” and then click Next.

**a** Go to step 11.

**7** Select the bearer fabric type of your system, either IP or ATM.

| If | Do |
|---|---|
| you chose IP | step 11 |
| you chose ATM | step 8 |

**8** Select the appropriate ATM bearer fabric type.

| If | Do |
|---|---|
| the UAS bearer fabric type is ATM-AAL1 | step 9 |
| the UAS bearer fabric type is ATM-AAL2 | step 10 |

**9** In the InstallShield Wizard Complete screen, click Finish.

***Note 1:*** Up to 60 seconds may pass before the InstallShield Wizard Complete screen first appears.

***Note 2:*** If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

**a** Perform the following steps to install the PCI drivers:

**i** Right-click My computer, and then select “Properties.”

**ii** In the pop-up window that displays, select the Hardware tab and click Device Manager (located in the middle of the window).

**iii** In the Device Manager window that displays, right-click PCI Memory Controller (located under “Other devices” on the window) and select “Properties.”

**iv** In the PCI Memory Controller Properties window that displays, select the Driver tab and then click the Update Driver button.

**v** In the Upgrade Device Driver Wizard window that displays, click Next.

**vi** In the Install Hardware Device Drivers subscreen (of the Upgrade Device Driver Wizard window), the radio button, “Search for a suitable driver for my device” is selected by default. Click Next.

**vii** In Locate Driver Files subscreen (of the Upgrade Device Driver Wizard window), deselect “Floppy disk driver” and “CD-ROM driver”, then select “Specify a location” box, and, finally, click Next.

**viii** In the Upgrade Device Driver Wizard pop-up window, type (or browse for) “c:\NMS_PA200\Pa200\system” in the “Copy manufacturer’s files from” box, and then click OK.

**ix** In the Driver Files Search Results subscreen (of the Upgrade Device Driver Wizard window), click Next.

**x** In the Completing the Upgrade Device Driver Wizard subscreen (of the Upgrade Device Driver Wizard window), click Finish.

**xi** In the PA200 Base Board WDM Properties window, click Close.

**xii** Close the Device Manager window (click X, located in the upper right-hand corner of the window).

**xiii** Close the System Properties window (click OK).

**b** Re-boot the system by performing the following steps:

**i** select **Start -> Shutdown**

**ii** select “restart the computer” in the Shutdown Windows screen.

**c** After the system re-boots, log back into the system as “administrator” (user name), and enter “superuser” as the password.

**d** Open a command line interface at the UAS:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

**v** press Enter

**vi** If you are performing an upgrade and you do not want to change configuration file content, go to step 17, otherwise continue with the next step.

**e** Launch the Local Configuration Interface GUI by performing the following steps:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **lci** on the command line

***Note:*** The first letter in the lci command is an “l”, as in “local.”

**v** press Enter

*The Bearer Type ATM/AAL1 Local Configuration Interface GUI screen displays.*

**f** Enter information for the following fields in the screen:

***Note 1:*** Fields containing default data that cannot be changed appear in the color grey.

***Note 2:*** When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  *This is the computer name associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent IP Address**

  *This is the IP address associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent Port**

  *This is the port of the Call Agent application (default is 2427).*

- **Atm Companding Mode**

  *This is the companding mode, either A-Law or Mu-Law.*

- **Primary DBServer Host**

  *This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the*

*system does not support its own APS, accept the default settings.*

- **Primary DBServer IP**

  *This is the IP address of the APS that is hosting the database server used by this UAS node.*

- **Backup Storage IP**

  *This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.*

**g** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step h |
| you do not want to save the information | step k |

**h** Click Apply.

**i** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

**j** Go to step 12.

**k** Click Cancel.

*The entries in the screen fields revert to the default values.*

**l** Either return to step f and enter new information in the screen or go to step 12.

**10** In the InstallShield Wizard Complete screen, click Finish.

***Note 1:*** Up to 30 seconds may pass before the InstallShield Wizard Complete screen first appears.

***Note 2:*** If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

**a** Perform the following steps to install the ArTeMux S007 drivers, protocol, and bindings:

**i** Right-click My computer, and then select “Properties.”

**ii** In the pop-up window that displays, select the Hardware tab and click Device Manager (located in the middle of the window).

**iii** In the Device Manager window that displays, right-click ATM Network Controller (located under “Other devices” on the window) and select “Properties.”

**iv** In the ATM Network Controller Properties pop-up window that displays, click the Reinstall Driver button, located at the bottom of the window.

**v** In the Upgrade Device Driver Wizard window that displays, click Next.

**vi** In the Install Hardware Device Drivers window that displays, select the radio button that asks to “Display a list of the known drivers for this device ...”, and then click Next.

**vii** In the Hardware Type window that displays, select “Network Adapters” and then click Next.

**viii** In the Select Network Adapter window that displays, click the Have Disk button, located below the list of network adapters in the window.

**ix** In the Install From Disk window that displays, you may either:

click the Browse button and then select **“Open”**

or

enter **c: \ArTeMux\Driver\s00x_W2K** to the left of the Browse button

**x** In the Install From Disk window that displays, click OK after the directory name appears correctly in the line next to the Browse button.

**xi** In the Select Network Adapter window that displays, choose (highlight) “ArTeMux s00x Adapter - Win2K” and then click Next.

**xii** In the Update Driver Warning pop-up window that displays, click Yes.

**xiii** In the Start Device Driver Installation window that displays, click Next.

*A window that shows the progress of the installation displays for about 60 seconds.*

**xiv** In the Update Device Driver Wizard window that displays, “Completing the Upgrade Device Driver Wizard” and lists the ArTeMux s00x Adapter - Win2K, click Finish.

**xv** In response to the query about restarting the computer that appears in the System Settings Change window, enter “No.”

**xvi** The Device Manager lists the network adapters, including the s00x adapter. Exit from the window by pressing the “X” located in the upper right corner of the window.

**xvii** In the System Properties window, click OK.

**xviii** Right-click the “My Network Places” icon, and select “Properties.”

**xix** When the four local area connections display, right-click the last (fourth) one, and select “Properties.”

**xx** Choose “Install” in the Local Area Connection 4 Properties window.

**xxi** In the Select Network Component Type window that displays, choose “Protocol” and click the Add ... button.

**xxii** In the Select Network Protocol window that displays, click the Have Disk ... button.

**xxiii** In the Install From Disk window that displays, you may either:

click the Browse button and then select **“Open”**

or

enter **c: \ArTeMux\Protocol\W2K** to the left of the Browse button

**xxiv** In the Install From Disk window that displays, click OK after the directory name appears correctly in the “Copy manufacturer’s files from:” field, located next to the Browse button.

**xxv** In the Select Network Protocol window that displays, choose (highlight) “ArTeMux Protocol Driver” and then click OK.

*A file transfer progress window displays briefly.*

**xxvi** In the Local Area Connection 4 Properties window, deselect (remove the check marks from) all protocols except the ArTeMux Protocol Driver, and then click Close.

**xxvii** Right-click the “My Network Places” icon, and select “Properties.”

**xxviii** When the four local area connections display, right-click Local Area Connection 3, and select “Properties.” If checked, deselect the ArTeMux Protocol Driver from the components list. Click OK.

**xxix** Following the procedure outlined in steps xxvii and xxviii, ensure that for both the Local Area Connection 2 and Local Area Connection the ArTeMux Protocol Driver is not selected.

**b** Re-boot the system by performing the following steps:

**i** select **Start -> Shutdown**

**ii** select “restart the computer” in the Shutdown Windows screen.

**c** After the system re-boots, log back into the system as “administrator” (user name), and enter “superuser” as the password.

**d** Open a command line interface at the UAS:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

**v** press Enter

**vi** If you are performing an upgrade and you do not want to change configuration file content, go to step 17, otherwise continue with the next step.

**e** Launch the Local Configuration Interface GUI by performing the following steps:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **lci** on the command line

***Note:*** The first letter in the lci command is an “l”, as in “local.”

**v** press Enter

*The Bearer Type ATM/AAL2 Local Configuration Interface GUI screen displays.*

**f** Enter information for the following fields in the screen:

***Note 1:*** Fields containing default data that cannot be changed appear in the color grey.

***Note 2:*** When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  *This is the computer name associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent IP Address**

  *This is the IP address associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent Port**

  *This is the port of the Call Agent application (default is 2427).*

- **Legacy Call Server**

  *This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.*

  ***Note:*** If Legacy Call Server is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Call Server is Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **Audio Synch on Restart**

  *For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled,*

*hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.*

- **Atm Companding Mode**

  *This is the companding mode, either A-Law or Mu-Law.*

- **Primary Language**

  *This is the primary language associated with the node.*

  ***Note:*** A Primary Language is required only if the Legacy Call Server field is Enabled. If Legacy Call Server is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  *This is the secondary language associated with the node.*

  ***Note:*** A Secondary Language is required only if the Legacy Call Server field is Enabled. If Legacy Call Server is Disabled, then the Secondary Language field will also be Disabled.

- **Primary DBServer Host**

  *This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, accept the default settings.*

- **Primary DBServer IP**

  *This is the IP address of the APS that is hosting the database server used by this UAS node.*

- **Backup Storage IP**

  *This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.*

- **Gateway Control Protocol**

  *This is the control protocol for the UAS, either H.248 or MGCP.*

**g** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step h |

| If | Do |
|---|---|
| you do not want to save the information | step k |

**h** Click Apply.

**i** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

**j** Go to step 12.

**k** Click Cancel.

*The entries in the screen fields revert to the default values.*

**l** Either return to step f and enter new information in the screen or go to step 12.

**11** In the InstallShield Wizard Complete screen, which displays after a slight delay, select “Yes, I want to restart my computer now.” Click Finish.

***Note 1:*** The system re-boot (restart) is required in order for the installation program to complete registry updates.

***Note 2:*** If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

**a** After the system re-boots, log back into the system as “administrator” (user name), and enter “superuser” as the password.

**b** Open a command line interface at the UAS:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

**v** press Enter

**vi** If you are performing an upgrade and you do not want to change configuration file content, go to step 17, otherwise continue with the next step.

**c** Launch the Local Configuration Interface GUI by performing the following step:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **lci** on the command line

***Note:*** The first letter in the lci command is an “l”, as in “local.”

**v** press Enter

*The Bearer Type IP Local Configuration Interface GUI screen displays.*

**d** Enter information for the following fields in the screen:

***Note:*** When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes

can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  *This is the computer name associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent IP Address**

  *This is the IP address associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent Port**

  *This is the port of the Call Agent application (default is 2427).*

- **Rtp Base Port**

  *This is the number of base ports for the RTP stream, within the range 1024 through 63094*.

  ***Note:*** This must be an even number. In addition, commas must not be entered in the number.

- **Legacy Call Server**

  *This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.*

  ***Note:*** If Legacy Call Server is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Call Server is Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **IVR Support**

  *This field determines whether IVR support is enabled in this system.*

- **Audio Synch on Restart**

  *For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled,*

*hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.*

- **Primary Language**

  *This is the primary language associated with the node.*

  ***Note:*** A Primary Language is required only if the Legacy Call Server field is Enabled. If Legacy Call Server is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  *This is the secondary language associated with the node.*

  ***Note:*** A Secondary Language is required only if the Legacy Call Server field is Enabled. If Legacy Call Server is Disabled, then the Secondary Language field will also be Disabled.

- **Conferencing State:**

  *This field determines whether Conferencing is enabled in this node.*

  ***Note:*** If Conferencing State is Disabled, then the Conference Spanning field is also Disabled.

- **Conference Spanning**

  *This field determines whether Conference Spanning is supported by the node.*

  ***Note:*** If “Conferencing State” is Disabled, then the Conference Spanning field is also Disabled.

- **Primary DBServer Host**

  *This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the*

*system does not support its own APS, accept the default settings.*

- **Primary DBServer IP**

  *This is the IP address of the APS that is hosting the database server used by this UAS node.*

- **Backup Storage IP**

  *This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.*

- **Gateway Control Protocol**

  *This is the control protocol for the UAS, either H.248 or MGCP.*

  ***Note:*** This field can be datafilled only for systems with bearer type IP and bearer type ATM-AAL2.

- **Force G711**

  *This field indicates G.711 audio codec support.*

  ***Note:*** If Force G711 is Enabled, then the G729B field is Disabled.

- **G729B**

  *This field indicates G.729B audio codec support.*

**e** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step f |
| you do not want to save the information | step i |

**f** Click Apply.

**g** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

**h** Go to step 12.

**i** Click Cancel.

*The entries in the screen fields revert to the default values.*

**j** Either return to step d and enter new information in the screen or go to step 12.

**12** Determine whether SNMP management configuration parameters need to be changed.

| If | Do |
|---|---|
| SNMP management configuration parameters need to be changed | step 13 |
| SNMP management configuration parameters do not need to be changed | step 14 |

**13** Click the "Reconfigure SNMP" button, located at the bottom of the Local Configuration Interface GUI screen.

*The Local Configuration Interface GUI SNMP screen displays, showing default values delivered with the UAS06 system.*

**a** Enter information for the following fields in the screen:

- **v2c read/write community**

  This is the SNMPv2c community name for read/write access through the SNMP-based management station.

- **v2c read only community**

  This is the SNMPv2c community name for read-only access through the SNMP-based management station.

- **v3 read/write user**

  This is the SNMPv3 community name for read/write access through the SNMP-based management station.

- **v3 read only user**

  This is the SNMPv3 community name for read-only access through the SNMP-based management station.

- **trap version**

  This is the SNMP version of the SNMP traps sent by the UAS.

- **trap destination**

  This is the destination IP address associated with the remote SNMP management station. This is the destination IP address associated with the remote SNMP

management station. This is the address to which SNMP traps are sent.

- **trap port**

  This is the UDP port associated with the remote SNMP management station.

**b** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step c |
| you do not want to save the information | step f |

**c** Click OK.

**d** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

**e** Go to step 14.

**f** Click Cancel.

*The entries in the screen fields revert to the default values.*

**g** Either return to step 13 and enter new information in the screen fields or go to step 14.

**14** Determine whether the bearer fabric of the UAS you are installing is ATM or IP.

| If | Do |
|---|---|
| the bearer fabric type is IP | step 16 |
| the bearer fabric type is ATM | step 15 |

**15** Close the Local Configuration Interface GUI screens by selecting **File -> Exit**

**a** Go to step 17.

**16** In the Topology pane of the Local Configuration Interface GUI screen, select the “Nodes” folder and then select the “Cards” folder, which is located in the Nodes folder.

*The Local Configuration Interface GUI cards screen displays.*

**a** Review the card list. The Card Type field will be set automatically to “CG6000C” if a card is present. The Card Type field will be set to “none” and the information detail field

labels will be colored grey, if no card is present. Note the current configuration.

| If | Do |
|---|---|
| If card information is not to be changed | step i |
| If card information is to be changed, | step b |

**b** Double click the “Cards” folder, located in the Topology pane and, from the list of cards that displays below the Cards folder, click the bullet associated with a card to be changed. Enter information in the following fields in the dedicated card details screen that displays:

- IP address associated with each CG6000C card
- default router associated with each CG6000C card
- network mask associated with each CG6000C card
- Bearer Channel Tandeming (BCT) support capability for each CG6000C card, either Enabled or Disabled.

**c** For each card, determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step d |
| you do not want to save the information | step g |

**d** Click Apply.

**e** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI card detail screen) and select “Save”. Click OK when the confirmation screen displays.

**f** When you have finished updating the cards, go to step i.

**g** Click Cancel.

**h** Either return to step b and enter information for another card, or go to step i.

**i** Close the Local Configuration Interface GUI screens by selecting **File -> Exit**

**17** If you are installing a PRI gateway, and if you are performing an upgrade, you should already have a valid “ugw.conf” file; go to step 18. If you are installing a PRI gateway, and if you are

performing a ground-up installation, ftp a new ugw.conf file to c:\uas\etc. Contact UAS Product Design if you need a new ugw.conf file, then go to step 18.

***Note:*** This step is to be performed only if you are installing a PRI gateway. If you are not installing a PRI gateway, go to step 18.

**18** This optional step validates configuration files and updates other configuration files. Any problems encountered will cause error messages to display in the command window. Note that this same action is performed upon the next application start-up.

**a** select **Start -> Run**

**b** type **cmd** in the window that displays

**c** press Enter

**d** Enter the following command in the window that displays:

```
ConfigMgr -install -v
```

**e** press Enter

**19** This optional step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server. For additional information about this capability, see Automatic configuration file back-up on page 333. The following steps are performed on a remote Unix system.

**a** In a Unix shell, as Root user, 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
```

**b** 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
```

c 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
```

20 Start the application by performing the following steps:

a select **Start -> Run**

b enter **net start pmgrdaemon** in the window that displays

c press Enter

21 Inspect the UAS installation log file (UASinstLog.txt) for indications of any errors that may have occurred during the application software installation. The file is located in the c:\winnt\temp directory. If you find errors, contact your next level of support or your Nortel Networks service representative for assistance.

22 Refer to any existing UAS06 patch documentation and reapply any patches that had been previously applied to the UAS06 software now.

23 You have completed this procedure.

# UAS07 application software installation

This procedure enables you to install the UAS07 application software.

### UAS07 application software installation

***At your console***

**1** Close all applications.

**2** Insert the UAS07 installation CD into the CD-ROM drive.

**3** Launch the InstallShield Wizard for Universal Audio Server program by performing the following steps:

**a** select **Start -> Run**

**b** In the Run window, click Browse.

**c** In the Browse window, navigate to the file, *<cd-rom>*: \winnt\setup.exe, select the file, and click Open.

***Note:*** *<cd-rom>* is the “drive letter” assigned to the CD-ROM device.

**d** Click OK.

*The Welcome window for the InstallShield Wizard for Universal Audio Server displays.*

**4** In the Welcome window for the InstallShield, click Next.

*The Choose Node Type screen displays.*

**5** Select the appropriate gateway type, Gateway or Universal Audio Server (audio server).

| If | Do |
|---|---|
| you chose Gateway (in support of release IMS 1.0 or IMS 1.1) | step 6 |
| you chose Universal Audio Server | step 8 |

**6** Click Next.

**7** In the screen that displays, select “PRI” and then click Next.

**a** Go to step 11.

**8** Select the bearer fabric type of your system, either IP or ATM.

| If | Do |
|---|---|
| you chose IP | step 11 |
| you chose ATM | step 9 |

**9** In the InstallShield Wizard Complete screen, click Finish.

***Note 1:*** Up to 60 seconds may pass before the InstallShield Wizard Complete screen first appears.

***Note 2:*** If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

**10** Perform the following steps.

**a** Perform the following steps to install the PCI drivers:

**i** Right-click My computer, and then select “Properties.”

**ii** In the pop-up window that displays, select the Hardware tab and click Device Manager (located in the middle of the window).

**iii** In the Device Manager window that displays, right-click PCI Memory Controller (located under “TDM/ATM bridge 2” on the window) and select “Properties.”

***Note:*** For ground-up installations, PCI Memory Controller will appear under “Other devices” on the window.

**iv** In the PCI Memory Controller Properties window that displays, select the Driver tab and then click the Update Driver button.

**v** In the Upgrade Device Driver Wizard window that displays, click Next.

**vi** In the Install Hardware Device Drivers subscreen (of the Upgrade Device Driver Wizard window), the radio button, “Search for a suitable driver for my device” is selected by default. Click Next.

**vii** In Locate Driver Files subscreen (of the Upgrade Device Driver Wizard window), deselect “Floppy disk driver” and

"CD-ROM driver", then select "Specify a location" box, and, finally, click Next.

**viii** In the Upgrade Device Driver Wizard pop-up window, type (or browse for) "c:\NMS_PA200\Pa200\system" in the "Copy manufacturer's files from" box, and then click OK.

**ix** In the Driver Files Search Results subscreen (of the Upgrade Device Driver Wizard window), click Next.

**x** In the Completing the Upgrade Device Driver Wizard subscreen (of the Upgrade Device Driver Wizard window), click Finish.

**xi** In the PA200 Base Board WDM Properties window, click Close.

**xii** Close the Device Manager window (click X, located in the upper right-hand corner of the window).

**xiii** Close the System Properties window (click OK).

**b** Re-boot the system by performing the following steps:

**i** select **Start -> Shutdown**

**ii** select "restart the computer" in the Shutdown Windows screen.

**c** After the system re-boots, log back into the system as "administrator" (user name), and enter either "superuser" as the password or the password supplied by your network administrator.

**d** Open a command line interface at the UAS:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

**v** press Enter

**e** Launch the Local Configuration Interface GUI by performing the following steps:

**i** select **Start -> Run**

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

**iii** press Enter

**iv** type **lci** on the command line

***Note:*** The first letter in the lci command is an “l”, as in “local.”

**v** press Enter

*The main Local Configuration Interface GUI screen displays.*

**vi** select the “nodes” folder in the Network Element Tree pane.

*An ATM Local Configuration Interface GUI screen displays.*

**f** Examine the Adaptation Layer heading on the screen and ensure that the appropriate screen for the ATM bearer fabric type of your system displays.

| If | Do |
|---|---|
| the appropriate screen for the bearer fabric type displays | step h |
| the appropriate screen for the bearer fabric type does not display | step g |

**g** Pull down the Adaptation Layer menu and select the appropriate bearer fabric type.

*An ATM Local Configuration Interface GUI screen for your fabric type displays.*

| If | Do |
|---|---|
| your UAS bearer fabric type is ATM-AAL1 | step i |
| your UAS bearer fabric type is ATM-AAL2 | step k |

**h** Determine whether the fabric type of your system is ATM-AAL1 or ATM-AAL2.

| If | Do |
|---|---|
| your UAS bearer fabric type is ATM-AAL1 | step i |
| your UAS bearer fabric type is ATM-AAL2 | step k |

i Verify and/or enter information for the following fields in the screen:

***Note 1:*** Fields containing default data that cannot be changed appear in the color grey.

***Note 2:*** When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  *This is the computer name associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent IP Address**

  *This is the IP address associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent Port**

  *This is the port of the Call Agent application (default is 2944).*

- **UAS Call Control Port**

  *This is the port associated with receiving the call control message stream (default is 2944).*

- **Atm Companding Mode**

  *This is the companding mode, either A-Law or Mu-Law.*

- **Optical Carrier Mode**

  *This field allows selection of the appropriate optical carrier standard for your ATM card, either SONET (a North American standard for optical carriers) or SDH (a European standard for optical carriers). The default for AAL1 systems is SONET.*

- **IVR Support**

  *This indicates whether IVR support is enabled on this system.*

- **Backup Storage IP**

  *This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.*

- **ATM CTone Support**

*This field, which must be datafilled when ATM BCT Support is ENABLED (ATM BCT Support is always ENABLED for an AAL1 system), determines how the audio endpoints for the ATM card are defined. The possible responses are: ENABLED or DISABLED.*

- **NTP Server IP**

  *This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.*

  ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

**j** Go to step l.

**k** Verify and/or enter information for the following fields in the screen:

***Note 1:*** Fields containing default data that cannot be changed appear in the color grey.

***Note 2:*** When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes

can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  *This is the computer name associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent IP Address**

  *This is the IP address associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent Port**

  *This is the port of the Call Agent application (default is 2944).*

- **UAS Call Control Port**

  *This is the port associated with receiving the call control message stream.*

- **Gateway Control Protocol**

  *This is the control protocol for the UAS, either H.248 or MGCP.*

- **Atm Companding Mode**

  *This is the companding mode, either A-Law or Mu-Law.*

- **Optical Carrier Mode**

  *This field allows selection of the appropriate optical carrier standard for your ATM card, either SONET (a North American standard for optical carriers) or SDH (a European standard for optical carriers). The default for AAL2 systems (including wireless systems) is SDH. If a North American AAL2 system is being configured, this field must be set to SONET.*

- **Legacy Announcements**

  *This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.*

  ***Note:*** If Legacy Announcements is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Announcements field is

Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **IVR Support**

  *This field determines whether IVR support is enabled in this system.*

- **Primary Language**

  *This is the primary language associated with the node.*

  ***Note:*** A Primary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  *This is the secondary language associated with the node.*

  ***Note:*** A Secondary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Secondary Language field will also be Disabled.

- **Audio Synch on Restart**

  *For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled, hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.*

- **Primary DBServer Host**

  *This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, accept the default settings.*

- **Primary DBServer IP**

  *This is the IP address of the APS that is hosting the database server used by this UAS node.*

- **Backup Storage IP**

  *This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.*

- **ATM BCT Support**

*This indicates whether Bearer Channel Tandeming is supported on this system*

- **ATM CTone Support**

  *This field, which must be datafilled when ATM BCT Support is ENABLED, determines how the audio endpoints for the ATM card are defined. The possible responses are: ENABLED or DISABLED.*

- **NTP Server IP**

  *This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.*

  ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

**l** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step m |
| you do not want to save the information | step p |

**m** Click Apply.

**n** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

**o** Go to step 12.

**p** Click Cancel.

*The entries in the screen fields revert to the default values.*

**q** Either return to step i (for the ATM-AAL1 fabric type) or step k (for the ATM-AAL2 fabric type) and enter new information in the screen, or go to step 12.

**11** In the InstallShield Wizard Complete screen, which displays after a slight delay, select “Yes, I want to restart my computer now.” Click Finish.

***Note 1:*** The system re-boot (restart) is required in order for the installation program to complete registry updates.

***Note 2:*** If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

**a** After the system re-boots, log back into the system as “administrator” (user name), and enter either “superuser” as the password or the password supplied by your network administrator.

**b** Open a command line interface at the UAS:

- **i** select **Start -> Run**
- **ii** type **cmd** in the window that displays
- **iii** press Enter
- **iv** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications
- **v** press Enter

**c** Launch the Local Configuration Interface GUI by performing the following steps:

- **i** select **Start -> Run**
- **ii** type **cmd** in the window that displays
- **iii** press Enter
- **iv** type **lci** on the command line

  ***Note:*** The first letter in the lci command is an “l”, as in “local.”
- **v** press Enter

  *The main Local Configuration Interface GUI screen displays.*
- **vi** select the “nodes” folder in the Network Element Tree pane.

*The Bearer Type IP Local Configuration Interface GUI screen displays.*

**d** Verify and/or enter information for the following fields in the screen:

***Note 1:*** When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes can be applied and saved until all entry errors in the screen are corrected.

***Note 2:*** Ensure that the Gateway Control Protocol is set to H.248 and ensure that the UAS Call Control Port and

Primary Call Agent Port are set to the appropriate value (the UAS default is 2944).

- **Primary Call Agent Name**

  *This is the computer name associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent IP Address**

  *This is the IP address associated with the remote node that is hosting the Primary Call Agent application.*

- **Primary Call Agent Port**

  *This is the port of the Call Agent application (default is 2944).*

- **UAS Call Control Port**

  *This is the port associated with receiving the call control message stream (default is 2944).*

- **Gateway Control Protocol**

  *This is the control protocol for the UAS, either H.248 or MGCP.*

  ***Note:*** This field can be datafilled only for systems with bearer type IP and bearer type ATM-AAL2.

- **Rtp Base Port**

  *This is the number of base ports for the RTP stream, within the range 1024 through 63094*.

  ***Note:*** This must be an even number. In addition, commas must not be entered in the number.

- **Legacy Announcements**

  *This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.*

  ***Note:*** If Legacy Announcements is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Announcements field is

Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **IVR Support**

  *This field determines whether IVR support is enabled in this system.*

- **Primary Language**

  *This is the primary language associated with the node.*

  ***Note:*** A Primary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  *This is the secondary language associated with the node.*

  ***Note:*** A Secondary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Secondary Language field will also be Disabled.

- **Conferencing State:**

  *This field determines whether Conferencing is enabled in this node.*

  ***Note:*** If Conferencing State is Disabled, then the Conference Spanning field is also Disabled.

- **Conference Spanning**

  *This field determines whether Conference Spanning is supported by the node. Conference Spanning allows conferences with up to 64 participants.*

  ***Note:*** If “Conferencing State” is Disabled, then the Conference Spanning field is also Disabled.

- **Audio Synch on Restart**

  *For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled,*

*hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.*

- **Primary DBServer Host**

  *This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, accept the default settings.*

- **Primary DBServer IP**

  *This is the IP address of the APS that is hosting the database server used by this UAS node.*

- **Backup Storage IP**

  *This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.*

- **G729B**

  *This field indicates G.729B audio codec support.*

- **Default TOS**

  *This field determines the Type of Service bit usage for this UAS. 0-255.*

- **RFC2833 DTMF**

  *This field indicates how the UAS will determine whether RFC2833 is enabled for each RTP connection. RFC2833 defines a method for passing DTMF digits "out-of-band" in special RTP packets, in order to provide more reliable DTMF recognition than is possible with low-bandwidth codecs. The possible selections include:*

  — *AlwaysOff (RFC2833 support is always disabled, regardless of call control)*

  — *Negotiated (RFC2833 support is enabled per call control messaging, that is, SDP and/or LCO negotiation)*

- **RFC2833 DTMF Squelch**

  *Not applicable*

- **Tone set**

  *This is the default tone set provided for the country that you select from the pull-down menu associated with this field.*

- **NTP Server IP**

*This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.*

***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

- **Supported Codec**

  *These check boxes determine which codecs, G711, G723, G726, G729, and T.38 are supported. The following guidelines should be followed when you are selecting the codecs:*

  — *T.38 is selectable only when at least one CG6000 card with BCT capability is installed in the system.*

  — *In an all-BCT system, all voice codecs should be disabled.*

  — *In a non-BCT system, up to a maximum of four voice codecs can be selected; the T.38 codec cannot be selected.*

  — *In a mixed system (BCT + IVR, BCT + Conf, BCT + IVR + Conf), up to a maximum of four of the codecs can be selected; one of the four codecs selected must be a voice codec.*

  — *It is recommended that you select G.711 for systems supporting conferencing service, to avoid any possible deterioration of voice quality.*

**e** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step f |
| you do not want to save the information | step i |

**f** Click Apply.

**g** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

**h** Go to step 12.

**i** Click Cancel.

*The entries in the screen fields revert to the default values.*

**j** Either return to step d and enter new information in the screen or go to step 12.

**12** Determine whether SNMP management configuration parameters need to be changed.

| If | Do |
|---|---|
| SNMP management configuration parameters need to be changed | step 13 |
| SNMP management configuration parameters do not need to be changed | step 14 |

**13** Click the “Reconfigure SNMP” button, located at the bottom of the Local Configuration Interface GUI screen.

*The Local Configuration Interface GUI SNMP screen displays, showing default values delivered with the UAS07 system.*

**a** Enter information for the following fields in the screen:

- **v2c read/write community**

  This is the SNMPv2c community name for read/write access through the SNMP-based management station.

- **v2c read only community**

  This is the SNMPv2c community name for read-only access through the SNMP-based management station.

- **v3 read/write user**

  This is the SNMPv3 community name for read/write access through the SNMP-based management station.

- **v3 read only user**

  This is the SNMPv3 community name for read-only access through the SNMP-based management station.

- **trap version**

  This is the SNMP version of the SNMP traps sent by the UAS.

- **trap destination**

This is the destination IP address associated with the remote SNMP management station. This is the address to which SNMP traps are sent.

- **trap port**

  This is the UDP port associated with the remote SNMP management station.

**b** Determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step c |
| you do not want to save the information | step f |

**c** Click OK.

**d** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

**e** Go to step 14.

**f** Click Cancel.

*The entries in the screen fields revert to the default values.*

**g** Either return to step a and enter new information in the screen fields or go to step 14.

**14** Determine whether the bearer fabric of the UAS you are installing is ATM or IP.

| If | Do |
|---|---|
| the bearer fabric type is IP | step 16 |
| the bearer fabric type is ATM | step 15 |

**15** Close the Local Configuration Interface GUI screens by selecting **File -> Exit**

**a** Go to step 17.

**16** In the Topology pane of the Local Configuration Interface GUI screen, select the “Nodes” folder and then select the “Cards” folder, which is located in the Nodes folder.

*The Local Configuration Interface GUI cards screen displays.*

**a** Review the card list. The Card Type field will be set automatically to “CG6000C” if a card is present. The Card

Type field will be set to “none” and the information detail field labels will be colored grey, if no card is present. Note the current configuration.

| If | Do |
|---|---|
| If card information is not to be changed | step i |
| If card information is to be changed, | step b |

**b** Double click the “Cards” folder, located in the Topology pane and, from the list of cards that displays below the Cards folder, click the bullet associated with a card to be changed. Enter information in the following fields in the dedicated card details screen that displays:

- IP address associated with each CG6000C card
- default router associated with each CG6000C card
- network mask associated with each CG6000C card
- Bearer Channel Tandeming (BCT) support capability for each CG6000C card, either Enabled or Disabled.

**c** For each card, determine whether you want to save the information that you have entered.

| If | Do |
|---|---|
| you want to save the information | step d |
| you do not want to save the information | step g |

**d** Click Apply.

**e** Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI card detail screen) and select “Save”. Click OK when the confirmation screen displays.

**f** Go to step h.

**g** Click Cancel.

**h** Either return to step a and enter information for another card, or go to step i.

**i** Close the Local Configuration Interface GUI screens by selecting **File -> Exit**

**17** If you are installing a PRI gateway, and if you are performing an upgrade, you should already have a valid “ugw.conf” file; go to

step 18. If you are installing a PRI gateway, and if you are performing a ground-up installation, ftp a new ugw.conf file to c:\uas\etc. Contact UAS Product Design if you need a new ugw.conf file, then go to step 18.

**18** This optional step validates configuration files and updates other configuration files. Any problems encountered will cause error messages to display in the command window. Note that this same action is performed upon the next application start-up.

**a** select **Start -> Run**

**b** type **cmd** in the window that displays

**c** press Enter

**d** Enter the following command in the window that displays:

```
configmgr -update -v
```

**e** press Enter

**19** This optional step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server. For additional information about this capability, see UAS system configuration backup/restore strategy on page 333. The following steps are performed on a remote Unix system.

**a** In a Unix shell, as Root user, 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
```

**b** Configure NFS to share the “/opt/uas” file system 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
```

**c** 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
```

**20** Start the application by performing the following steps:

**a** select **Start -> Run**

**b** enter **net start pmgrdaemon** in the window that displays

**c** press Enter

**21** Inspect the UAS installation log file (UASinstLog.txt) for indications of any errors that may have occurred during the application software installation. The file is located in the c:\winnt\temp directory. If you find errors, contact your next level of support or your Nortel Networks service representative for assistance.

**22** Refer to any existing UAS07 patch documentation and reapply any patches that had been previously applied to the UAS07 software now.

**23** You have completed this procedure.

# Upgrading the USP

**ATTENTION**

This document details the upgrade procedure for a major upgrade only. To perform a point release upgrade, see the USP Readme file.

USP releases are designated by three numbers separated by a period, for example USP8.0.10. The first and second numbers, 8 and 0, specify the major release. The third number, 10, specifies a point release. USP 8.0 to USP 10.0.0 is a major upgrade and USP9.0.2 to 9.0.3 is a point upgrade.

The following are examples of major releases: USP8.0.0, USP8.1.0, and USP9.0.0. The following are examples of point releases which correspond to the major release: USP8.0.10, USP8.1.3, and USP9.0.3.

Contact your Nortel Networks representative for more information.

**ATTENTION**

The CLI is not available for use during an upgrade.

**ATTENTION**

The USP10.0 software upgrade supports direct in-service software upgrade from USP9.0/SN07 to USP10.0/SN08 and USP8.0/SN06 to USP10.0/SN08.

**ATTENTION**

The USP must be at the latest point release of USP8.0 or USP9.0, for example 8.0.10, before upgrading to the current load. This ensures that all fixes related to upgrade are in place and tested. USP10.0 does not support a direct upgrade from USP8.1.x. Customers with USP8.1.x must upgrade to USP9.0.x and then upgrade to USP10.0. See the USP9.0 customer documentation for the specific procedures used to upgrade to USP9.0.

**ATTENTION**

Auto-negotiate capability is supported for the CS LAN and can be enabled during the upgrade.

**ATTENTION**

The RouteMaster application is outside the scope of upgrades. Contact Nortel Networks for more information on using the RouteMaster application for end office consolidation.

**ATTENTION**

An in-service cutover procedure is not performed during an upgrade. Contact Nortel Networks for more information.

**ATTENTION**

The procedures for cutover from Core Bounce to Direct Messaging are not performed during an upgrade. Contact Nortel Networks for more information.

**ATTENTION**

Perform all software upgrade procedures from your alternate boot server, unless otherwise noted. You must have administrative privileges to perform a software upgrade.

## Supported upgrade paths

Nortel Networks supports the following upgrade paths:

- USP8.0/SN06 to USP10.0/SN08
- USP9.0/SN07 to USP10.0/SN08

## Estimated upgrade times

The following table provide upgrade time estimates for the various cards in the system.

| Card type | Upgrade time (minutes) | Soak time (minutes) | Total (minutes) |
|---|---|---|---|
| RTC15 | 10 | 30 | 40 |
| RTC12 | 10 | 15 | 25 |
| First CC | 5 | 5 | 10 |
| CC | 5 | 5 | 10 |
| First Link | 5 | 20 | 25 |
| Link | 5 | 5 | 10 |
| NPC/NPS with no chain | 6 | 5 | 11 |
| NPC/NPS with one NPE | 12 | 5 | 17 |
| NPC/NPS with two NPE | 18 | 5 | 23 |
| NPC/NPS with three NPE | 24 | 5 | 29 |

### Example: Control shelf

A Control shelf with 12 link cards of the same type would take 2 hours and 40 minutes. If there were two types for links cards the time would increase to 3 hours.

***Note:*** Nortel Networks also requires you to perform test calls for the first time you have upgraded all the link cards that provide the links for a linkset. This would also increase the time to upgrade the Control Shelf.

**Example: Extension shelf**

An extension shelf with 16 link cards of two different types would take 2 hours and 10 minutes.

## Large versus small system upgrade considerations

Larger systems will require more than one maintenance window for upgrade. A maintenance window is six hours. The breakdown is as follows:

| System Size | Time required (hours) | Maintenance windows required |
|---|---|---|
| one shelf | 3 | one |
| two shelves | 5 | one |
| three shelves | 8 | two |
| four shelves | 10 | two |
| five shelves | 12 | two |
| eight shelves | 20 | four |

Small system are defined as one or two shelf system, larger systems are defined as three or more shelves. Upgrades are performed during a maintenance window where system activity should be at it lowest level.

## Card upgrade order for a one maintenance window upgrade

The card upgrade order for a one maintenance window upgrade varies slightly for one- and two-shelf systems.

For a one-shelf system, you upgrade the following cards:

- upgrade RTC 15
- upgrade CC1 in slot 1
- upgrade the link cards
- upgrade the NP cards
- upgrade CC2 in slot 18
- upgrade RTC 12
- activate new features

For a two-shelf system, you upgrade the following cards:

- upgrade RTC 15
- upgrade CC1 in slot 1 on the control shelf
- upgrade CC1 in slot 1 on the extension shelf
- upgrade the link cards on the extension shelf
- upgrade the link cards on the control shelf
- upgrade the NP cards in the control shelf
- upgrade the NP cards in the extension shelf
- upgrade CC2 in slot 18 on the extension shelf
- upgrade CC2 in slot 18 on the control shelf
- upgrade RTC 12
- activate new features

For a list and detailed procedures of the card upgrade order for a one-and two-shelf system, see Using the Upgrade Wizard on page 1033.

## Card upgrade order for a multiple maintenance window upgrade

When performing a large system upgrade that requires more than one maintenance window to complete, you must upgrade the entire Control CAM shelf and one card for each unique card type before the end of the first maintenance window. The subsequent windows are used to upgrade the remaining cards in the system.

For upgrades spanning multiple maintenance windows, you upgrade the following cards:

- upgrade RTC 15
- upgrade CC1 in slot 1 on the control shelf
- upgrade link cards in the control shelf
- upgrade NP cards in the control shelf
- upgrade CC2 in slot 18 on the control shelf
- upgrade one link card for each unique card type on any extension shelf
- SWACT RTC 12; if you cannot SWACT RTC 12, you need to upgrade a card of a type that you have not yet upgraded
- perform test calls and monitor the system for at least 15 minutes to evaluate your acceptance of the upgrade

- upgrade RTC 12

  ***Note:*** The RTC12 upgrade completes the upgrade requirement for the first maintenance window. You can continue the upgrade in this current maintenance window and in the next maintenance window.

- upgrade CC1 in slot 1 on the extension shelf
- upgrade the link cards on the extension shelves
- upgrade the NP cards in the extension shelves
- upgrade CC2 in slot 18

For a list and detailed procedures of the card upgrade order for a multiple shelf systems, see Using the Upgrade Wizard on page 1033.

## NP chain upgrade considerations

There are four possible NP card configurations to consider when planning to perform an upgrade over multiple maintenance windows:

1. All NP cards on the Control Shelf

   If:

   - both NPCs on the control shelf
   - all the chain related NPx cards on the control shelf

   All NP cards will be upgraded during the first window as all cards must be upgraded in the Control shelf during the first window.

2. Only the NPC on the Control Shelf, other NP cards on Extension shelves

   If:

   - both NPCs are on the control shelf
   - at least one chain associated NPx on an extension shelf

   You must finish upgrading both NPC associated chains and all NPx cards on the first maintenance window.

3. NPCs on an Extension shelf, other NP cards on the Control shelf

   If:

   - both NPCs are on an extension shelf,
   - at least one chain related NPx provisioned on the control shelf

You must finish upgrading all NPx cards associated to that chain in the first maintenance window.

***Note:*** Nortel Networks suggests locating both NPCs on the control shelf to avoid extension shelf isolation.

4. All NP cards on Extension shelves

   If:

   - both NPCs are on one extension shelf
   - all the chain associated NPx also provisioned on extension shelves

   You can choose to finish upgrading one NPC associated chain and one NPS associated chain (If an alternate NPS is already involved with the selected NPC associated chain, the NPS associated chain does NOT have to be upgraded in the first maintenance window).

   ***Note:*** Nortel Networks suggests locating both NPCs on the control shelf to avoid extension shelf isolation.

## Analyzing upgrade impacts

Avoid making changes to your system configuration and performing provisioning and maintenance activities during the software upgrade procedure. The system prohibits these activities.

The software upgrade procedure impacts system capacity, system performance, and the OAMP workstations.

Before beginning the upgrade, consider the following system limitations.

### System limitations during upgrade

During a software upgrade, the system prohibits the following actions, listed by subsystem:

- System administration
  - — adding, deleting, or modifying users
  - — setting the time of day
  - — changing passwords
- System management
  - — modifying the system name or shelf names
  - — adding or deleting RTC, CC, or application system nodes
  - — modifying the IP address or the PEC of the RTC system nodes

- SS7 management (MTP Level 3)
  - adding, deleting, or modifying a system identity
  - adding, deleting, or modifying a capability code
  - adding, deleting, or modifying links, linksets, linkset groups, combined linksets, or routesets
  - adding, deleting, or modifying ASP, AS, ASP Paths, AS destinations, or AS assignments
- SS7 management (MSU/Gateway Screening)
  - deleting gateway screening criteria files
- SS7 management (Global Title Translations)
  - adding, deleting, or modifying all GTT results
  - adding, deleting, or modifying all GTA results
  - adding, modifying, or deleting GTT translation type text
  - adding, modifying, or deleting GTT translations
- SS7 management (Special Study Operational Measurements)
  - adding, deleting, or modifying SSOMs
  - enabling/disabling SSOMs on linksets
- SS7 management (SCCP)
  - adding or deleting remote point codes (RPCs)
  - adding, deleting, or modifying remote subsystems (RSSs)
  - adding or deleting concerned point codes
  - adding, deleting, or modifying local subsystems (LSSs)
  - adding or deleting
    local subsystems concerned point codes (CPCs)
  - adding or deleting LSS instances
- IPS7 management
  - adding, deleting, or modifying application server process
  - adding, deleting, or modifying application server process path
  - adding, deleting, or modifying application server
  - adding, deleting, or modifying application server destination
  - adding, deleting, or modifying application server assignment

### System performance

The software upgrade procedure can impact USP system performance in the following ways:

- An upgrade database conversion is necessary due to internal USP data format changes. This affects the RTC system node in slot 15 (the inactive RTC system node). The RTC in slot 15 is the first system node upgraded to the new version.
- Depending on the scope of data format changes, the inactive RTC in slot 15 takes approximately 20 minutes to load and convert internal data to the new format. During this time, the inactive RTC system node is not enabled and the system operates with a single RTC system node.
- You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade. This is because the Link system nodes must be reloaded during the upgrade. As a result, all SS7 traffic is rerouted from the links and linksets that reside on the disabled Link system node.

### System capacity

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAMP workstation and the RTC system nodes are required for converting existing databases.

The pre-checking procedure checks for adequate disk space on the RTC system nodes. A message box informs you if your disk space is too low. If disk space is too low, delete any old snapshots.

Once the update is complete, the additional disk space is no longer required and is made available for use.

### OAMP workstation functionality

The GUI allows multiple sites to be configured on an OAMP workstation at one time. Since the sites are not upgraded at the same time, the following conditions apply:

- If the GUI is upgraded and the USP is not, you can access existing USP capabilities. You cannot use the new capabilities.
- The new USP GUI allows you to log in to a previous system (USP8.0 release and later only), a new system, or a USP system that has an upgrade in progress (USP8.0 release and later only).

- You cannot use a previous version of the GUI to log into a newer version of the USP software.
- Only one version of the GUI can be installed at a time, because the GUI upgrade requires the conversion of local files.

# Upgrading the Universal Signaling Point GUI

**ATTENTION**

Prior to installing the Alternate Boot Server Package please ensure that all unnecessary snapshots and old release loads (i.e. maintenance releases that are no longer in use) are deleted. This will ensure adequate disk space is available during the install procedure.



**CAUTION**

The GUI may not function properly with non-ASCII based character sets. Please ensure the OAMP workstation is set to either English or German language character sets.

This section covers software installation procedures and GUI installation procedures. The following topics are covered in this section:


- Uninstalling the previous version of the USP GUI from Windows-based workstations
- Installing the new USP GUI on a Windows-based workstation
- Upgrading the ABS software on a CS2000 Management Tools (CMT) Server
- Uninstall the USP Java GUI from the CMT


## Uninstalling the previous version of the USP GUI from Windows-based workstations

Perform the following steps to remove the previous version of the USP GUI from your Windows-based workstation(s):

***At the OAMP workstation***

1. Close all open applications and exit the USP Distinct Servers and Signaling Server Monitor.
2. Click the Windows **Start** button on your desktop taskbar.
3. On the Settings menu, select **Control Panel**.
4. In the Control Panel window, double-click **Add/Remove Programs**.

5 In the Install/Uninstall tab window of the Add/Remove Programs Properties window, select Universal Signaling Point from the alphabetical list of programs.

6 Click the **Add/Remove** button. A popup window asks if you are sure you want to completely remove the previous version and all of its components.

7 Click **Yes**. If a popup window asks if you want to remove shared files, click **Yes to All**. Click **Yes** to confirm your choice. All of the files are removed.

8 Restart your computer and proceed to the next section.

## Installing the new USP GUI on a Windows-based workstation

**ATTENTION**
Installing this USP software on a workstation other than your Nortel Networks-approved workstation may overwrite some system files used by other applications. This may cause failure of existing applications. Also, installing software other than Nortel Networks-approved applications on your USP OAMP workstation may cause failure of the USP application.

For information on OAMP workstation requirements for Windows and UNIX, see the USP Product Specification.

**ATTENTION**
Prior to installing the Alternate Boot Server Package please ensure that all unnecessary snapshots and old release loads (i.e. maintenance releases that are no longer in use) are deleted. This will ensure adequate disk space is available during the install procedure.

**ATTENTION**
If you are upgrading your system, uninstall the previous USP GUI version according to the previous section before proceeding with this section.

**ATTENTION**
When adding the USP GUI on an NTST30DA workstation (equipped with Reach Through) the GUI should be installed via the Add/Remove Programs utility in the Windows Control Panel.

To install the USP GUI, perform the following steps:

***Note:*** The following procedure requires approximately 15 minutes.

***At the OAMP workstation***

1. Obtain your record of site names and their RTC IP addresses from the pre-Upgrade check.
2. Close any open applications.
3. Insert the USP Software CD-ROM disk into the CD-ROM drive.

4 Double-click the **My Computer** icon on your desktop.

5 Double-click the CD-ROM disk icon.

6 Double-click **Install.exe**. A popup dialog box appears with the warning that installing this software on a workstation other than a Nortel Networks-approved workstation may overwrite some system files used by other applications. If this is a Nortel Networks-approved workstation, or you want to proceed regardless of the warning, click **Yes** to continue.

7 At the Welcome window for the USP setup program, click **Next.**

8 Select the package(s) that you want to install on this workstation.

- Select USP Software Loads and ABS manager if you want this workstation to act as the alternate boot server. If you are using a CMT-based alternate boot server, do not select this option. See the procedure Upgrading the ABS software on a CS2000 Management Tools (CMT) Server.
- Select USP Graphical User Interface Client if you want this workstation to be able to log into the USP site.
- Select USP User Manuals and Documentation Suite to install the complete collection of FCAPS documents, Centillion Manuals, and Interface Specifications.
- Select USP GR-310 Mediation Application to install a SEAS OSS Interface.
- Select Acrobat Reader if you do not have a version of Adobe Acrobat Reader installed on this workstation.

| If | Do |
|---|---|
| you select the alternate boot server (ABS) package | complete this procedure and the procedure in section Installing the Alternate Boot Server on a Windows-based workstation on page 1027 |
| you select the GUI package | step 9 |
| Acrobat Reader | step 12 - step 16 |
| select USP GR-310 Mediation Application | enter your Nortel-provided serial number when prompted by the system. |

***Note:*** Each USP system needs one workstation configured as an alternate boot server. Do not configure more than one alternate boot server for each USP system.

9 Select **Next**.

10 Select an Installation Directory and click **Install**.

11 If you selected the ABS pkg the following pop-up will appear: “Prior to installing the Alternate Boot Server Package please ensure that all unnecessary snapshots and old release loads (i.e. maintenance releases that are no longer in use) are deleted. This will ensure adequate disk space is available during the install procedure.” Select **OK** and then select an installation directory.The Copying Program Files window appears with a status bar to show progress in copied files.

12 If you chose to install Acrobat reader, a Welcome window for the Adobe Acrobat Reader Setup Program appears. Adobe Acrobat Reader is required to view the Solution information. If Adobe Acrobat Reader is already installed on this workstation, click **No**. Click **Yes** to the “Are you sure” message. If you do not want to install Adobe Acrobat Reader, skip to step 17.

13 Click **Next**. The Acrobat Reader License Agreement appears.

14 Click **Yes** to accept the terms of the agreement. The Acrobat Reader Destination Location window appears.

15 Click **Next**.

***Note:*** Do not modify the destination path for Acrobat Reader.

16 The Acrobat Reader Setup Complete window appears. Click **OK**.

17 Click the radio button next to **Yes, I want to restart my computer now**.

18 Click **Done**. The computer restarts.

19 Remove the USP Software CD-ROM disk from the drive using the eject cdrom command. The installation is complete. Keep the USP Software CD-ROM disk handy to your system hardware.

20 Log in to the USP from the new release of the USP GUI and monitor the OAMP workstation for 10 minutes while logged in to the USP. Check logs during this time. Your USP GUI is now upgraded. You will use the GUI to upgrade your USP software.

***Note:*** when you first connect the GUI it will detect that the lab is running USP9.0 and will logout and log back in

automatically to re-initialize based on the USP9.0 feature set. (it is expecting an 9.0 release by default).

### Installing the Alternate Boot Server on a Windows-based workstation

If this workstation is not your alternate boot server, skip this section and proceed to the next section. If this workstation is the alternate boot server (if you selected Alternate Boot Server in step 8), the Signaling Server Monitor, Alternate Boot Server Configuration Manager, and the three Distinct servers start up automatically when the workstation restarts. You will need to modify the BOOTP file. To do this, perform the following steps:

***At the OAMP workstation***

**1**



**CAUTION**

Make a record of the password immediately.

If this is the initial install of the ABS, a popup window prompts you to create a password for the Alternate Boot Server Configuration Manager.

**2** Click the **Distinct BOOTP Server** button on the taskbar to maximize the Distinct BOOTP Server window.

**3** Click the **Configure** menu and select **Administrator** and then **Login** to display the Distinct BOOTP Login window.

**4** Enter your administrator password in the **Enter the administrator password** field and click **OK** to log into the server.

The Distinct BOOTP Login window closes.

**5** Click the **Configure** menu and select **Server** to display the Configure BOOTP window.

**6** In the **Addresses** tab window, view the contents of the field at the bottom of the window, next to the Add, Modify, and Remove buttons. This field should contain the hexadecimal Ethernet hardware addresses of the RTC system nodes in your system.

**7** Select the Ethernet hardware address that matches the Ethernet hardware address for the RTC system node in slot 12 of your system. The information for that Ethernet hardware address should appear in the various fields.

8 In the Boot File field, change the value to /c/ntssgusp/abs/sites/<site_name>/rtc1/rtcboot (site_name is the name of your system as it appears in the site configuration information).

9 Click **Modify** to save the changes.

10 Select the Ethernet hardware address that matches the Ethernet hardware address for the RTC system node in slot 15 of your system. The information for that Ethernet hardware address should appear in the various fields.

11 In the Boot File field, change the value to /c/ntssgusp/abs/sites/<site_name>/rtc2/rtcboot (site_name is the name of your system as it appears in the site configuration information).

12 Click **Modify**, then **Apply** to save the changes.

13 Open the Alternate Boot Server Configuration Manager.

14 Login to the Alternate Boot Server Configuration Manager.

15 Under the File dropdown menu, select **ABS Configuration**.

16 Select a site from the Site list.

17 Confirm that the Alternate Boot Loads displayed for each RTC are for the pre-upgrade load.

18 Confirm that the Alternate Boot Snapshot display is the snapshot taken earlier in this procedure. A pre-upgrade snapshot

19 Click **Apply** to save the changes.

20 Logout of the Alternate Boot Server Configuration Manager.

## Upgrading the ABS software on a CS2000 Management Tools (CMT) Server

Use this procedure to install alternate boot server (ABS) software on a Succession Solutions CMT.

***Note:*** When you install the USP ABS on the CMT server, you must export the X-Windows display of the CMT server to a remote workstation. If you are using a Windows-based workstation, use X-Windows server software such as Hummingbird's Exceed.

If you do not have access to the CMT Server CD-ROM, perform the following steps on a remote workstation. The workstation must be equipped with a CD-ROM drive and an FTP client application that supports the recursive transfer of directory structures to the CMT, such as Hummingbird's FTP client or WS-FTP. In this case, begin the following procedure at step 2.

***At the workstation***

1 If you have direct access to the CMT, do the following:

**a** Place the USP CD in the CD-ROM drive of the CMT.

**b** Establish a telnet connection with the CMT.

**c** Login to the CMT as *root.*

**d** Enter **cd /cdrom/cdrom0**.

**e** Enter **ls** and ensure that you see the file `install.bin` listed.

**f** Proceed to step 3.

2 If you are accessing the CMT CD-ROM from a remote workstation, do the following:

**a** Establish a telnet connection with the CMT.

**b** Login to the CMT as *FIELD.*

**c** Enter **cd /data/usp**.

**d** Enter **ls -l absCD**. If the directory does not exist, proceed to step e. If the directory does exist, enter **rm -rf absCD** to remove any folders left over from the previous installations.

**e** Enter **mkdir absCD**.

**f** Set the directory permissions by entering **chmod -R 755 absCD**. To validate the change, enter **ls -l**. The system responds with d`rwxr-xr-x 2 FIELD maint2 *date* *time* absCD`.

**g** Place the USP CD in the CD-ROM drive of the workstation and establish an FTP connection with the CMT using the FIELD account.

**h** Transfer the contents of the CD to the /data/usp/absCD directory. Ensure that all files are transferred in binary non-passive mode and that the case of all file and directory names is preserved.

**i** Enter cd **/data/usp/absCD**.

**j** Enter **ls** and ensure that you see the file `install.bin` listed.

**k** Set the file permissions by entering **chmod 755 install.bin**. To validate the change, enter **ls -l** . The system responds with `rwxr-xr-x 2 FIELD maint2 *date* *time* install.bin`.

3 Install the new version of the ABS software on the CMT:

**a** Ensure that your X-Windows server software is running and that host access permissions are allowed for the CMT. Refer to your X-Windows server software manual for details.

**b** Login to the CMT as *root.*

**c** Enter **DISPLAY=<IP address of your PC>:0.0**. To find the IP address of the PC you are using, you may need to enter **ipconfig** from a DOS window.

**d** Enter **export DISPLAY**. To confirm the export, enter **echo $DISPLAY**.

**e** If this is the first time an ABS has been installed on this CMT, proceed to step j.

**f** Enter **cd /data/usp/ntssgusp/abs**.

**g** Note the settings on your ABS Configuration Manager by doing the following:

**i** Enter **./ABS &** to launch the ABS application. It may take 2 to 3 minutes for the application to launch and be fully populated with data.

**ii** Enter **File>Login**.

**iii** Enter the Administrator Password and click **Login**.

**iv** Click **File>ABS Configuration**.

**v** Record all of the ABS Configuration Manager settings. You can use this information to ensure that the settings have not changed once the installation is complete.

**vi** Exit the ABS Configuration Manager by clicking **File>Exit**.

**vii** Enter **./Uninstall_ABS &**. It may take 2 to 3 minutes for the application to launch and be fully populated with data.

**viii** When the uninstall wizard opens, click **Uninstall** and click **Done**.

**h** Ensure that no instances of the ABS Configuration Manager are running. Enter **ps -ef | grep ABS**. The system responds with

```
FIELD 2155 1972 0 10:35:38 pts/1 0:00 grep ABS
FIELD 2119 1972 1 10:35:31 pts/1 0:00 /bin/sh
./ABS
```

Any instance of `/bin/sh ./ABS` indicates that the ABS application is running. Request the users of those ABS sessions to exit the application.

i Delete the old Java Runtime Environment (JRE) directory. Enter **rm -rf /data/usp/jre**.

j If you are accessing the CMT CD-ROM from a remote workstation, enter **cd /data/usp/absCD**. If you have direct access to the CMT, enter **cd /cdrom/cdrom0**.

k Enter **./install.bin**. The application may take 2 to 3 minutes to launch.

***Note:*** If the following error appears, the DISPLAY environment variable is not set up correctly and you must repeat steps c through e:

```
Invocation of this Java Application has
caused an InvocationTargetException. This
application will now exit. (LAX)

Stack Trace:

at java.lang.Class.forName0(Native Method)

at java.lang.Class.forName (Class.java:130)
```

If any other errors occur, ensure that your X-Windows server software is running and that host access permissions are allowed for the CMT. Refer to your X-Windows software manual for details.

If the errors persist, contact your Nortel Networks support representative.

l When the introduction panel displays, click **Next**.

m On the Package Selection panel, select the **USP Software Loads and ABS Manager** package. If you will be using the CMT webstart application, also select the **USP Graphical Interface Client** package. Do not select other packages. Click **Next**.

n A disk space warning may display. Click **OK**.

o On the Installation Directory panel, click **Install**.

p On the Install Complete panel, click **Done**.

4 Configure the new version of the ABS software on the CMT:

a Enter **cd /data/usp/ntssgusp/abs**.

b Ensure that your X-Windows software is running and that host access permissions are allowed for the CMT.

c Ensure that the DISPLAY environment variable is set up correctly. Repeat steps 3c through 3e if it is not correct.

d Enter **./ABS &** to launch the updated application. It may take 2 to 3 minutes for the application to launch and be fully populated with data.

e Click **File>Login**.

f Click **File>ABS Configuration**.

g Confirm that the settings in the ABS Configuration Manager for each USP are unchanged.

5 If you are installing the software on the CMT from a remote workstation, enter **rm -rf absCD** to delete the temporary files.

6 Remove the USP Software CD-ROM disk from the drive using the eject cdrom command. The installation is complete.

## Uninstall the USP Java GUI from the CMT

Use this procedure to uninstall the USP Java GUI and remove the Launch Point Link from the CMT.

***Note:*** When the USP ABS is on a CMT server, you must export the X-Windows display of the CMT server to a remote workstation. If you are using a Windows-based workstation, use X-Windows server software such as Hummingbird's Exceed.

***At the OAMP workstation***

1 From your workstation, telnet to the CMT.

2 Enter **DISPLAY=<IP address of your PC>:0.0**. To find the IP address of the PC you are using, you may need to enter **ipconfig** from a DOS window.

3 Enter **export DISPLAY**. To confirm the export, enter **echo $DISPLAY**.

4 Enter **cd /data/usp/ntssgusp/**

5 To launch the uninstaller, enter **./Uninstall_Universal_Signaling_Point &**

6 Click **Next.**

7 Select **Uninstall Specific Features**.

8 Click **Next**.

9 Deselect the check boxes next to **USP Graphical Interface Client** and **USP User Manuals and Documentation Suite.**

10 Click **Uninstall**.

11 Click **Done**.

# Using the Upgrade Wizard

When you have upgraded the GUI, perform the following procedures to prepare the system for the software upgrade.

**ATTENTION**
Do not use the software upgrade wizard to upgrade NPC/NPS/NPE system nodes if there are NPE chains provisioned. Manually upgrade these nodes instead. See "Manually Upgrading System Nodes" in Upgrading the USP, NN10045-461.

## Setup

The system performs the following actions to prepare the USP for an upgrade:

- Copies upgrade package to the RTCs from Alternate Boot Server
- Copies software loads to RTCs from Alternate Boot Server
- Sets the target upgrade software version

***Note:*** Setup can take up to an hour to complete.

### Running the setup

***At the OAMP workstation***

1. Login to the USP GUI.
2. Click **Administration>software-upgrade**. Select the software release you are installing in the Target Version text box. Use the notation *vn.n.n* (for example v9.0.0)
3. Click the **Run Setup** button. The system asks for confirmation.
4. Click **Yes**.
5. Click **Next**.

## Precheck

Run the precheck to ensure that the upgrade is ready to proceed. The system confims:

- That no USP9.0 GUI users are still logged into the system- they must log out before the upgrade can proceed.
- Both RTCs are in-service with an operational state of enabled
- RTC in slot 12 of control shelf is the current active RTC.

- The Alternate boot server is configured properly for current system configuration for both RTCs.
- All other system nodes are in-service with an operational state of enabled or have an availability state of offline.
- Software upgrade packages have been transferred to both RTCs.

If any of the checks fail, resolve them before proceeding with the upgrade.

**Running the precheck**

***At the OAMP workstation***

1 Click the **Run Precheck** button. The system asks for confirmation.

2 Click **Next**.

***Note:*** If the status panel indicates that prechecking is successful, proceed to the next section. If prechecking was not successful, take steps to address any error messages and repeat the precheck before proceeding. For example, if the prechecking status panel indicates that disk space is low, delete any unused snapshots and loads from the RTC SCSI disk.

## Limit user access

Before beginning a software upgrade, you should limit connections to the USP to prevent other users from accidentally modifying provisioning data while the upgrade is in progress. To view and/or restrict user access to the USP during a software upgrade, perform the following steps:

**Viewing and restricting user access to the USP**

***At the OAMP workstation***

1 Click **Security>user-session>realtime**.

The Current User Access field displays the users who are currently allowed access to this USP. Any VB GUI users must be locked out before the upgrade can continue.

2 Double-click the session you want to lock out.

3 Click **force-out**.

## Create a pre-upgrade data snapshot

After you have copied the upgrade files, create a new data snapshot, copy the data snapshot to the OAM&P workstation, and change the alternate boot data snapshot for your site.

### Changing the alternate boot data snapshot

***At the OAMP workstation***

1 Open the Backup Active RTC window. In the menu bar, click **Administration>backup**.

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

3 Click the corresponding checkboxes to activate the following options, as appropriate:

- transfer snapshot to alternate boot server

  ***Note:*** Nortel Networks recommends that you enable this option. If you don't select this option a warning dialog will appear. Click Yes to continue.

- set as active snapshot on alternate boot server

  ***Note:*** Nortel Networks recommends that you enable this option. If you don't select this option a warning dialog will appear. Click Yes to continue.

- delete oldest snapshot on alternate boot server if maximum reached (16)
- delete oldest snapshot on rtc if maximum reached (5)

4 Click **Create** to create the data snapshot. The Backup Status box indicates that 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.

5 Open the File manager window. In the menu bar, click **Administration>file-manager**.

***Note:*** The left side of the screen displays the files present on the Alternate Boot Server (ABS). The right side of the screen displays files present on the selected rtc. To view files on rtc-15, select rtc-15 from the drop-down list box on the top of the right screen.

6 Select the active RTC system node from the drop-down list box.

7 Open the snapshot folder.

8 Open the folder corresponding to the version of the USP software that you are running.

9 Select the snapshot file you want to copy. When you select a file, its description is displayed in the Description box.

10 Copy the snapshot to the ABS by clicking **<-**. The folders in ABS portion of the window are updated with the information for the copied data snapshot when the copy operation is complete.

11 Open the Alternate Boot Server Configuration Manager. In the menu bar, click **Administration>alternate-boot-server**.

12 Select the snapshot from the Alternate Boot Data Snapshot List.

13 Click **Modify**.

## Start the upgrade

Run the Start Upgrade procedure to begin the software upgrade. All pre-check conditions must be met before upgrade will be allowed to be started. All upgrade packages and target software loads must be transferred to both RTCs.

**Running the Start Upgrade procedure**

***At the OAMP workstation***

1 Click the **Start Upgrade** button.

2 Click **Next**.

## Abort the upgrade

To stop software upgrade all nodes must be running the original back-level release (no nodes must have an upgrade state of *upgraded*. If nodes are upgraded, they must be downgraded prior to issuing the stop command.

## Software load setup

The Software Load Setup builds a mapping between the current software loads and the target software loads and automatically re-maps the software load pointer to the new target software release.

The system creates a default mapping based on the current software version and the target upgrade version specified during setup. All current software loads must be mapped to the target software loads. If a software mapping does not exist for the current load, you must resolve the missing pairing.

The current load list contains all software loads available on the active RTC that match the current software release.

The upgrade load list contains all software loads available on the active RTC that match the target upgrade software release.

### Running the software load setup

***At the OAMP workstation***

1 Review the software mapping displayed in the software load setup. Confirm the mapping is correct.

2 Click the **Next** button.

## Upgrade the system nodes

Run the node upgrade to perform the actual software upgrade for a specific node.

When performing a large system upgrade that requires more than one maintenance window to complete, you must upgrade the entire Control CAM shelf before the end of the first maintenance window. Use the additional window to upgrade the cards in the extension shelves.

Upgrade the nodes in the following order:

1. Inactive RTC in slot 15, see Upgrading the inactive RTC in slot 15 on page 1038.
2. CC in slot 1 of control CAM shelf 1, see Upgrading the CC node on page 1039.
3. CCs in slot 1 of extension CAM shelves, see Upgrading the CC node on page 1039.
4. Link system nodes on control and extension CAM shelves, see Upgrading a link node on page 1040.
5. NPC, NPS and NPE nodes in control and extension CAM shelves, see Upgrading NPC, NPS, and NPE nodes on page 1042.
6. CCs in slot 18 of extension CAM shelves, see Upgrading the CC node on page 1039.
7. CC in slot 18 of control CAM shelf, see Upgrading the CC node on page 1039.
8. SWACT and upgrade inactive RTC in slot 12, see Performing a SWACT and upgrade for the inactive RTC node in slot 12 on page 1047.

For multi-shelf systems, see Large versus small system upgrade considerations on page 1015. The upgrade order varies slightly when performing a large system upgrade.

***Note:*** If your system includes NPC, NPS and/or NPE nodes, you must upgrade the NPC, NPS and NPE system nodes (on all shelves if you have a dual-shelf or multi-shelf system) in a specific order depending on the local subsystem assignment. Re-ordering of the upgrade sequence may be required if performing a multi-node. upgrade operation.

### Inactive RTC node in slot 15

An alternate boot data snapshot must be taken before you upgrade an RTC. Refer to Create a pre-upgrade data snapshot on page 1035.

Upgrade of the RTC in slot 15 could take up to 20 minutes to complete.

#### Upgrading the inactive RTC in slot 15

***At the OAMP workstation***

**1** Verify that RTC12 is the active RTC.

**a** In the menu bar, click **Configuration>platform>node**.

**b** Click the **Graphical view** tab.

**c** Click the RTC in slot 12.

| If: | Do: |
|---|---|
| the Activity State is active | Continue to step 2. |
| the Activity State is not active | Perform a SWACT, then continue to step 2. |

**2** Select the RTC node to upgrade from the list of available nodes in the software upgrade wizard.

**3** Click the **Upgrade node** button. The system asks for confirmation.

**4** Wait for node upgrade to complete (upgrade state will change to *upgraded* on completion).

***Note 1:*** The system raises a minor alarm, indicating a mismatch in boot images during the upgrade procedure.

***Note 2:*** In the event that automatic node upgrade fails to complete successfully, then the upgrade may need to be performed manually. See "Manually Upgrading System Nodes" in Upgrading the USP, NN10045-461.

***Note 3:*** The system raises a minor alarm, indicating an image mismatch between mate nodes.

5 Monitor the USP to ensure it performs normally and does not report any LOG_SWERRS or LOG_TRAPS. If it does, contact your next level of support.

6 Set the alternate boot load for RTC system nodes to the new system load:

a Click **Administration>alternate-boot-server**.

b Update the RTC 12 to the new release version by selecting the new release from the ABS Active Loads drop-down menu.

c Update the RTC 15 to the new release version by selecting the new release from the ABS Active Loads drop-down menu.

d Click **Modify**.

***Note:*** The system raises a minor alarm, indicating a mismatch in boot images.

7 Continue to the next procedure.

## CC node

To upgrade a CC node, perform the following steps:

***Note:*** Start with CC1 of the control shelf.

### Upgrading the CC node

***At the OAMP workstation***

1 Select the node to upgrade in the list of available nodes.

2 Click the **Upgrade** button.

3 Wait for the node upgrade to complete (upgrade state will change to *upgraded* on completion).

***Note 1:*** The system raises a minor alarm, indicating a mismatch in boot images during the upgrade procedure.

***Note 2:*** The system raises a minor alarm, indicating an image mismatch between mate nodes.

***Note 3:*** In the event that the automatic node upgrade fails to complete successfully, then the upgrade may need to be performed manually.

4 Monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not

continue with the node upgrade, contact your next level of support.

5 Continue to the next procedure.

### Link node

**ATTENTION**
To upgrade an NPC, NPS, or NPE node see NPC, NPS, and NPE nodes on page 1041.

To upgrade a single system node, perform the following steps:

#### Upgrading a link node

***At the OAMP workstation***

1 Select the node to upgrade in the list of available nodes.

2 Click the **Upgrade node** button. The system asks for confirmation.

3 Wait for node upgrade to complete (upgrade state will change to *upgraded* on completion).

4 Monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.

5 Repeat this procedure for all remaining link nodes.

### Multiple link nodes

**ATTENTION**
To upgrade an NPC, NPS, or NPE node, see NPC, NPS, and NPE nodes on page 1041.

To upgrade multiple system nodes, perform the following steps:

#### Upgrading multiple link nodes

***At the OAMP workstation***

1 **Shift-click** or **ctrl-click** to select a range of nodes to upgrade in the list of available nodes.

2 Select the delay interval between each successive node upgrade. This will be used to soak the upgraded node before moving to the next system node.

3 Click the **Upgrade node** button. The system asks for confirmation.

***Note:*** In the event that automatic node upgrade fails to complete successfully, then upgrade may need to be performed manually.

4 Wait for the node upgrade to complete (upgrade state will change to *upgraded* on completion).

***Note:*** In the event that automatic node upgrade fails to complete successfully, then the upgrade may need to be performed manually.

5 The upgrade will now delay for the selected interval before continuing to the next node to upgrade. Upgrade of nodes can be cancelled at any time by clicking the **Stop** button. To skip the delay count down, click **No delay** and the next node will be upgrade immediately.

6 Monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.

7 Repeat this procedure for all remaining link nodes.

### NPC, NPS, and NPE nodes

The upgrade of an NPC, NPS and/or NPE node requires special handling to ensure that the local subsystem instances associated with an NPC, NPS and an NPE chain have been deactivated. Also, the upgrading node must not be the active NPC node. If it is then a switch of activity must be performed prior to upgrading the node.

The upgrade procedure for NPC and NPS system nodes without NP chains are upgraded as follows:

- Upgrade the inactive NPC system node.
- Upgrade all NPS system nodes.
- SWACT to the newly upgraded NPC node.
- Upgrade the inactive NPC system node.

The upgrade procedure for NPC, NPS, and NPE system nodes with NP chains are upgraded as follows:

- Upgrade the inactive NPC system node, the NPE nodes in that chain and any associated NPS nodes.
- Upgrade all NPS chains, their associated NPS nodes and the NPE nodes in those chains.
- SWACT to the newly upgraded NPC node.
- Upgrade the final NPC system node, the NPE nodes in that chain and any associated NPS nodes.

### Upgrading NPC, NPS, and NPE nodes

#### *At the OAMP workstation*

1 In the menu bar, click **Administration>Platform>Node**.

2 Select the NPC you want to upgrade.

3 Check the activity state of the NPC.

| If: | Do: |
|---|---|
| The NPC is active. | Perform a SWACT, then continue to step 5. |
| The NPC is Inactive. | Continue to step 5. |

4 Click **Lock**.

5 Deactivate the NP local subsystem instance running on the inactive NPC system node. To do this, click **Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Deactivate**.

6 If an NPE chain has been provisioned with this NPC node as the master and with an alternate NPS system node, then deactivate the local subsystem instance running on the alternate NPS. To do this, click **Configuration>SCCP>shared-local-subsystem-instance**, select the NPx of interest and click **Deactivate**.

7 Using the software upgrade wizard, select the NPC node to upgrade in the list of available nodes.

8 Click the **Upgrade node** button. The system asks for confirmation.

**9** Wait for node upgrade to complete (the upgrade state will change to *upgraded* on completion).

***Note 1:*** The system raises a minor alarm, indicating a mismatch in boot images during the upgrade procedure.

***Note 2:*** The system raises a minor alarm, indicating an image mismatch between mate nodes.

***Note 3:*** In the event that the automatic node upgrade fails to complete successfully, then upgrade may need to be performed manually.

**10**

| If: | Do: |
|---|---|
| an NPE chain is provisioned with this NPC node as master | repeat steps 7 to 9 for each NPE system node and the alternate NPS system node associated with this chain. |
| there is no NPE chain associated with this NPC node | continue this procedure. |

**11** Wait for the local subsystem instance to be *deactivated/prohibited*.

**12** Re-activate the local subsystem instance running on the inactive NPC To do this, click **Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Activate**.

**13**

| If: | Do: |
|---|---|
| an NPE chain is provisioned with an alternate NPS system node | Wait for the local subsystem instance to be *deactivated/prohibited*. Re-activate the local subsystem instance running on the alternate NPS To do this, click **Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Activate**. |
| there is no NPE chain provisioned with an alternate NPS system node | continue this procedure. |

**14** Wait for the re-activated local subsystem instances to return to the *activated/allowed* state.

**15** Monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.

**16**

| If: | Do: |
|---|---|
| NPS system nodes are provisioned without a chain, or NPS system nodes which are masters of a chain | select an NPS system node to be upgraded. This node cannot be an NPS system node already upgraded in the previous steps or the NPS system node associated with the currently active NPC chain. |
| there are no further NPS system nodes to be upgraded | Proceed to step 29. |

**17** Deactivate the NP local subsystem instance running on the NPS system node. To do this, click **Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Deactivate**.

**18** If an NPE chain has been provisioned with an alternate NPS for the selected NPS, deactivate the NP LSS instance running on the alternate NPS system node. To do this, click **Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Deactivate**.

**19** Using the software upgrade wizard, select the NPS node to upgrade in the list of available nodes

**20** Click the **Upgrade node** button.

**21** Wait for node upgrade to complete (upgrade state will change to *upgraded* on completion).

***Note 1:*** The system raises a minor alarm, indicating a mismatch in boot images during the upgrade procedure.

***Note 2:*** In the event that the automatic node upgrade fails to complete successfully, then the upgrade may need to be performed manually.

**22**

| If: | Do: |
|---|---|
| an NPE chain has been provisioned for this NPS node | repeat steps 19 to 21 for each NPE system node and the alternate NPS system node associated with this chain. |
| there is no NPE chain associated with this NPS node | continue this procedure. |

**23** Wait for the local subsystem instance to be *deactivated/prohibited*.

**24** Re-activate the local subsystem instance running on the NPS. To do this, click **Configuration>SCCP>shared-local-subsystem-instance**, select the NPx of interest and click **Activate**.

**25** If an NPE chain has been provisioned with an alternate NPS system node:

**a** Wait for the local subsystem instance to be *active/allowed*.

**b** Re-activate the NP local subsystem instance running on the alternate NPS. To do this, click **Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Activate**.

**26** Wait for the re-activated local subsystem instances to return to the *activated/allowed* state.

**27** Monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.

**28** Repeat steps 16 to 27 for any remaining NPS system nodes in the system, otherwise proceed to step 29.

**29** Swact the active NPC node. To do this, click **Administration>platform>node** for the currently active NPC node, then click the **Swact** button.

**30** Deactivate the NP local subsystem instance running on the inactive NPC system node. To do this, click **Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Deactivate**.

**31** If an NPE chain has been provisioned with an alternate NPS system node, then deactivate the local subsystem instance running on the alternate NPS. To do this, click

**Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Deactivate**.

**32** Using the software upgrade wizard, select the newly inactive NPC node to upgrade in the list of available nodes.

**33** Click the **Upgrade node** button.

**34** Wait for the node upgrade to complete (upgrade state will change to *upgraded* on completion).

***Note 1:*** The system raises a minor alarm, indicating a mismatch in boot images during the upgrade procedure.

***Note 2:*** In the event that the automatic node upgrade fails to complete successfully, then the upgrade may need to be performed manually.

**35** If an NPE chain has been provisioned for this NPC, repeat steps 32 to 34 for each NPE system node and the alternate NPS system node associated with this chain.

**36** Wait for the local subsystem instance to be *deactivated/prohibited*, then, re-activate the local subsystem instance running on the inactive NPC. To do this, click **Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Activate**.

**37** If an NPE chain has been provisioned with an alternate NPS system node, wait for the local subsystem instance to be deactivated/prohibited, then re-activate the local subsystem instance running on the alternate NPS. To do this, click **Configuration>SCCP>local-subsystem**, select the NPx of interest and click **Activate**.

**38** Wait for the re-activated local subsystem instances to return to the *activated/allowed state*.

**39** Monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.

**40** Ensure that the activity state of the NPC is set to not-active. To do this click **Administration>shared>local-subsystem**. If the NPC's activity state is currently active then go to step 37, otherwise skip to step 38.

| If: | Do: |
|---|---|
| the NPC's activity state is currently active | continue to step 41. |

| If: | Do: |
|---|---|
| the NPC's activity state is currently inactive | continue to step 42. |

41 SWACT the currently active NPC node. To do this click **Administration>platform>node**.

42 Monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.

### Inactive RTC node in slot 12

An alternate boot data snapshot must be taken before you upgrade an RTC. Refer to Create a pre-upgrade data snapshot on page 1035.

Upgrade of the RTC in slot 12 could take up to 20 minutes to complete.

#### Performing a SWACT and upgrade for the inactive RTC node in slot 12

***At the OAMP workstation***

1 Verify that RTC15 is the active RTC.

**a** In the menu bar, click **Configuration>platform>node**.

**b** Click the **Graphical view** tab.

**c** Click the RTC in slot 15.

| If: | Do: |
|---|---|
| the Activity State is Active | continue to step 2. |
| the Activity State is not Active | perform a SWACT, then continue to step 2. |

2 Select the RTC node to upgrade from the list of available nodes in the software upgrade wizard.

3 Click the **Upgrade node** button.

4 Wait for the node upgrade to complete (upgrade state will change to *upgraded* on completion).

***Note 1:*** The system raises a minor alarm, indicating a mismatch in boot images during the upgrade procedure.

***Note 2:*** The system raises a minor alarm, indicating an image mismatch between mate nodes.

***Note 3:*** In the event that automatic node upgrade fails to complete successfully, then upgrade may need to be performed manually.

5 Wait 10 minutes and then perform a SWACT.

6 Monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.

## Activate features

You must activate the new features of the software load. All system nodes must be upgraded to activate features.

**ATTENTION**
When you activate new features, all GUI connections will logout and log back in automatically to re-initialize in order to pickup the new 9.0 features. Select Administration>software-upgrade to continue with the feature activation.

To activate new features, perform the following steps:

### Activating new features

***At the OAMP workstation***

1 Click **Activate Features**. A confirmation dialog box appears.

2 Click **Yes**.

3 Perform test calls to verify that messages are correctly routed. Monitor the USP to ensure it does not report any LOG_SWERRs or LOG_TRAPs.

4 Monitor the USP for 15 minutes. Ensure that the USP performs without degradation.

When you have completed the procedures in this document, complete the procedures in Cleanup on page 1049.

## Cleanup



**CAUTION**

After completing this procedure, you will not be able to abort the upgrade process, except by performing an alternate boot to the data snapshot taken before you started the upgrade procedure.

Cleanup performs the final procedures for completing a software upgrade. All other upgrade steps must be completed prior to performing the upgrade cleanup steps.

### Running the cleanup

***At the OAMP workstation.***

1. Verify all nodes have been upgraded
2. Ensure new features are activated
3. Click **Run Cleanup**.The system asks for confirmation.
4. Click **Yes**.
5. Click **Next**.

## Complete the upgrade

Finish the cleanup to shut down the wizard, create a data snapshot, and restore access privileges.

### Completing the cleanup

***At the OAMP workstation***

1. Ensure all cleanup procedures have been performed
2. Click **Stop Upgrade**. The system asks for confirmation.
3. Click **Finish** on the wizard action and navigation panel.
4. Create a data snapshot, copy it to the Alternate Boot Server and set the alternate boot server snapshot.
5. Set user privileges back to pre-upgrade settings and re-enable any user accounts that were disabled during the upgrade.

# Configure Passport port to auto-negotiate

**ATTENTION**

Perform this procedure if you have a Passport 8600 in your Succession Solution, and you want to enable Autonegotiation.

If you are not using Autonegotiation skip this procedure and continue to Post-upgrade checklist on page 1051

To enable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Passport router switch.

## Configuring the Passport port

### *At the CLI for the Passport*

**1** Determine the slot and port on the Passport that connects to the device:

```
> show ip arp info <ip_address>
```

**ip_address**
is the physical IP address of the IPS7 GW card.

The slot and port are reported.

```
prompt:cpu> show ip arp info 172.30.242.25
================================================================================
                                      Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL
--------------------------------------------------------------------------------
172.30.242.25    00:90:69:1a:d4:fc   200   1/2   DYNAMIC 272
```

***Note:*** If the response indicates MLT instead of the slot and port, perform this operation from the mate Passport unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.

**2** Set the slot and port to auto-negotiate:

```
> config ethernet <slot>/<port> auto-negotiate
enable
```

The slot and port are reconfigured to auto-negotiate and the prompt returns.

```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

3 Verify the port configuration:

**> show ports info config <slot>/<port>**

The slot and port configuration is displayed.

```
prompt:cpu> show ports config info 1/2

================================================================================
                                      Port Config
================================================================================

PORT              AUTO  SFFD  ADMIN       OPERATE     DIFF-SERV  QOS MLT
NUM   TYPE        NEG.        DUPLX SPD   DUPLX SPD   EN   TYPE  LVL ID
--------------------------------------------------------------------------------
1/2   100BaseTX   true  false  half  100   full  100   fals  core  1   0
```

4 Commit the change:

**> save config**

## Post-upgrade checklist

This checklist provides system cleanup on your upgraded USP. You should perform this checklist on your alternate boot server. To complete the post-upgrade checklist, perform the following steps:

***Note:*** Wait 24 hours after completing all of the upgrade procedures.

### Performing the post-upgrade checklist

#### *At the OAMP workstation*

1 Begin a new log time period to end the upgrade log tracking time period. To do this, click **Fault>Logs>New Period**.

2 Delete all snapshots associated with the previous USP release from both RTC system nodes. To do this, perform the following steps:

a In the File Manager window, select the data snapshot to be deleted from the Snapshot field in the RTC portion of the window.

***Note:*** You cannot delete the boot data snapshot. If you attempt to delete the boot data snapshot, you will receive an error message.

b Expand the Snapshot folder.

c Expand the folder for the previous version of the software.

d Click **Delete** to delete the snapshot. An hourglass appears while the data snapshot is deleted. When the deletion operation is complete, snapshot is removed from the RTC side of the File Manager window.

3 Delete old loads from the Alternate Boot Server:

a Open the ABS configuration manager application from the Windows **Start** menu.

b Click on file, then select **uninstall release** from the dropdown menu. The uninstall existing release window appears.

c Select the load to be deleted from the dropdown menu.

d Click **Apply**.

4 Delete old snapshots from the Alternate Boot Server.

a Click the **Administration** button on the main menu.

b Click **File Manager**.

c In the Alternate Boot Server window, navigate to the release associated with the snapshots you wish to remove.

d Click on the snapshot you want to delete.

e Click **Delete**.

5 Perform a hard disk defragmentation on your alternate boot PC. On a Windows 2000 machine, open the Disk Defragmenter utility (**Start>Programs>Accessories>System Tools>Disk Defragmenter**). Select the **Analyze** option. If Windows recommends that the disk be Defragmented, run the utility.



Copyright © 2005, Nortel Networks 

# Migrating the Alternate Boot Server (ABS) from USP PC to CS2000 Management Tools

The purpose of this method is to provide information and instructions for migrating the Alternate Boot Server (ABS) from the USP EM PC to the CS2000 Management Tools server.

## Material requirements

The following is a list of material requirements.

### Required documents

The required documents are listed as follows:

- Job Site Information Package
- Customer Information Documentation (CI or CNCD)
- Installation Safety Manual (ISM/IM0). This document can be requested from the Regional Tool Facility.
- EHS (European Health and Safety) EHS_MAN_002
- WMS (Workmanship Standards) WMS-001

### Tools

The tools listed in the following table are required.

| U.S. Tools | Canadian Tools | Description |
|---|---|---|
| E003389 | E003389 | Installation Data Toolkit |

### Software

Software for USP10.0.0/SN08, USP Compact, or BBSTP on CD is required.

## Precautions

Observe the general safety precautions against personal injury and equipment damage outlined in the ISM/IM0 at all times.

Due to the nature of the BOOTP protocol, the BOOTP server must either be located on the same IP subnet as the USP or be used with a BOOTP server and router that support BOOTP forwarding.

Do not power down a terminal if connected to a console port on the T240. Powering down the terminal will take the T240 down.

Do not disconnect a serial connection to the Netra T240 before closing any application that was previously using the port. This will cause the server to lock-up and will have to be powered down to gain access once again.

Prior to integrating any equipment into the network it is critical to verify the IP Address assigned to the new equipment is not already assigned to existing equipment on the network. A Ping test should be performed prior to assigning IP Addresses to any equipment to verify the IP Address is not currently assigned. Verify no response is received when performing the Ping test prior to integrating any equipment into the network.

## Preparations

Prior to starting the operations presented in this method, arrange all materials, tools, and test equipment at the work location so as to minimize fatigue and inconvenience.

For the installation, you can use either a graphical interface (Hummingbird suite) or a command line interface. If you require it, ensure the FT laptop has Hummingbird install and contains FTP and Exceed.

The following information must be provided by the customer or site specific documentation. Use the following table to help insert the customer provided information throughout the method. The following table will be used for an initial install.

| System variable | Actual value |
|---|---|
| **Client PC Information (Current ABS)** | |
| PC HostName | |
| PC IP Address | |

| System variable | Actual value |
|---|---|
| List all PC usernames and passwords that will be needed<br>DISTINCT BOOTP/FTP/NFS Server passwords<br>ABS Configuration Manager password | |
| Configured Sites | |
| Alternate Boot Loads<br>RTC-12<br>RTC-15 | |
| ABS Snapshot | |
| **CS2000 Management Tools Server (new ABS)** | |
| CMT HostName | |
| CMT IP Address | |
| Root user<br>Root password | root<br>(root password is set to root during factory loading of the ssPFS) |
| User account<br>Password | FIELD<br>SERVICE |
| **BOOTP settings** | |
| SiteName | |
| Gateway IP Address | |
| RTC-12 MAC address | Note: Do not include the :'s |
| RTC-15 MAC address | Note: Do not include the :'s |
| Host IP Address | Note: This is the RTC IP address |
| Server IP Address | Note: This is the CMT IP address |
| Subnet Mask | |

## Overview

In the Succession solution, a customer has the option of moving the existing PC ABS function to the CS2000 Management Tools (CMT) server (ssPFS). The following method will provide the procedures to complete the migration of the ABS and install the USP EM on the ssPFS platform.

This method contains the following procedures:

- Preparing the PC ABS workstation on page 1056
- Creating a user account for the CMT Server on page 1057
- Install/configure the ABS application using only one of the following procedures:
  - Install and configure the ABS application using Exceed on page 1058
  - Install and configure the ABS application using a console on page 1060
- Access verification and pre-migration completion on page 1061
- CMT Server migration on page 1062
- Verification procedure on page 1069
- Post migration procedures on page 1072

## PC ABS workstation

To prepare the PC ABS workstation for installation and configuration procedures, perform the following steps:

### Preparing the PC ABS workstation

***From the ABS PC workstation***

**1** To reduce the amount of data that will need to be moved, uninstall any unused releases from the ABS Manager. To do this, perform the following steps:

***Note:*** The tool checks to ensure that no existing USP sites are using the release loads files and snapshots.

**a** Log into the ABS Configuration Manager: Click **File>Login**.

**b** Type **SERVICE** for the password and click **OK**.

**2** Select **File>Uninstall Release**.

**3** Click on the release that you want to uninstall and select **apply**.

***Note:*** You DO NOT want to remove the current release.

4 Close the Uninstall window when all unused releases have been removed.

5 Delete any old snapshots from the existing USP sites if they are no longer required.

To open the ABS Configuration Window, select **File>ABS Configuration**.

6 Select each Site using the drop-down menu. Using the drop-down menu, select the Snapshot record you want to delete.

7 Click **Delete**.

***Note:*** You will only be able to delete snapshots that begin with bv******. It is also recommended that a customer should keep at least one recent snapshot.

8 Click **OK** when all old snapshots have been removed.

9 Repeat for all sites in office.

10 In the ABS Configuration window, record all the sites that are configured along with their Alternate Boot loads and Snapshot records. (See the table provided on page 1054.)

11 Log out of the ABS Configuration Manager.

12 Click **YES** to confirm and minimize window.

13 Record the BOOTP settings for reference when setting up the CMT as follows:

**a** Open the Distinct BootP Server window.

***Note:*** You may have to log in using **File>Login** (FIELD passwd SERVICE).

**b** Click **Configure>Server**.

**c** Click on each of the Address and Networks tabs.

**d** Capture data.

## CMT Server user account

You will need to complete the setup of the FIELD user account on the ssPFS server. By default, the FIELD account is created in the Succession group. However, the password now needs to be set.

### Creating a user account for the CMT Server

#### *Setup UserID and Password for ABS Server on CMT*

1 Open a Telnet session. To do this, click **Start>Run**.

2 Enter the <CMT IP address>:

**Telnet <CMT IP address>**

3 Click **OK**.

The session opens.

4 Log in as maint:

Type: **maint**

Type: **<maint password>**

5 Switch user to root:

Type: **su - root**

Type: **<root password>**

***Note:*** The FIELD user is created as part of the ssPFS install.

6 Change the password to SERVICE:

Type: **passwd FIELD**

7 Type: **SERVICE**

You will be prompted to re-enter your new password:

8 Do not close the Telnet window.

## Install and configure the ABS application using Exceed

**ATTENTION**
The procedures in this section assume that you are using the software distribution CD.

When installing the BPS/USP EM on the SSPFS server, you will have to export the display to your PC. If you prefer to use a command line interface for this installation, see Install and configure the ABS application using a console on page 1060. The ssPFS is a headless server (no keyboard or monitor) and therefore a GUI install must be re-routed to a PC with a display.

In this procedure, use Exceed to assist in the installation of the USP EM.

### Installing and configuring the ABS application using Exceed

***From the FT Laptop PC***

1 Open Exceed Xconfig. To do this, click **Start >Run**.

2 Type: <directory path of the xconfig.exe file> and click **OK**.

3 Double click on **Security**.

Ensure that in the "Host Access Control List" the **Disabled** (any host access) radio button is selected.

4 Click **OK**.

The Xconfig window opens.

5 Double-click on **Communication**.

Ensure the Mode is set to **Passive**.

6 Click **OK**.

You return to the Xconfig window.

7 Double-click **Screen Definition**.

Ensure that the Window Mode is set to **Multiple**.

8 Click **OK**.

The Xconfig window opens.

9 To close the window, click **File>Exit**.

10 To start an Exceed session, click **Programs>Hummingbird Suite>Exceed>Exceed**.

The program will be running and minimized to the task bar.

11 Return to your Telnet session.

Type: **DISPLAY=<IP address of your PC>:0.0**

***Note:*** To find the IPaddress of the PC you are using, you may need to type: ipconfig from a DOS window.

12 Type: **export DISPLAY**

13 Type: **echo $DISPLAY**

You will see “<IP address of your PC>:0.0”.

14 Type: **cd /cdrom/cdrom0**

Type: **ls**

Ensure that you see the file “install.bin”.

15 Type: **./install.bin**

This may take several minutes to launch, you will see the following response:

- Preparing to install...
- Extracting the JRE from the installer archive...
- Unpacking the JRE...

- Extracting the installation resources from the installer archive...
- Configuring the installer for this system's environment...
- Launching installer...
- .....
- (new PC window)

A new window will appear on your PC (from the Exceed session).

16 Click **Next** and you will see the selection of components to install.

17 Select the components you want to install using the **Choose** button.

18 Click **Next** and you will see a warning for disk space.

19 Click **OK**, and you will see the USP installation directory.

20 When the installation is complete, close the window by selecting **Done**.

## Install and configure the ABS application using a console

If you have already performed this installation with Exceed in the last procedure, skip this procedure.

**Installing and configuring the ABS application using a console**

***From the FT Laptop PC***

1 To switch to the CDROM, enter **cd /cdrom**.

This command may be slightly different depending on the system you are using.

2 To ensure that the file is there, type **LS**.

Check that you see the file “install.bin”.

3 Enter **./install.bin -i console**.

You will now see preparations for console mode installation. This may take a few minutes.

4 Press **Enter** to continue.

You will be presented with a list of components to install.

***Note:*** Selecting these items will toggle the existing setting. For example if the second component is currently selected, and you specify 1 and 2, than only the first component will now be selected as you have deselected the second.

5 You will be asked to confirm your selection.

Press **Enter** to see the default USP directory. You may change this if you wish.

6 Press **Enter** again to start the installation. You will be updated with the installation progress.

7 Press **Enter** to exit.

## Access verification and pre-migration completion

This procedure will verify the access to the ABS Configuration Manager and ensure that there are no sites at this time.

This procedure will also locate the “ntssgusp/abs” directory in preparation for the migration.

### Verifying access and completing pre-migration steps

***From the FT laptop PC***

1 Type: **su - root**

password **<root password>**

2 Type: **cd /data/usp/ntssgusp/**

Type: **chown -R FIELD:maint2 abs**

Type: **chmod -R 775 abs**

3 Check to ensure permissions are set correctly.

Type: **ls -l**

Response:

*drwxrwxrwx 2 FIELD maint2 *date* *time* abs*

4 Start Exceed (see the previous procedure) and ensure that **DISPLAY** is set correctly. (See steps

Type: **cd abs**

5 The following command will start the ABS Configuration Manager and export the display back to the IP assigned in the previous steps.

Type: **./ABS**

You will be prompted to set your password.

6 Enter the Password twice:

Type: **SERVICE**

Type: **SERVICE**

Click **OK**.

7 Log in to the ABS Configuration Manager. To do this, click **File>Login**.

8 Enter **SERVICE** as the password and click **Login**.

9 If you successfully logged into the ABS Configuration Manager, you have verified access.

***Note:*** The window will appear blank. You can Click on the File pull-down menu - if you see logout highlighted then you are logged in.

You can minimize the ABS window.

## CMT Server migration

To migrate to the CMT Server, you perform the following procedures:

- Configure the FTP and NFS servers on the CMT to allow the transfer of files from existing PC ABS, see Configuring the FTP and NFS servers on page 1062.
- Set permissions on the ABS files, see Setting permissions on the ABS files (CMT) on page 1065.
- Verify the data transfer, see Verifying the data transfer on page 1066.
- Enable and configure the BOOTP server on the CMT ABS, see Enabling and configuring the BOOTP server on the CMT ABS on page 1066.
- Disable the BOOTP server on the PC ABS, see Disabling the BOOTP server on the PC ABS on page 1068.
- Verify correct settings for the USP (RTC), see Verifying correct settings for the USP (RTC) on page 1068.

### Configuring the FTP and NFS servers

***From the FT Laptop PC***

1 Open a new Telnet session to the CMT Server.

**maint**

**<maint password>**

2 Switch to user root.

**su - root**

**<root password>**

Root privileges are required for ssPFS modifications.

**3** From the # prompt,

Type: **cli**

The following options appear:

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

**4** Select: **Configuration**.

You will see the Configuration options.

**5** Select **NFS Configuration**.

You will see the NFS Configuration options.

**6** Select **usp_nfs_on** (turn on the USP NFS configuration).

You will see the following followed by the NFS Configuration options:

*=== Executing "usp_nfs_on"*
*USP NFS successfully turned on*
*=== "usp_nfs_on" completed successfully*

**7** Select **X** three times to exit the CLI tool.

**8** Minimize the Telnet session.

***Note:*** The next several steps will move the existing ABS data from the USP EM PC over to the CMT Server. These steps will be performed from the Field Technician's laptop. An abstemp folder will need to be created on the FT laptop to temporarily hold the data during the transfer.

**9** Open a DOS prompt. To do this, click **Start >Run**. Type **cmd** and click **OK**.

**10** Type: **cd **.

**11** Type: **mkdir abstemp**.

**12** Type: **dir /w**.

**13** Ensure that the abstemp folder is present, and close the DOS window.

**14** Before any transfer of data, the FT laptop MUST disable the CyberArmor Personal Firewall.

Mouse over the CyberArmor icon in the task bar (right lower corner of the screen).

a Right-click on the CyberArmor.

b Select **Stop Profile** from the pop-up menu.

c When prompted to stop the profile, click **Yes**.

15 To open an FTP session, click: **Start>Programs> Hummingbird suite>Host Access>FTP for windows Explorer**.

The Hummingbird Neighborhood window appears.

16 To connect to the USP EM PC, click: **File>New FTP Profile**.

17 Complete the FTP Site Properties in the General tab window:

Host Address: **<USP PC IPaddress>**

User Name: **ntssg**

Password: **1ntssgstp** (note: 1 is the #1)

Account:

Initial Directory: **/c/ntssgusp/abs**

18 In the “FTP Site Properties” window, select the **Advanced** tab.

19 De-select **Enable Directory Caching**.

20 De-select **Passive Mode**.

21 In the FTP Site Properties window, select the **Other** tab.

Use the drop-box to select **Binary** for Uploading and Downloading.

22 Click **OK**.

23 Save the FTP profile:

Type: **USP PC**

Click **OK**.

24 Double-click on the **USP PC**.

A new Explorer window appears.

25 Ensure that the FT Laptop PC FTP window has the c:\abstemp directory expanded (use the + to expand the directory structure).

Ensure that the USP PC has the ntssgusp\abs directory expanded.

26 Copy the releases folder from the USP PC to the FT laptop PC.

Right-click on the releases folder and drag it to the C:\abstemp folder. Select **Copy Here**.

You will see the file transfer window while copying the files.

27 Copy the sites folder from the USP PC to the FT laptop PC.

28 Right-click on the sites folder and drag it to the C:\abstemp folder. Select **Copy Here**.

29 Check the C:\abstemp folder to ensure that the releases and sites folders exist (and sub-folders).

30 Close the Explorer window.

31 Double-click on the **CMT server**.

A new Explorer window appears.

***Note:*** The CMT Server profile was created in Creating a user account for the CMT Server on page 1057.

32 Ensure that the FT Laptop PC has the abstemp directory expand and that the CMT has the *\data\usp* directory expanded.

33 Copy folders from the FT Laptop PC to the CMT Server by holding down the Ctrl key and selecting all releases that are not currently present on the CMT Server. Drag and drop these folders by right-clicking **Copy Here**.

34 Ensure that the FT Laptop PC has the abstemp\sites directory expanded. Ensure that the CMT has the \data\usp expanded.

35 Copy all files and folders from the FT Laptop PC to the CMT Server.

36 Right-click and drag and drop the entire Sites folder onto the data\usp\ntssgusp\abs directory.

37 Check to ensure that all data was transferred correctly by expanding the CMT server \data\usp\ntssgusp\abs.

38 Expand each of the releases and sites folders to ensure correct data.

39 Close the Explorer window and the Hummingbird FTP program.

### Setting permissions on the ABS files (CMT)

#### *From the FT Laptop PC*

1 Open/restore a Telnet session to the CMT Server.

2 Ensure that you are logged in as root.

**su - root**

3 Type: **cd /**

Type: **chmod -R 775 /data/usp**

4 Ensure permissions are set correctly.

Type: **cd /data**

Type: **ls -l**

Look for the following line:

*drwxr-xr-x 5 FIELD maint2 *date* *time* usp*

**5** Minimize the Telnet session.

### Verifying the data transfer

#### *From the FT Laptop PC*

**1** Restore or open the ABS Configuration Manager on the CMT Server.

**2** Click on **File>ABS Configuration**.

The Alternate Boot Server window appears.

**3** Verify that all required sites and releases are present.

**4** Select each site in the drop down menu and verify the following:

- RTC loads
- Snapshots

**5** Click on the **Apply** button for each site. When you click the Apply button, the ABS Configuration Manager will rebuild the site specific configuration files based on the CMT directory structure.

**6** Minimize the ABS Configuration Manager window.

### Enabling and configuring the BOOTP server on the CMT ABS

#### *From the FT Laptop PC*

**1** Open a new Telnet session to the CMT Server.

**2** Ensure that you are logged in as root:

**su - root**

Root privileges are required for ssPFS modifications.

**3** From the # prompt,

Type: **cli**

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

**4** Select **Configuration**.

You will see the Configuration options.

**5** Select **Bootp Configuration**.

You will see the Bootp Configuration options.

**6** Select **bootp_add**.

*=== Executing "bootp_add"*

***Note:*** RTC 12 or 15

**7** Enter the bootfile value [bf] for bootp entry.

**8** The following value is for RTC12.

Type: **/data/usp/ntssgusp/abs/sites/<sitename>/ rtc1/rtcboot**

For RTC 15, type:

**/data/usp/ntssgusp/abs/sites/<sitename>/rtc2/ rtcboot**

**9** Enter the gateway IP address [gw] for bootp entry.

Type: **<gateway IP address>**

**10** Enter the home directory [hd] for bootp entry.

Type: **.**

***Note:*** The above character is a period [**.**].

**11** Enter the hardware type [ht] for bootp entry.

Type: **ethernet**

**12** Enter the hardware address [ha] for bootp entry.

***Note:*** Do not include the colon [:] character. The following is an example: (010080E944056B)

Type: **<MAC address>**

**13** Enter the host IP address [ip] for bootp entry.

Type: **<Host IP address>**

***Note:*** RTC IP Address

**14** Enter the server IP address [sa] for bootp entry.

Type: **<Server IP address>**

***Note:*** CMT IP Address

**15** Enter the subnet mask value [sm] for bootpentry.

Type: <subnet mask> Bootfile: *****

Gateway IP Address: **********

Home Directory: **.**

Hardware Type: **ethernet**

Hardware Address: **********

Host IP Address:**********

Server IP Address: **********

Subnet Mask: **********

Type **ok** to accept current settings.

**16** Ensure that all data you entered is correct. If not, type anything other than OK and press Enter. Re-enter the data.

Type: **ok**

=== "bootp_add" completed successfully

Bootp Configuration

1 - bootp_add (Add Entries To The Bootptab File)
2 - bootp_del (Delete Entries From The Bootptab File)
3 - bootp_list (List Out The Bootptab File)
X - exit
select -

**17** Repeat step 1 to step 15 for RTC#2 which is called RTC15.

**18** Type: **X**

You will see the Configuration options.

**19** Select **X** three times to exit the CLI tool.

### Disabling the BOOTP server on the PC ABS

#### *From the USP EM PC*

**1** Restore the (PC) Distinct BOOTP Server window.

**2** Click **Configure>Disabled**.

**3** Exit the Distinct BOOTP Server window. To do this, click **File>Exit**. Click **Yes**.

### Verifying correct settings for the USP (RTC)

#### *From the BOOTP server*

**1** You can use the USP EM PC to perform step 1 to step 5 or log in to the CMT and perform the steps.

**2** Telnet to RTC-12 or RTC-15.

**3** Log in with a valid username and password.

4 Type: **admin abs test rtc-12**

Verify the prompt is returned after issuing the command. This can take a couple of seconds to respond.

The following response indicates that there were no issues.

*CMD>*

5 Type: **admin abs test rtc-15**

Verify the prompt is returned after issuing the command. This can take a couple seconds to respond.

The following response indicates that there were no issues.

*CMD>*

6 Type: **admin abs show all**

Verify that the abs-ipaddress is the address of the CMT ABS and that the correct RTC loads and snapshot are selected.

(Example response ONLY for a site named Ireland):

*~CMD>admin abs show all*
*rtc-12-loadname = ss7rtc_ppc750_08_00_02_25g*
*rtc-15-loadname = ss7rtc_ppc750_08_00_02_25g*
*snapshot-version = v8.0.2*
*snapshot-name = bv2_0-6277d3091d27*
*snapshot-date = 07/29/2003 09:39:39*
*snapshot-description = usp8.0.2.25g_02_purge*
*abs-ipaddress = 47.142.142.26*
*abs-path = /data/usp/ntssgusp/abs/sites/Ireland/rtc2/rtcboot*
*virtual-index = 1*
*~CMD>*

The CMT Server migration is complete.

## Verification procedure



**CAUTION**

Do not perform step 17 to step 33 if this is an in-service site.

### Verifying and testing your work

***From the USP EM PC***

1 Launch the Application Launch Point.

2 Launch the USP GUI.

3 Click **File>session-login**.

4 Log in to the site:

**FIELD**

**SERVICE**

5 Click **Administration**, then select **alternate-boot-server**.

Verify that the BootP response displays the IP address of the CMT Server. Also verify that the bootP path matches what was set during the procedure Enabling and configuring the BOOTP server on the CMT ABS.

6 Click **Test**.

Click **OK**.

7 Check the logs using the **Logs** button on the USP GUI. The "Site" log window appears.

8 Verify that the test completed successfully for each RTC and that there are no ABS related alarms.

In the information field you should see abs test: success.

9 In the Alternate Boot settings window, click **Apply** and verify that the ABS settings are successfully applied (no adverse logs, alarms or pop-ups).

In the log information field you should see abs mod:success.

10 From the USP GUI, click **Administration>Backup**.

11 Enter a snapshot description of "CMT ABS Test Snapshot". Click **Backup**.

***Note:*** This action can take up to 10 minutes.

When the action is complete, a Successful snapshot window will open.

12 Click **OK** and close the backup window.

13 From the USP GUI, click **Administration>File Manager**.

After a couple of minutes, the File Manager window opens.

14 In the right-hand side of the screen (RTC **), double-click **snapshots**.

Double-click the appropriate v8.0.x release folder and locate the snapshot that was just created.

***Note:*** You might have to highlight each snapshot and view the description field to find the snapshot called "CMT ABS Test snapshot" or use the date field.

**15** Select the snapshot and click the left arrow in the middle of the screen to transfer the snapshot to the CMT ABS.

The transfer will be completed when "Ready" is displayed in the bottom left corner of the GUI.

**16** In the left-hand side of the screen (Alternate Boot Server), double-click **snapshots**.

Double-click the appropriate v8.0.x release folder and locate the snapshot that was just transferred.

***Note:*** Use the description field to ensure that you are using the correct snapshot.

**17** Select the snapshot on the ABS (located on the left side of the file manager screen). Click the **delete** button.

Verify that the snapshot is deleted (no adverse logs, alarms or pop-ups). Use the Log manager to verify the logs.

**18** Select the snapshot on the RTC side (located on the right side of the file manager screen). Click the **delete** button.

Verify that the snapshot is deleted (no adverse logs, alarms or pop-ups). Use the Log manager to verify the logs.

**19** Close the window.

***Note:*** Do not perform step 20 to step 35 if this is an in-service site. If this is an in-service site, skip to step 35 (End of Procedure).

***From the FT laptop PC***

**20** Establish an Exceed connection to the CMT Server and launch the ABS Configuration Manager (refer to the procedure Verifying the data transfer to open the ABS Configuration Manager from the CMT Server).

**21** Select **File>Login**. Enter the password **SERVICE**.

**22** Select **File>SSMON**.

The Signaling Server Monitor window will open.

**23** Leave the Signaling Server Monitor window open on the FT laptop and perform the next steps from the USP EM PC.

***From the USP EM PC***

**24** Start the USP EM GUI and log in.

**25** Click **System Mgmt**.

The "Site" System Management window will open.

**26** Click the first shelf on the top left.

The control shelf window will open

**27** Look at the graphical representation of the RTC cards in slot 12 and slot 15. The active RTC will have a check mark in a small box. You must perform this test on the inactive RTC.

Click the inactive RTC to open the screen and note the IP address for this card. This IP address is used in the next step as the <Inactive IP address>.

**28** Click **Start>Run** and type: **FTP <Inactive IP address>**.

**29** Log in using the FIELD username with password SERVICE account.

**30** Type: **cd /sd0 *** Changed directory to "/sdo"**.

**31** Type: **del sysconf**.

**32** From the USP GUI, click the lock button on the inactive RTC that is currently open. Click **Yes**.

The RTC changes to LOCK status.

**33** From the USP GUI, click the load button on the inactive RTC that is currently open. Click **Yes**.

***Note:*** Several pop-ups may be generated indicating a loss of connection to the RTC (This step could several minutes).

**34** Monitor the SSMON window for status messages as the RTC performs an alternate boot. The entire process can take up to 15 to 30 minutes.

**35** When connectivity to the RTC is restored (a pop up message will open). Click **OK**.

**36** Click the unlock button on the inactive RTC that is currently open.

The verification is complete.

## Post migration procedures

For SN07, you cannot uninstall the USP GUI (the uninstall would also remove the ABS package). The following procedure will remove the

items that are used for the ABS functionality on the USP EM PC. The absCD temporary folder will also be removed from the CMT Server.

### Removing the items used for ABS functionality

***From the USP EM PC***

1. Delete the ABS Manager icon from the desktop by right-clicking on the icon and selecting **Delete**. Click **Yes** to confirm the shortcut delete.
2. Remove the ABS Manager, SSMON, BOOTP, FTP, and NFS shortcuts from the startup folder. Click on **Start >Programs> Startup** and right-click on the ABS Manager and select **Delete**.
3. Click **Yes** to confirm the ABS Manager can be sent to the recycling bin.
4. Repeat steps 2 and 3 for each of the following: BootP Server, FTP Server, NFS Server, and Signaling Server Monitor.
5. If there is an entry in the Start>Programs>Universal signaling point folder for the ABS Manager, delete the entry by highlighting the entry with the mouse and then right-clicking it and selecting delete.
6. Click **Yes** to confirm the file delete.
7. Reboot the PC and verify that the ABS Manager, SSMON, BOOTP, FTP, and NFS applications are not started.

### Telnet to the CMT and removing the absCD folder

***From the USP EM PC***

1. Click **Start>Run**.

   Type: **Telnet <CMT IP Address>**.

   *Login prompt*
2. Log in as maint:

   Type: **maint**.

   Type: **<maint password>**.

   *Prompt*
3. Switch user to root:

   Type: **su - root**.

   Type: **<root password>**.
4. Type: **cd /data/usp**.

Type: **ls**.

The following is an example response.

*absCD*
*data*
*ntssgusp*
*UninstallerData*
*Universal_Signaling_Point_v10.0.0_InstallLog.log*

**5** Type: **rm -rf absCD**.

The command will remove the absCD directory and all the contents inside the directory.

**6** Exit from the Telnet session.

Type: **exit**

***Note:*** You might need to type exit a couple of times.

**7** Contact the Network Engineer for the site and inform them of the changes to the bootp server addresses on the USP. They can update the site specification book with this information.

# In-Service Introduction of Inter-CAM Communication Media (ICCMs)



**CAUTION**

To reduce the risk of service-affecting issues, Nortel Networks recommends that you perform the procedure during low traffic periods in the maintenance time frame.



**CAUTION**

Make sure that the dual-shelf system is working properly before starting the conversion procedure. Check alarm information to make sure there are no alarms pointing to problems with CC cards, RTC cards, fibre-optic cable states, loss of communication redundancy (LOCR), isolation, or shelf states. Make sure that all connecting nodes and network connections are in service. Review and coordinate the conversion procedure with other operating companies in the network.



**CAUTION**

If your system has a mate system, do not perform maintenance activities on the mate while you perform the conversion procedure on the first node. Performing maintenance activities during an inservice conversion can affect service.

This section describes the procedure for the in-service conversion of the USP from a dual-shelf system, that links directly through OC-3 cables, to a system where the shelves link through two Inter-CAM Communication Media (ICCM). The system can be expanded to a multi-shelf system with up to eight Communications Application Module (CAM) shelves.

One shelf remains designated as the control CAM shelf and the additional shelves are designated as extension CAM shelves. Each extension shelf contains two CCs and a maximum of 16 additional system nodes.

To maintain the existing redundancy and availability of the Signaling Server platform, two ICCMs are deployed in the system configuration. One CC node on each shelf is connected to the first ICCM. The other CC node on each shelf is connected to the second ICCM. This configuration allows full redundancy of SS7 messaging as well as the inservice upgrade capability of the ICCMs. The servicing of one ICCM can take place while the second ICCM carries traffic. This ensures no service impact to SS7 traffic on the link cards.

## Hardware requirements

The following tables describe the additional minimum hardware requirements needed for the in-service conversion.

**Additional minimum hardware required for dual-shelf in-service conversion**

| Name | PEC | Quantity |
|---|---|---|
| ICCM (Marconi TNX-210 ATM Switch) | NTST87AA | 2 for the system |
| RTC CE3 (Computing Engine 3 with PP4) | NTST11BA | 2 for the control shelf |
| OC-3 Fibre Cables | NTST88AA | 4 (2 for each shelf) |

**Additional minimum hardware required for four-shelf in-service conversion**

| Name | PEC | Quantity |
|---|---|---|
| ICCM (Marconi TNX-210 ATM Switch) | NTST87AA | 2 for the system |
| RTC CE3 (Computing Engine 3 with PP4) | NTST11BA | 2 for the control shelf |
| OC-3 Fibre Cables | NTST88AA | 8 (2 for each shelf) |

**Additional minimum hardware required for five-shelf in-service conversion**

| Name | PEC | Quantity |
|---|---|---|
| ICCM (Marconi TNX-210 ATM Switch) | NTST87AA | 2 for the system |
| RTC CE3 (Computing Engine 3 with PP4) | NTST11BA | 2 for the control shelf |
| OC-3 Fibre Cables | NTST88AA | 10 (2 for each shelf) |

**Additional minimum hardware required for eight-shelf in-service conversion**

| Name | PEC | Quantity |
|---|---|---|
| ICCM (Marconi TNX-210 ATM Switch) | NTST87AA | 2 for the system |
| RTC CE3 (Computing Engine 3 with PP4) | NTST11BA | 2 for the control shelf |
| OC-3 Fibre Cables | NTST88AA | 16 (2 for each shelf) |

The conversion procedure has the following prerequisites:

- The USP software upgrade must be complete, and all nodes in the system must be running the same load.
- The USP must be provisioned with all hardware required for a dual-shelf system.
- The RTC must be provisioned with a CE3 (Computing Engine 3 with PP4), running a PP4 750-based load.
- Two ICCMs and associated cabling must be available on-site.

A brief description of each of the minimum hardware requirements follows.

**ICCM** (Marconi TNX-210 ATM Switch) — Each ICCM provides room for expansion to up to 16 OC-3 ports. The ICCM terminates the OC-3 links

from the CAM shelves and provides routing between the CAM shelves on the system.

***Note:*** Nortel Networks arranges the provisioning of the ICCMs to allow the CAM shelves to communicate properly. Once the ICCMs are powered up, they are ready to route ATM messages. If a routing error occurs, contact your next level of support.

**OC-3 fibre cables** -- The OC-3 fibre cable between the CCs and the ICCMs is a standard multi-node fibre cable with SC connectors. This cable is custom-built for the application. The same OC-3 cable is used for connection of dual-shelf systems. Nortel Networks recommends that you have extra OC-3 cables on site in case of fibre optic cable failure.

**OAMP workstation** -- The workstation hosts the USP GUI.

***Note:*** For additional information on provisioning the hardware, contact your installation prime.

## In-service introduction of ICCMs process

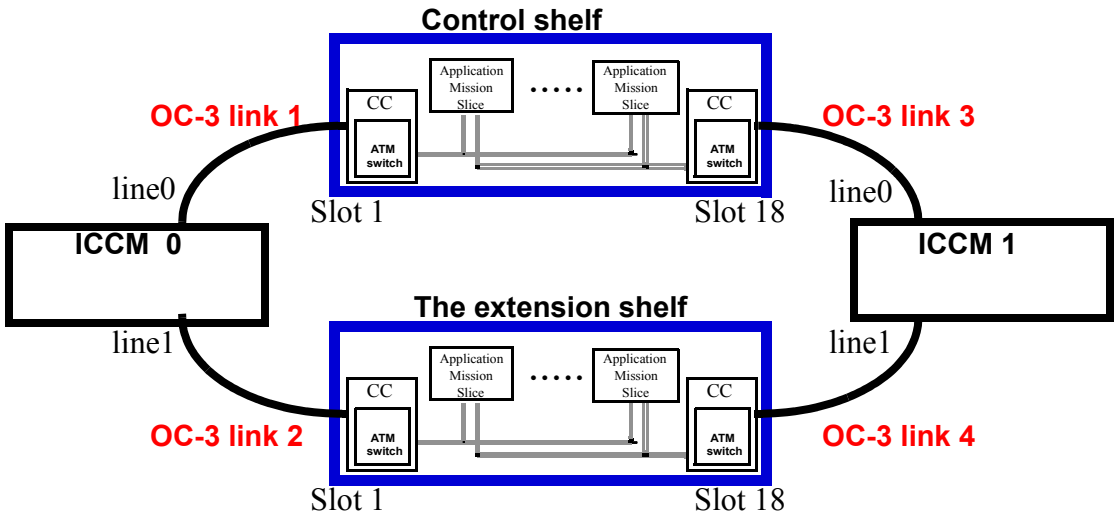


**CAUTION**

During most of the conversion procedure, the system operates without redundancy. Nortel Networks recommends that the conversion take place during low traffic periods in the maintenance window in order to avoid loss of service.

This section describes the step-by-step inservice conversion procedure for converting a system from a dual-shelf system, that links directly through OC-3 fibre optic cables, to a system where the CAM shelves link through ICCMs.

## ICCM connectivity with system shelves




A dual-shelf system with ICCMs uses four OC-3 cable links. The following is a summary of the cable connections:

- OC-3 link 1 connects the CC in slot 1 on the control CAM shelf to line 0 on line card 0 of ICCM 0.
- OC-3 link 2 connects the CC in slot 1 on the extension CAM shelf to line 1 on line card 0 of ICCM 0.
- OC-3 link 3 connects the CC in slot 18 on the control CAM shelf to line 0 on line card 0 of ICCM 1.
- OC-3 link 4 connects the CC in slot 18 on the extension CAM shelf to line 1 on line 0 of ICCM 1.

***Note:*** In order for the pre-configured ICCMs to operate correctly with the CAM shelves, the system must be connected as specified in this document.

To avoid disruption to service, only one set of the CCs is disabled at one time, and all traffic is carried on the other set of CCs during the conversion procedure. In this document, conversion of the CCs in slot 1 occurs first, followed by the conversion of the CCs in slot 18.

### In-service introduction of ICCMs procedures

In-service introduction of ICCMs in a dual-shelf system requires the completion of the following separate procedures:

1. Upgrade USP software.
2. Login and check alarms.

3. Disable and offline the CC in slot 1 on the extension CAM shelf.
4. Disable and offline the CC in slot 1 on the control CAM shelf.
5. Remove OC-3 cable connections for the CCs in slot 1 and connect the CCs to ICCM 0.
6. Enable the CC in slot 1 on the control CAM shelf.
7. Enable the CC in slot 1 on the extension CAM shelf.
8. Check OMs to ensure messaging goes through ICCM 0.
9. Soak the system after conversion of the CCs in slot 1.
10. Disable and offline the CC in slot 18 on the extension CAM shelf.
11. Disable and offline the CC in slot 18 on the control CAM shelf.
12. Remove OC-3 cable connections for the CCs in slot 18 and connect the CCs to ICCM 08.
13. Enable the CC in slot 18 on the control CAM shelf.
14. Enable the CC in slot 18 on the extension CAM shelf.
15. Check OMs to ensure messaging goes through ICCM 1.
16. Add ICCMs to the system GUI.
17. Soak the dual-shelf system.

### Upgrading the USP software

***In the Upgrade customer documentation***

**1** See Upgrading the USP on page 1012.

### Logging in and checking alarms

***At the OAMP workstation***

**1** Double-click the system icon on your OAMP workstation to display the login window.

**2** To log into the system GUI, select a site and enter a user identification and password.

**3** Check alarm information to make sure there are no alarms pointing to problems with CC cards, RTC cards, fibre-optic cable states, loss of communication redundancy (LOCR), isolation, or shelf states. To view alarms, click the alarm banner. The Alarms window appears.

### Disabling and offlining the CC in slot 1 on the extension CAM shelf

*On the system GUI*

1 Click **Configuration>platform>node>graphical view**.

2 Click the icon for the extension shelf to open the *shelf_name* window for the extension CAM shelf.

3 Click the icon for the CC in slot 1 to open the CC in slot 1 on the **graphical view** window for the extension CAM shelf.

4 Click **Lock** to lock the CC in slot 1. A popup window appears. Click **Yes** to confirm the change. Check the Administrative state (the word “Locked” should be highlighted).

5 Click **Offline** to offline the CC in slot 1. A popup window appears. Click **Yes** to confirm the change. Click **OK** to continue. Check the Availability status in the Maintenance portion of the window. The word “Offline” should be highlighted.

6 Click **Close** to return to the *shelf_name* window for the extension CAM shelf. Click **Close** to return to the **System Configuration** window.

### Disabling and offlining the CC in slot 1 on the control CAM shelf

*On the system GUI*

1 Click **Configuration>platform>node>graphical view**.

2 Click the icon for the control CAM shelf to open the *shelf_name* window for the control CAM shelf.

3 Click the icon for the CC in slot 1 to open the CC in slot 1 on the **maintenance and provisioning** window for the control CAM shelf.

4 Click **Lock** to lock the CC in slot 1. A popup window appears. Click **Yes** to confirm the change. Check the Administrative state in the Maintenance portion of the window. The word “Locked” should be highlighted.

5 Click **Offline** to offline the CC in slot 1. A popup window appears. Click **Yes** to confirm the change. Click **OK** to continue. Check the Availability status in the Maintenance portion of the window. The word “Offline” should be highlighted.

6 Click **Close** to return to the *shelf_name* window for the control CAM shelf. Click **Close** to return to the **System Configuration** window.

### Removing OC-3 cable connections for the CCs in slot 1 and connecting the CCs to ICCM 0



**CAUTION**

When you remove the OC-3 cable, make sure that you remove the cable from the CCs in slot 1. Removal of the OC-3 cable from the CCs in slot 18 can disrupt service. Make sure that the LED on the CC TM is OFF before you remove the OC-3 cable. If the LED is ON, the CC is enabled, and loss of service can occur

***On the system***

1 Remove the OC-3 cable connecting the CC in slot 1 on the control CAM shelf to the CC in slot 1 on the extension CAM shelf.

2 Use the OC-3 cable to connect the CC in slot 1 on the control CAM shelf to line 0 on line card 0 of the ICCM 0. Check the lights on the ICCM 0 for line 0. A green light indicates the cable connection is correct. If the red light is on, a line error occurred. If a problem occurs, perform the steps in the Troubleshooting an OC-3 cable connection on page 1089.

3 Use an OC-3 cable to connect the CC in slot 1 on the extension CAM to line 1 on line card 0 of the ICCM 0. Check the lights on the ICCM 0 for line 0. A green light indicates the cable connection is correct. If the red light is on, a line error occurred. If a problem occurs, perform the steps in the Troubleshooting an OC-3 cable connection on page 1089.

### Enabling the CC in slot 1 on the control CAM shelf

***On the system GUI***

1 Click **Configuration>platform>node>graphical view**.

2 Click the icon for the control CAM shelf to open the *shelf_name* window for the control CAM shelf.

3 Click the icon for CC in slot 1 to open the CC in slot 1 on the **maintenance and provisioning** window for the control CAM shelf.

4 Click **Load** to load the CC in slot 1. A popup window appears. Click **Yes** to confirm the change. Check the Operational state in the Maintenance portion of the window to verify the changes. The word “Unlocked” should be highlighted.

5 Click **Unlock** to unlock the CC in slot 1. A popup window appears. Click **Yes** to confirm the change. Check the Administrative state in the Maintenance window. The word “Unlocked” should be highlighted.

6 Click **Close** to return to the *shelf_name* window for the control CAM shelf. Click **Close** to return to the **System Configuration** window.

### Enabling the CC in slot 1 on the extension CAM shelf

***On the system GUI***

1 Click **Configuration>platform>node>graphical view**.

2 Click the icon for the extension CAM shelf to open the *shelf_name* window for the extension CAM shelf.

3 Click the icon for CC in slot 1 to open the CC in slot 1 on the **maintenance and provisioning** window for the extension CAM shelf.

4 Click **Load** to load the CC in slot 1. A popup window appears. Click **Yes** to confirm the change. Check the Operational state in the Maintenance portion of the window to verify the changes. The word “Unlocked” should be highlighted.

5 Click **Unlock** to unlock the CC in slot 1. A popup window appears. Click **Yes** to confirm the change. Check the Administrative state in the Maintenance window. The word “Unlocked” should be highlighted.

6 Click **Close** to return to the *shelf_name* window for the extension CAM shelf. Click **Close** to return to the **System Configuration** window.

7 Wait for at least 10 minutes after enabling the CC in slot 1 on the extension shelf. Check the system logs and OMs for any unusual events.

### Checking OMs to ensure messaging goes through LCCM 1

***On the system GUI***

1 Click **Performance>om**.

2 Click **Search**.

3 In the critera box select:

- *application-name* from the **Field** drop-down menu
- *equal* from the **Condition** drop-down menu
- *ATM Driver Messaging* from the **Value** drop-down menu

4 Click **Retrieve**.

### Soaking the system after the conversion of CCs in slot 1

#### *At the OAMP workstation*

1 Allow the system to soak for one hour after the conversion of the CCs in slot 1.

2 Check the logs for the system. Click **Logs** on the main menu to open the Logs window.

3 Check the alarms for the system. To view alarms, click the alarm banner. The Alarms window appears. Check alarm information to make sure there are no alarms pointing to problems with CC cards, RTC cards, fibre-optic cable states, loss of communication redundancy (LOCR), isolation or shelf states.

If a problem or failure occurs at any time during soak do not proceed to the following steps until the problem is resolved and the alarm clears. If you cannot resolve the problem, contact your next level of support.

### Disabling and offlining the CC in slot 18 on the extension CAM shelf

#### *On the system GUI*

1 Click **Configuration>platform>node>graphical view**.

2 Click the icon for the extension CAM shelf to open the *shelf_name* window for the extension CAM shelf.

3 Click the icon for the CC in slot 18 to open the CC in slot 18 on the **maintenance and provisioning** window for the extension CAM shelf.

4 Click **Lock** to lock the CC in slot 18. A popup window appears. Click **Yes** to confirm the change. Check the Administrative state in the Maintenance portion of the window. The word “Locked” should be highlighted.

5 Click **Offline** to offline the CC in slot 18. A popup window appears. Click **Yes** to confirm the change. Click **OK** to continue. Check the Availability state in the Maintenance portion of the window. The word “Offline” should be highlighted.

6 Click **Close** to return to the *shelf_name* window for the extension CAM shelf. Click **Close** to return to the **System Configuration** window.

### Disabling and offlining the CC in slot 18 on the control CAM shelf

***On the system GUI***

1 Click **Configuration>platform>node>graphical view**.

2 Click the icon for the control CAM shelf to open the *shelf_name* window for the control CAM shelf.

3 Click the icon for the CC in slot 18 to open the CC in slot 18 on the **maintenance and provisioning** window for the control CAM shelf.

4 Click **Lock** to lock the CC in slot 18. A popup window appears. Click **Yes** to confirm the change. Check the Administrative state in the Maintenance portion of the window. The word “Locked” should be highlighted.

5 Click **Offline** to offline the CC in slot 18. A popup window appears. Click **Yes** to confirm the change. Click **OK** to continue. Check the Availability state in the Maintenance portion of the window. The word “Offline” should be highlighted.

6 Click **Close** to return to the *shelf_name* window for the control CAM shelf. Click **Close** to return to the **System Configuration** window.

### Removing the OC-3 cable connections for the CCs in slot 18 and connecting the CCs to ICCM 1



**CAUTION**

When you remove the OC-3 cable, make sure that you remove the cable from the CCs in slot 18. Removal of the OC-3 cable from the CCs in slot 1 can disrupt service. Make sure that the LED on the CC TM is OFF before you remove the OC-3 cable. If the LED is ON, the CC is enabled, and loss of service can occur

***On the system***

1 Remove the OC-3 cable connecting the CC in slot 18 on the control CAM shelf to the CC in slot 18 on the extension CAM shelf.

2 Use the OC-3 cable to connect the CC in slot 18 on the control CAM shelf to line 0 on line card 0 of the ICCM 1. Check the lights on the ICCM 1 for line 0. A green light indicates the cable connection is correct. If the red light is on, a line error occurred.

If a problem occurs, perform the steps in the Troubleshooting an OC-3 cable connection on page 1089.

3 Use an OC-3 cable to connect the CC in slot 18 on the extension CAM to line 1 on line card 0 of the ICCM 1. Check the lights on the ICCM 1 for line 0. A green light indicates the cable connection is correct. If the red light is on, a line error occurred. If a problem occurs, perform the steps in the Troubleshooting an OC-3 cable connection on page 1089.

### Enabling the CC in slot 18 on the control CAM shelf

***On the system GUI***

1 Click **Configuration>platform>node>graphical view**.

2 Click the icon for the control CAM shelf to open the *shelf_name* window for the control CAM shelf.

3 Click the icon for CC in slot 18 to open the CC in slot 18 on the **maintenance and provisioning** window for the control CAM shelf.

4 Click **Load** to load the CC in slot 18. A popup window appears. Click **Yes** to confirm the change. Check the Operational state in the Maintenance portion of the window to verify the changes. The word “Unlocked” should be highlighted.

5 Click **Unlock** to unlock the CC in slot 18. A popup window appears. Click **Yes** to confirm the change. Check the Administrative state in the Maintenance window. The word “Unlocked” should be highlighted.

6 Click **Close** to return to the *shelf_name* window for the control CAM shelf. Click **Close** to return to the **System Configuration** window.

### Enabling the CC in slot 18 on the extension CAM shelf

***On the system GUI***

1 Click **Configuration>platform>node>graphical view**.

2 Click the icon for the extension CAM shelf to open the *shelf_name* window for the extension CAM shelf.

3 Click the icon for CC in slot 18 to open the CC in slot 18 on the **maintenance and provisioning** window for the extension CAM shelf.

4 Click **Load** to load the CC in slot 18. A popup window appears. Click **Yes** to confirm the change. Check the Operational state in

the Maintenance portion of the window to verify the changes. The word “Unlocked” should be highlighted.

5 Click **Unlock** to unlock the CC in slot 18. A popup window appears. Click **Yes** to confirm the change. Check the Administrative state in the Maintenance window. The word “Unlocked” should be highlighted.

6 Click **Close** to return to the *shelf_name* window for the extension CAM shelf. Click **Close** to return to the **System Configuration** window.

7 Wait for at least 10 minutes after enabling the CC in slot 18 on the extension shelf.

### Checking OMs to ensure messaging goes through ICCM 1

#### *On the system GUI*

1 Click **OMs** on the main menu to open the **Operation Measurements** window.

2 Set the interval to five minutes in the **Interval Type** field. Click **Query Interval Data** to open the **OMBrowser Interval Selection** window.

3 Click on the bottom line of the window to select the last five-minute interval. Click **Get Selected Intervals**. A popup window appears. Click **Yes** to confirm your change.

4 Click **Open Filter Selection Window** to open the **Operational Measurements Filter** window.

5 Select “ATM Driver Messaging” in the **Application Filter** list.

6 Select the CC in slot 18 on the extension shelf in the **Element Filter** list.

7 Click **Close** to return to the **Operational Measurements** window.

8 In the Register portion of the window, locate “Plane 1 Message Count” and “Plane 2 Message Count”. The OM Value should be the same for each count. If the OM value is not the same for the two counts, contact your next level of support.

## Adding ICCMs on the system GUI

### *On the system GUI*

1 Click **System mgmt** on the main menu to open the **System Configuration** window.

2 Click **Add ICCM**. A popup window appears. Click **Yes** to confirm the change. Click **OK** to continue. Two ICCMs appear on the GUI.

3 Check the OC-3 link state indicator on the GUI to make sure all the OC-3 links are up.

If an OC-3 link is down, the OC-3 link indicator changes to show a broken link in the black square below the shelf.

## Soaking the dual-shelf system

**ATTENTION**

If a failure occurs at any time during this phase, refer to Conversion failure management on page 1089. If you cannot resolve the problem, contact your next level of support.

**ATTENTION**

When you complete this procedure, you can now install additional shelves on the system. Refer to the section “Adding an Extension Shelf” in the Configuration Management guide.

### *At the OAMP workstation*

1 Allow the system to soak for one hour after the conversion to a system with two ICCMs.

2 Check the logs for the system. Click **Logs** on the main menu to open the Logs window.

3 Check the alarms for the system. To view alarms, click the alarm banner. The Alarms window appears. Check for alarms pointing to problems with CC cards, RTC cards, fibre-optic cable states, loss of communication redundancy (LOCR), isolation or shelf states.

4 Check the OC-3 link state indicator on the system GUI. Make sure all of the OC-3 links are up.

## Troubleshooting and system recovery

This section provides the procedures for troubleshooting and recovering a system from problems encountered during the conversion process.

Each line on the ICCM has a green light and a red light. A green light indicates a correct OC-3 cable connection. A red light indicates a problem with the connection. After you connect the CAM shelves to the ICCMs using OC-3 cables, check the lights. If the red light is on, perform the following steps:

### Troubleshooting an OC-3 cable connection

***At the ICCM***

1 A reversal of the RX and TX nodes on the OC-3 cable can be the problem. To solve the problem, unplug the cable, switch the RX and TX nodes, and plug the cable in again. If the green light is on, continue with the conversion procedure. Otherwise, perform the next step.

2 Use another OC-3 cable to replace the current cable. Make sure that you connect the RX and TX nodes correctly. If the green light is on, continue with the conversion procedure. If the problem continues, contact your next level of support.

## Conversion failure management

To abort the conversion, perform the following backout procedures:

1. Remove ICCMs on the system GUI.
2. Perform a back out for the ICCM 1.
3. Remove the ICCM and connect the CCs with direct OC-3 cable links.
4. Perform a back out for the ICCM 0.

### Removing ICCMs from the system GUI

**ATTENTION**
If you added ICCMs on the system GUI, perform the following steps to remove them. If no ICCMs were added, skip this procedure.

***At the OAMP workstation***

1 On the system GUI, open the System Configuration window. To do this, click **Configuration>platform>system**.

2 Click **Delete ICCM**. A popup window appears. Click **Yes** to confirm. Click **OK** to continue. The system removes the ICCMs from the GUI.

***Note:*** After this step, you can continue the backout procedure or contact your next level of support.

### Performing a back out for ICCM 1

#### *At the OAMP workstation*

1 Disable and offline the CC in slot 18 on the extension shelf. See Disabling and offlining the CC in slot 18 on the extension CAM shelf on page 1084.

2 Disable and offline the CC in slot 18 on the control shelf. See Disabling and offlining the CC in slot 18 on the control CAM shelf on page 1085.

3 Remove ICCM 1 and connect the CCs in slot 18 with direct OC-3 cable links. See Removing the OC-3 cable connections for the CCs in slot 18 and connecting the CCs to ICCM 1 on page 1085.

4 Enable the CC in slot 18 on the control shelf. See Enabling the CC in slot 18 on the control CAM shelf on page 1086.

5 Enable the CC in slot 18 on the extension shelf. See Enabling the CC in slot 18 on the extension CAM shelf on page 1086.

### Removing the ICCM and connecting the CCs with direct OC-3 cable links



**CAUTION**

When you remove the OC-3 cables, make sure that you remove the OC-3 cables from the CCs in slot 18 connecting to ICCM 1. Removal of the OC-3 cables from the CCs in slot 1 connecting to ICCM 0 can result in loss of service. Make sure that the LED on the CC TM card is OFF before removing the OC-3 cables. If the LED is ON, the CC is enabled and service can be disrupted.

#### *At the system*

1 Remove the OC-3 cable connecting the CC on the control CAM shelf to the line card of the ICCM.

2 Remove the OC-3 cable connecting the CC on the extension CAM shelf to the line card of the ICCM.

3 Use an OC-3 cable to connect the CC on the control CAM shelf to the CC on the extension CAM shelf.

### Performing a back out for ICCM 0

***At the system***

1 Disable and offline the CC in slot 1 on the extension shelf. See Disabling and offlining the CC in slot 1 on the extension CAM shelf on page 1081.

2 Disable and offline the CC in slot 1 on the control shelf. See Disabling and offlining the CC in slot 1 on the control CAM shelf on page 1081.

3 Remove ICCM 0 and connect the CCs in slot 1 with direct OC-3 cable links. See Removing OC-3 cable connections for the CCs in slot 1 and connecting the CCs to ICCM 0 on page 1082.

4 Enable the CC in slot 1 on the control shelf. See Enabling the CC in slot 1 on the control CAM shelf on page 1082.

5 Enable the CC in slot 1 on the extension shelf. See Enabling the CC in slot 1 on the extension CAM shelf on page 1083.

# USP High-Speed Link Cutover Procedure



**CAUTION**

Cutover should be conducted during a maintenance window, where the low speed link traffic is below 0.2 erlang.

To cutover from 16 LSL to two HSLs, the low speed link traffic must be less than 0.1 erlang.

This section details procedures for converting a Common Channel Signaling System 7 (SS7) low-speed link (LSL) linkset into an high-speed link (HSL) linkset.

Throughout this document, links originating on DS0A, V.35 or Channelized E1/T1 link system nodes are referred to as low-speed links (LSLs). Links originating on high-speed link or SS7 IP link system nodes are referred to as high-speed links (HSL). The ATM high-speed link system node physically consists of the T1/E1 Transition Module (TM) and a link mission card. The computing engine mission card consists of a Power/SCSI/Ethernet (PSE) TM, an SS7 IP link mission card, and an MTP2 E1 HSL.

This section also provides the procedures to transition from low-speed link (LSL) linksets to high-speed link (HSL) linksets.

## Hardware requirements

The following hardware is required for ATM high-speed links:

- T1/E1 Transition Module NTST81BA, or NTST81AB
- Link Mission Card
  - NTST10BA (base link card)

The following hardware is required for E1 MTP2 high-speed links:

- T1/E1 Transition Module NTST81BA
- Link Mission Card
  - NTST10CA

The following hardware is required for SS7 IP High Speed links:

- PSE TM NTST09AA, NTST09AB, or NTST09AC
- IP Link Mission Card which includes:
  - NTST11BA (LE3)

For further information about issues related to hardware installations involving high-speed links (HSL), contact the installation prime.

## Software requirements

Software release USP8.0 or later is required for this cutover.

# HSL cutover process

**ATTENTION**

Ensure that the network to be converted and all connecting nodes and network connections are in service.

Ensure that all alarms have been cleared before proceeding with the cutover procedure.

Review and coordinate the cutover procedure with other operating companies in the network that are involved in the cutover procedure.

Up to sixteen ATM/E1or MTP2 HSL system nodes can be commissioned on an extension shelf (12 on a control shelf). For IP HSLs, up to eight HSL, can be commissioned on each shelf. On a fully populated system, an LSL link system node must be decommissioned before installing each HSL system node. Existing links on the LSL system node must be moved to other link system nodes or decommissioned. If your system is fully populated, contact your next level of support.

The cutover procedure requires operating company personnel to be present at each office that is affected by a link change during any step of the procedure. Nortel Networks recommends that you appoint a cutover project manager to coordinate all the steps for the cutover.

## HSL cutover guidelines

Note the following guidelines when performing the HSL cutover:

- The high-speed link system node can support HSLs for C-links, B/D links, or A-links.
- Carry out the C-linkset cutover before the signaling transfer point (STP) quad B/D-linkset cutover because only two nodes are involved in the C-linkset cutover.
- An HSL system node provides a single port in the same space that an LSL system node provides four or eight ports. Therefore, on a full system, four or eight LSL ports must be decommissioned for each HSL added.

The HSL cutover applies to:

- C-linkset cutover for a signaling transfer point (STP) pair
- B-linkset cutover for an STP quad
- D-linkset cutover for an STP quad
- A-links-to-service control point (SCP) cutover
- A-links-to-SSP cutover

***Note:*** Nortel Networks recommends performing the C-linkset cutover for an STP pair before attempting the B-linkset and D-linkset cutover for an STP quad.

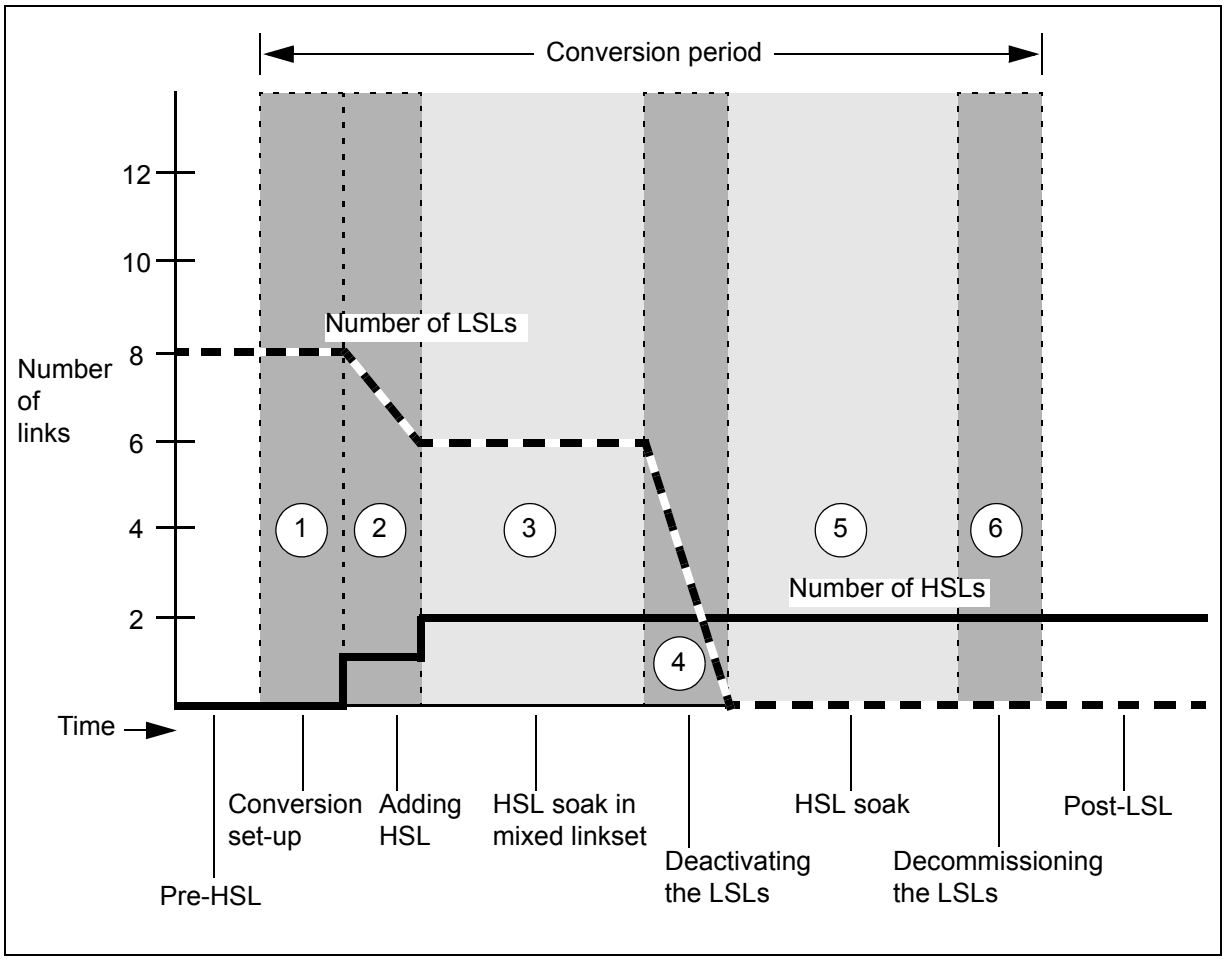
### HSL cutover procedures

**ATTENTION**
During cutover, HSLs and LSLs are supported in the same mixed linkset. The USP supports mixed HSL and LSL linksets only during the cutover procedure. After the cutover is complete, linksets should be homogeneous.

**ATTENTION**
Contact your next level of support to determine the correct version of the engineering bulletin and to determine if any other engineering bulletins apply.

The following figure shows the cutover steps.

## Link count during cutover



The HSL cutover requires completing the following procedures:

1. Cutover setup.
   a. Configure the HSL system node. Refer to the procedure “Provisioning Links” in the Operational Configuration section of the customer documentation.
   b. Configure ports. Refer to the procedure “Provisioning Links” in the Operational Configuration section of the customer documentation.

      ***Note:*** For MTP2 E1 HSLs the cable must be connected to RJ45 cable.

   c. Load the HSL system nodes. Refer to the procedures “Provisioning Links” in the Operational Configuration section of the customer documentation.
2. Add HSLs.
   a. Configure SAAL timers. Refer to the procedure “Adding a SAAL Timer or Parameter Index” in the Operational Configuration section of the customer documentation.
   b. Configure SAAL parameters. Refer to the procedure “Adding a SAAL Timer or Parameter Index” in the Operational Configuration section of the customer documentation.
   c. Deactivate LSLs. Refer to the procedure “Activating and Deactivating Links” in the Operational Configuration section of the customer documentation.
   d. Delete LSLs. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.
   e. Configure HSLs. Refer to the applicable ATM, E1 MTP2, or IP HSL procedure in the Operational Configuration section of the customer documentation.
   f. Perform BERT on ATM and E1 MTP2 before RTSing the links, “Perform BERT” in the Security and Administration guide.
   g. RTS the link. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
3. Soak the HSLs in a mixed linkset. Refer to the procedure Soaking the HSLs on page 1099.

4. Offline the LSLs.
   a. Calculate LSL traffic. Refer to the procedure “Performing USP traffic calculations” in the Operational Configuration section of the customer documentation.

      ***Note:*** If the Erlang level is above 0.2 E, contact the personnel responsible for your next level of support. Use Operational Measurements to calculate traffic and to determine if you can proceed with the cutover.

   b. Calculate LSL traffic on the mate node. Refer to the procedure “Performing USP traffic calculations” in the Operational Configuration section of the customer documentation.

      ***Note:*** If the Erlang level is above 0.2 E, contact the personnel responsible for your next level of support. Use Operational Measurements to calculate traffic and to determine if you can proceed with the cutover.

   c. Deactivate the LSL. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
   d. Deactivate all remaining LSLs in the linkset. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
   e. Deactivate the LSL on the mate node. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
   f. Deactivate all remaining LSLs in the linkset on the mate node. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.

5. Soak the HSLs. Refer to the procedure Soaking the HSLs on page 1099.
6. Decommission the LSLs.
   a. Delete the datafill for the LSLs. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.
   b. Delete LSLs for remaining links in the linkset. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.
   c. Delete the datafill for the LSLs on the mate node. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.
   d. Delete LSLs for remaining links in the linkset on the mate node. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.

### Soaking the HSLs

**ATTENTION**
If a failure occurs at any time during this phase, refer to Performing the recovery procedure for HSL failure on page 1100.

**1** Allow the system to soak for one hour.

**2** Check the logs for the system. Click **Fault>Logs** on the main menu to open the **Logs** window.

**3** Check the alarms for the system. To view alarms, click the alarm banner. The **Alarms** window appears. Check for alarms.

## Recovery procedure for HSL failure

If an HSL fails during either phase, traffic is redistributed over the remaining links in the linkset or combined linkset. The following steps describe the HSL recovery procedure.

## Performing the recovery procedure for HSL failure

### *At the OAMP workstation*

1 Deactivate and offline the failed HSL. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.

2 Perform a remote Loopback at the far end of the link. Refer to the procedure “Remote Loopback” in the Fault Management section of the customer documentation. On the local end of the link, perform a BERT Operation. Refer to the procedure “Performing Bert” in the Security and Administration guide. Clear any faults before proceeding.

3 RTS the HSL. To RTS the link, refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.

4 Select one of the following options.:

| If: | Do: |
|---|---|
| The failure condition exists | Continue to step 6. |
| The failure condition clears | This procedure is complete. |

5 Provision LSLs. Refer to the procedure “Provisioning links” in the Operational Configuration section of the customer documentation.

6 RTS the LSLs. To RTS the link, refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.

7 Contact your next level of support.

# Upgrading the USP Compact

**ATTENTION**
The USP Compact load naming convention has changed in this release. It was previously referred to as USP Lite7.0 or USPL7.0. The new naming convention used throughout this document is USPc7.0. This also follows for the USPc9.0 release

**ATTENTION**
Installing this USP Compact software on a workstation other than your Nortel Networks-approved workstation may overwrite some system files used by other applications. This may cause failure of existing applications. Also, installing software other than Nortel Networks-approved applications on your USP Compact OAM&P workstation may invalidate the certification of the workstation, and may cause failure of the USP Compact application.

**ATTENTION**
When you upgrade your USP Compact software, existing data is preserved.

**ATTENTION**
This document details the upgrade procedure for a major upgrade only. To perform a point release upgrade, see the USPc Readme file. Contact your Nortel Networks representative for more information.

**ATTENTION**
The CLI is not available for use during an upgrade.

**ATTENTION**
The USP must be at the latest release of USPc7.0.x before upgrading to the current load. This ensures that all fixes related to upgrade are in place and tested.

**ATTENTION**
Auto-negotiate capability is supported for the CS LAN and can be enabled during the upgrade.

## Supported upgrade paths

Nortel Networks supports the following upgrade paths for USPc7.0:

- USPc7.0.x to USPc9.0.x

## Estimated upgrade times

The following table provides upgrade time estimates for the various cards in the system.

| Card type | Upgrade time (minutes) | Soak time (minutes) | Total (minutes) |
|---|---|---|---|
| USPc0 | 15 | 15 | 30 |
| USPc1 | 15 | 15 | 30 |

***Note:*** Nortel also requires you to perform test calls after you have upgraded one of the two USPc cards using the newly upgraded links. This could increase the time to upgrade the USPc.

**ATTENTION**
If your network requires cutover from Core Bounce to Direct Messaging, see your solution level customer documentation for the step-by-step procedure.

**ATTENTION**
You must have administrative privileges to perform a software upgrade.

# Analyze upgrade impacts

Avoid making changes to your system configuration and performing provisioning and maintenance activities during the software upgrade procedure. The system prohibits these activities. The software upgrade procedure impacts system capacity, system performance, and the OAMP workstations. Before beginning the upgrade, consider the actions described in the following section.

## System limitations during upgrade

During a software upgrade, the system prohibits the following actions, listed by subsystem:

- System Administration
  - adding, deleting, or modifying users
  - setting the time of day
  - changing passwords
- System Management
  - modifying the system name or shelf names
  - adding or deleting system nodes
  - modifying the IP address or the PEC of the USPc cards
- SS7 Management (MTP Level 3)
  - adding, deleting, or modifying a system identity
  - adding, deleting, or modifying a capability code
  - adding, deleting, or modifying links, linksets, linkset groups, combined linksets, or routesets
  - adding, deleting, or modifying ASP, AS, ASP Paths, AS destinations, or AS assignments
- SS7 Management (MSU Trace Screening)
  - deleting MSU Trace criteria file
- IPS7 Management
  - adding, deleting, or modifying application server process
  - adding, deleting, or modifying application server process path
  - adding, deleting, or modifying application server
  - adding, deleting, or modifying application server destination
  - adding, deleting, or modifying application server assignment

### System performance

The software upgrade procedure can impact USP system performance in the following ways:

- An upgrade database conversion is necessary due to internal USP data format changes. This affects the inactive USPc card (card on the right in the shelf).
- Depending on the scope of data format changes, the inactive USPc card takes approximately 15 minutes to load and convert internal data to the new format. During this time, the inactive USPc card is not enabled and the system operates with a single USPc card.
- The network capacity is reduced during software upgrade. This results from taking down one of the USPc cards which takes down approximately half of the SS7 signaling links. Therefore, you must perform software upgrade procedures during maintenance periods.

### System capacity

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAM&P workstation and the SAM21 disk complex are required for converting existing databases. The pre-checking procedure checks for adequate disk space on the disk complex. A message box informs you if your disk space is too low. If disk space is too low, delete any old snapshots. Once the update is complete, the additional disk space is no longer required and is made available for use.

### Tools and utilities

This upgrade procedure requires the following user supplied tools:

- FTP client application

### OAMP workstation functionality

The GUI allows multiple sites to be configured on an OAMP workstation at one time. Since the sites are not upgraded at the same time, the following conditions apply:

- There is a separate GUI for performing the upgrade to USPc9.0 called the ‘upgrade GUI’. When the upgrade is complete, the upgrade GUI is exited and the new USPc9.0 Java GUI is used from then on. This is required because the GUI has changed technologies between USPc7.0 and USPc9.0.
- The upgrade GUI can only be used to access existing USP capabilities. You cannot access the new capabilities until the new USPc9.0 GUI is running and the USPc is fully upgraded to USPc9.0.
- The upgrade GUI allows you to log in to a USPc7.0 system with or without an upgrade in progress.

- You cannot use a previous version of the GUI to log into a newer version of the USP software.
- Only one version of the USPc7.0 or upgrade GUI can be installed at a time, because the GUI upgrade requires the conversion of local files. You can have the upgrade GUI and the new USPc9.0 GUI installed at the same time (but only one running at a time).

## Software upgrade preparation

Complete the following procedure before you install the upgrade GUI and begin a software upgrade.

Before beginning upgrade procedures, complete this check from your GUI workstation to make sure your system is running in a predictable, stable manner. To perform the pre-upgrade check, perform the following steps:

### Performing a pre-upgrade check

***At the OAMP workstation***

1 Record the list of site names and their RTC IP addresses.

   **a** Open the USPc7.0 GUI (double-click the desktop icon)

   **b** Click **Configure**.

   **c** Record the list of site names and their RTC IP addresses.

   This information will be entered into the new USPc9.0 Java GUI.

2 Log in to the USP.

3 Make sure that both USPc cards are in-service. To do this, click System Mgmt on the main menu and click the shelf icon. The Shelf_name window appears. Verify that the LED icons for each in-service system node are green.

4 Take corrective action to clear all outstanding alarms.

5 Virtual linksets are not supported on the USP Compact. Verify that there are no virtual linksets provisioned on the system. To do this, perform the following check:

   **a** Click **Network Management**, then **MTP** and then **Linkset**.

   **b** Scan the “Linkset Records” portion at the bottom of the screen watching the “Virtual Linkset” column.

   **c** All of the linksets should have this field set to false.

   **d** If any of the linksets are setup as virtual linksets, these must be removed prior to starting the upgrade.

6 Take a snapshot of the current running configuration.

a Click the **Administration** button.

b Click the **Backup** button.

c Enter a description of the backup and click the **Backup** button.

7 Perform test calls and verify the calls complete successfully.

8 Ensure that the left USPc card (as seen on the **System Configuration** screen of the GUI) is the Master. If not, perform a SWACT. Wait 10 minutes before proceeding. Monitor logs and OMs during the 10-minute period.

## Upgrading the USP Compact GUI

This section contains the following GUI installation procedures:

- Uninstalling the USPc7.0 GUI
- Installing the USPc9.0 upgrade GUI
- Installing the new Java GUI for USPc9.0

### Uninstalling the USPc7.0 GUI



**CAUTION**

Before beginning this procedure, you should close all open applications.

***At the USP Compact OAMP workstation***

1 Click the Window's **Start** button on your desktop.

2 On the **Settings** menu, click **Control Panel**.

3 In the **Control Panel** window, double-click **Add/Remove** Programs.

4 In the **Install/Uninstall** tab window of the **Add/Remove Programs Properties** window, select Universal Signaling Point Compact from the alphabetical list of programs.

5 Click the **Add/Remove** button. A popup window asks if you are sure you want to completely remove the USP and all of its components.

6 Click **Yes**.

7 If a popup window asks if you want to remove shared files, click **Yes to All**.

8 Click **Yes** to confirm your choice. All of the files are removed.

9 Restart your computer.

### Installing the USPc9.0 upgrade GUI



**CAUTION**

Installing this software on a workstation other than a Nortel Networks-recommended workstation may overwrite some system files used by other applications. Installing software other than Nortel Networks-specified applications on your USP Compact OAM&P workstation may cause failure of the USP Compact application.



**CAUTION**

If you are upgrading your system, uninstall the previous USP Compact version according to the previous section before proceeding with this section.



**CAUTION**

The GUI may not function properly with non-ASCII based character sets. Please ensure the OAMP workstation is set to either English or German language character sets.

**ATTENTION**

The upgrade GUI is used to take you through upgrade only. When new features are activated in a later procedure, this GUI will exit and you will need to switch to using the standard USPc9.0 GUI.

#### *At the OAMP workstation*

1 Close any open applications.

2 Insert the USP Compact Software CD-ROM disk into the CD-ROM drive.

3 Double-click the **My Computer** icon on your desktop.

4 Double-click the CD-ROM disk icon.

5 Double-click the upgrade-gui folder.

6 Double-click Setup.exe. A popup dialog box appears with the warning that installing this software on a workstation other than a Nortel Networks-approved workstation may overwrite some system files used by other applications. If this is a Nortel Networks-approved workstation, or you want to proceed regardless of the warning, click **Yes** to continue.

7 At the Welcome window for the USP Compact setup program, click **Next**.

8 Select the package(s) that you want to install on this workstation.

- Select USPc GUI Client if you want this workstation to be able to log into the USP Compact site.
- Select Acrobat Reader if you do not have a version of Adobe Acrobat Reader installed on this workstation.

***Note:*** Adobe Acrobat Reader is required to view the documentation.

| If you select: | Do: |
|---|---|
| the GUI package | step 9. |
| Acrobat Reader | step 10 to step 16. |

9 A popup dialog box prompts you for the location where you want to install the USP package. Select an installation directory for the program and click **Next**. The Copying Program Files window appears with a status bar to show progress in copied files. Skip to step 18.

10 A Welcome window for the Adobe Acrobat Reader Setup Program appears.

11 Click **Next**. The Acrobat Reader License Agreement appears.

12 Click **Yes** to accept the terms of the agreement. The Acrobat Reader Destination Location window appears.

13 Click **Next**.

Note: Do not modify the destination path for Acrobat Reader.

14 If you want to view the Readme file for Adobe Acrobat Reader, click on the radio button next to Display Acrobat Reader 3.01 Readme file. Click **OK**.

15 The Readme file appears. After reading the Readme file, Click **Close**.

16 The Acrobat Reader Setup Complete window appears. Click **OK**.

17 Click the radio button next to Yes, I want to restart my computer now.

18 Click Finish. The computer restarts.

19 Remove the USP Compact Software CD-ROM disk from the drive using the eject cdrom command. The installation of the upgrade GUI is complete. Keep the USP Software CD-ROM disk handy to your system hardware.

20 Log in to the USP Compact from the USP Compact upgrade GUI and monitor the OAMP workstation for 10 minutes while logged in to the USP Compact. Check logs during this time. Your USP Compact upgrade GUI is now installed. You will use the GUI to upgrade your USP Compact software. The USPc9.0.x upgrade GUI should not be used for provisioning, it's purpose is for upgrade only.

### Installing the new Java GUI for USPc9.0



**CAUTION**

Installing this USP Compact software on a workstation other than your Nortel Networks-recommended workstation may overwrite some system files used by other applications. This may cause failure of existing applications. Also, installing software other than Nortel Networks-specified applications on your USP Compact OAM&P workstation may cause failure of the USP Compact application.



**CAUTION**

The GUI may not function properly with non-ASCII based character sets. Please ensure the OAMP workstation is set to either English or German language character sets.



**CAUTION**

The GUI may not function properly with non-ASCII based character sets. Please ensure the OAMP workstation is set to either English or German language character sets.

**ATTENTION**

The upgrade GUI is used to take you through upgrade only. When new features are activated in a later procedure the upgrade GUI will exit and you will need to switch to using the standard GUI.

***At the OAMP workstation***

1 Close any open applications.

2 Insert the USP Software CD-ROM disk into the CD-ROM drive.

3 Double-click the **My Computer** icon on your desktop.

4 Double-click the CD-ROM disk icon.

5 Double-click **install.exe**. A popup dialog box appears indicating that it is preparing to install. This is followed by a splash screen.

6 At the Introduction window for the USP Compact setup program, click **Next**.

**7** Select the package(s) that you want to install on this workstation.

- Select USPc Graphical Interface Client if you want this workstation to be able to log into the USPc site.
- Select USPc User Manuals and Documentation Suite to install the complete collection of FCAPS documents and Interface Specifications.
- Select Adobe Acrobat PDF Reader Version 5.1 if you do not have a version of Adobe Acrobat Reader installed on this workstation.

| If you select: | Do: |
|---|---|
| the GUI package | step 8 |
| Acrobat Reader | step 9 to step 15 |

**8** Select an Installation Directory and click **Install**. Skip to step 15.

**9** Select an Installation Directory and click **Install**.

**10** If you chose to install Acrobat reader, a Welcome window for the Adobe Acrobat Reader Setup Program appears. Adobe Acrobat Reader is required to view the Solution information. If Adobe Acrobat Reader is already installed on this workstation, click **No**.

Click **Yes** to the “Are you sure” message. If you do not want to install Adobe Acrobat Reader, skip to step 15.

**11** Click **Next**. The Acrobat Reader Destination Location window appears.

**12** Click **Next**.

***Note:*** Do not modify the destination path for Acrobat Reader.

**13** The Acrobat Reader Setup Complete window appears. Click **OK**.

**14** Click **Finish**.

**15** The installation screen will indicate that installation was successful. Click **Done**.

**16** Remove the USP Software CD-ROM disk from the drive using the eject cdrom command. The installation of the standard GUI is complete. Keep the USP Software CD-ROM disk handy to your system hardware.

**17** Your new USPc9.0 Java GUI is now installed. You will use the GUI once you have activated new features in Procedure 9. This GUI will not work with the USP prior to the activation of new features.

# Upgrade the USP Compact cards

This section contains the following software upgrade procedures for the USP Compact:


- Transferring software to the NFS Server
- Transferring the upgrade package to the NSF Server for the USP Compact master card
- Running the upgrade pre-check utility and starting the upgrade
- Upgrading the slave USP Compact card
- Upgrading the master USP Compact card
- Activating new features and cleaning up
- Completing the post-upgrade checklist


### Transferring software to the NFS Server

***At the USP Compact OAMP workstation***

**1** Locate these files on your upgrade media (i.e. Program\ntssgusp\loads):

- uspc_09_00_XX_XXX
- uspc_09_00_XX_XXX_base
- uspc_09_00_XX_XXX_t1e1ha

***Note:*** XXX is a build version, for example,

uspc_09_00_00_04E

**2** Use an FTP client to transfer these files to both of the NFS server cards. The destination directory is:

/nfsserv/usp/sd0/loads/

**3** Telnet to the both NFS server cards, and ensure that the samss7 user has read permission for the load files.

### Transferring the upgrade package to the NSF Server for the USP Compact master card

***At the USP Compact OAMP workstation***

**1** Locate the upgrade package in the USP Compact zip file:

upgrade_pkg.tar.gz

**2** Telnet to the NFS server for the Master card and determine which directory the USP Compact is using for its database. View the /nfsserv/usp/sd0/sysconf file and search for the data_dir variable. An example data dir would look like:

data_dir = stp/data/.curr1

3 Using an FTP client transfer this file to the following directory on the Master USP Compact card NFS server:

/nfsserv/usp/sd0/stp/data/<data_dir>/

4 Execute the following commands on the NFS server:

cd /nfsserv/usp/sd0/<data_dir>/

gunzip upgrade_pkg.tar.gz

tar -xvpf upgrade_pkg.tar

chmod -R 777 upgrade_pkg

**Running the upgrade pre-check utility and starting the upgrade**

***At the USP Compact OAMP workstation***

1 Click on the **Administration** button on the main menu. Then click **Upgrade** and **Prechecking**.

2 Click on the **Administration** button on the main menu. Then click **Upgrade** and select **Start**. Click **Apply**.

3 Clear any error conditions the system identifies before you proceed to the next procedure.

**Upgrading the slave USP Compact card**

***At the USP Compact OAMP workstation***

1 Inhibit all of the links on the slave USP Compact card.

***Note:*** If there is only one available link on a linkset, you will not be able to inhibit it. If it is a one-link linkset, proceed to step 3 without inhibiting the link. If there are other links on the linkset, make at least one of them available before attempting to inhibit the link.

2 Deactivate all of the links on the slave USP Compact card.

3 Deactivate all of the paths on the slave USP Compact card.

4 Lock the slave USP Compact card on the USP Compact upgrade GUI. To do this, click on the **System Mgmt** button on the main menu and click on the card, then click on **Lock**.

***At the SAM21 Element Manager***

5 Lock the slave USP Compact card. This will disable the card on the USP Compact upgrade GUI.

6 Change the load name of the slave USP Compact card to the new boot ROM load name. The boot ROM load is the load that does not have a load type suffix (i.e. “_base” or “_t1e1ha”). It is located in the following directory:

/nfsserv/usp/sd0/loads/

7 Unlock the slave USP Compact card. The USP Compact card will start booting

***At the USP Compact OAMP workstation***

8 Unlock the USP Compact card. To do this, click on the **System Mgmt** button on the main menu and click on the card, then click on **Unlock**.

***Note:*** The system raises logs and alarms when the loads and images on the USP Compact cards do not match.

9 Verify the USP Compact 09 version is running. If not, double-check that the correct image is selected on the SAM 21 Element Manager. If the right image is selected but the incorrect load is running, stop the upgrade procedures and contact Nortel Networks technical support.

10 Activate all of the paths on the slave USP Compact card.

11 Activate all of the links on the slave USP Compact card.

12 Uninhibit any links you inhibited at the start of this procedure.

13 Monitor the USP Compact for 15 minutes to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. During this period, perform test calls to verify newly loaded USP Compact card performs. Take steps to make sure test calls are routed through links on this USP Compact card.

## Upgrading the master USP Compact card



**CAUTION**

Upgrade of the Master USP Compact card cannot be aborted unless a Complete Office Recovery is performed. This abort action causes an interruption in service.

***At the USP Compact OAMP workstation***

1 Perform a SWACT so that the master USP Compact card becomes the slave.

2 Inhibit all of the links on the new slave USP Compact card.

***Note:*** If there is only one available link on a linkset, you will not be able to inhibit it. If there are other links on the linkset, make at least one of them available before attempting to inhibit the link. If it is a one-link linkset, proceed to step 4 without inhibiting the link.

3 Deactivate all of the links on the slave USP Compact card.

4 Deactivate all of the paths on the slave USP Compact card.

5 Lock the slave USP Compact card. To do this, click on the **System Mgmt** button on the main menu and click on the card, then click on **Lock**.

***At the SAM21 Element Manager***

6 Lock the slave USP Compact card. This will disable the card on the USP Compact upgrade GUI.

7 Change the load name of the slave USP Compact card to the new boot rom load name. The boot rom load is the load that does not have a load type suffix (i.e. "_base" or "_t1e1ha"). It is located in the following directory:

/nfsserv/usp/sd0/loads/

8 Unlock the slave USP Compact card. The USP Compact card will start booting.

***At the USP Compact OAMP workstation***

9 Unlock the USP Compact card. To do this, click on the **System Mgmt** button on the main menu and click on the card, then click on **Unlock**.

***Note:*** The system raises logs and alarms when the loads and images on the USP Compact cards do not match.

10 Verify the USP Compact 09 version is running. If not, double-check that the correct image is selected on the SAM 21 Element Manager. If the right image is selected but the incorrect load is running, stop the upgrade procedures and contact Nortel Networks technical support.

11 Activate all of the paths on the slave USP Compact card.

12 Activate all of the links on the slave USP Compact card.

13 Uninhibit any links you inhibited at the start of this procedure.

14 Monitor the USP for 15 minutes to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. During this period, perform test calls to verify newly loaded USP

Compact card performs. Take steps to make sure test calls are routed through links on this USP Compact card.

**15** Wait 10 minutes and then perform a SWACT.

### Activating new features and cleaning up

#### *At the OAM&P workstation*

**1** Open the Upgrade Administration window to activate the upgrade features. To do this, click **Administration** on the main menu and click **Upgrade** on the Software Upgrade Menu window.

**2** Click **Activate New features** in the Upgrade Options section.

**3** Click **Apply**.

**4** At this time, all upgrade GUIs will be disconnected and can no longer connect to the USP Compact. You will need to launch the standard GUI to monitor the USP Compact from this point on. On your desktop, double-click the USPc GUI shortcut to launch the standard GUI.

**5** When you first launch the standard GUI you will be presented with the site-manager screen. To set up your site in the new GUI, enter your site name and RTC IP addresses obtained in the pre-upgrade procedure and click OK. When you complete this setup, you can log in with the new GUI.

**6** Perform test calls to verify that messages are correctly routed. Monitor the USP to ensure it does not report any LOG_SWERRs or LOG_TRAPs.

**7** Monitor the USP Compact for 15 minutes. Ensure that the USP Compact performs without degradation.

### Completing the post-upgrade checklist



**CAUTION**

Wait 24 hours after completing all of the upgrade procedures before beginning this procedure.



**CAUTION**

Make sure that the current software load files are not deleted.

***At the USP Compact OAMP workstation***

1 Begin a new log time period to end the upgrade log tracking time period. To do this, click the **Logs** button on the main menu and click the **Start New Log Period** button.

2 Telnet to one of the NFS servers.

3 Remove the following files corresponding to the previous software version:

- /nfsserv/usp/sd0/loads/uspl_07_00_XX_XXX
- /nfsserv/usp/sd0/loads/uspl_07_00_XX_XXX_base
- /nfsserv/usp/sd0/loads/uspl_07_00_XX_XXX_t1e1ha

***Note:*** XXX is a build version, for example, uspl_07_00_00_04E

4 Repeat step 3 on the other NFS server.

## Abort a software upgrade

This section contains the following software downgrade procedures for the USP Compact:

- Downgrading both USP Compact cards
- Downgrading a single USP Compact card

### Downgrading both USP Compact cards

**ATTENTION**
Perform this procedures if an upgrade has been completed (for example, both USPc cards) and it is necessary to abort the upgrade.



**CAUTION**

Downgrading both USP Compact cards requires a valid USP Compact 7.0 snapshot.



**CAUTION**

A Complete Office Recovery is required to downgrade both USP Compact cards. This action will cause an interruption in service.

***At the USP Compact OAMP workstation***

**1** Deactivate all links on both USP Compact cards.

**2** Deactivate all paths on both USP Compact cards.

**3** Make the desired USP Compact 7.0 snapshot the active snapshot for both cards.

If you have not activated the new features in a previous step and are using the upgrade GUI, perform the following steps:

- Click **System Mgmt**. Click on the left card and then click **Edit**.
- Click on the button beside the Boot Data Snapshot field and select the desired snapshot.
- Click **Apply** to save the changes.
- Repeat this procedure for the right card.
- Log out of the USP Compact upgrade GUI.

If you have activated new features in a previous step and are using the standard GUI, perform the following steps:

- Select **Configuration>platform>node**.
- Double-click on the left card and select the snapshot from the drop-down list beside the boot-snapshot field.
- Click **Apply** to save the changes.
- Repeat this procedure for the right card.
- Log out of the USP Compact standard GUI.

***At the SAM21 Element Manager***

**4** Lock both USP Compact cards on the SAM21 element manager.

**5** Change the load name of both USP Compact cards to the USP Compact 7.0 boot ROM load name. The boot ROM load is the load that does not have a load type suffix (i.e. “_base” or “_t1e1ha”). It is located in the following directory:

/nfsserv/usp/sd0/loads/

6 Unlock the left (as seen on the USP GUI's System Configuration screen) USP Compact card.

***At the USP Compact OAMP workstation***

7 Log in with the USP upgrade GUI.

8 Verify that the USP Compact is running the correct snapshot and load. To see the snapshot information, click on **System Mgmt**, then click on the left card.

9 Unlock the other USP Compact card and wait for it to complete booting and verify that it is also running the correct snapshot and load.

10 Uninstall the USP Compact 9.0 version of the USP upgrade GUI.

11 Uninstall the USP Compact 9.0 version of the new USP Java GUI.

12 Install the USP Compact 7.0 version of the USP GUI.

If only one card has been upgraded to USPc9.0, then perform the following steps to downgrade the USP Compact to USP Compact7.0.

**Downgrading a single USP Compact card**

***At the USP Compact OAMP workstation***

1 Ensure that the upgraded card is the slave. Perform a SWACT if it is not. This can be checked by clicking on **System Mgmt**, then clicking on the card.

2 Ensure that all links and paths on the master card are inservice.

3 Inhibit all of the links on the slave card.

***Note:*** If there is only one available link on a linkset, you will not be able to inhibit it. If there are other links on the linkset, make at least one of them available before attempting to inhibit the link. If it is a one-link linkset, proceed to step 4 without inhibiting the link.

4 Deactivate all of the links on the slave USP Compact card.

5 Deactivate all of the paths on the slave USP Compact card.

6 Lock the slave USP Compact card. To do this, click on the **System Mgmt** button on the main menu and click on the card, then click on **Lock**.

***At the SAM21 Element Manager***

**7** Lock the slave card. This will disable the card on the USP upgrade GUI.

**8** Change the load name of the slave card to the USP Compact 7.0 boot ROM load name. The boot ROM load is the load that does not have a load type suffix (i.e. "_base" or "_t1e1ha"). It is located in the following directory:

/nfsserv/usp/sd0/loads/

**9** Unlock the slave card.

***At the USP Compact OAMP workstation***

**10** Verify that the load running is the old version. If not, double-check that the correct image is selected on the SAM 21 Element Manager. If the right image is selected but the incorrect load is running, stop the upgrade procedures and contact Nortel Networks technical support.

***Note:*** The system raises logs and alarms if the loads and images on the USP Compact cards do not match.

**11** Stop the upgrade by clicking on **Administration**, then **Upgrade**, then select **Stop**, then click **Apply**.

**12** Lock and Unlock the slave card.

***At the USP Compact OAMP workstation***

**13** Unlock the slave card. To do this, click on the **System Mgmt** button on the main menu and click on the card, then click on **Unlock**.

**14** Activate all of the paths on the slave USP Compact card.

**15** Activate all of the links on the slave USP Compact card.

**16** Uninhibit any links you inhibited.

**17** Monitor the USP Compact for 15 minutes to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. During this period, perform test calls to verify that the newly loaded USP Compact card performs. Take steps to make sure test calls are routed through links on this USP Compact card.

**18** Uninstall the USP Compact 9.0 version of the USP upgrade GUI.

**19** Uninstall the USP Compact 9.0 version of the USP standard GUI.

**20** Install the USP Compact 7.0 version of the USP GUI.

# Upgrading the Enhanced Network and Message Switch

For details about upgrading the Enhanced Network (ENET) and Message Switch (MS), refer to the *Peripheral Module Release Document*, 297-9051-599 (intl) or 297-2663-599 (NA) in the DMS (SN07) Helmsman collection.

# Upgrading the CS 2000 core

Refer to the following documentation:

**For CS 2000-based solutions**

- *XA-Core Maintenance Manual*, 297-8991-510

*One Night Process Software Delivery Procedures*, 297-8991-303

**For CS 2000 - Compact based solutions**

- For the basic upgrade, refer to the Call Agent upgrade sections in this document. For full details, refer to *Upgrading the Call Agent*, NN10065-461

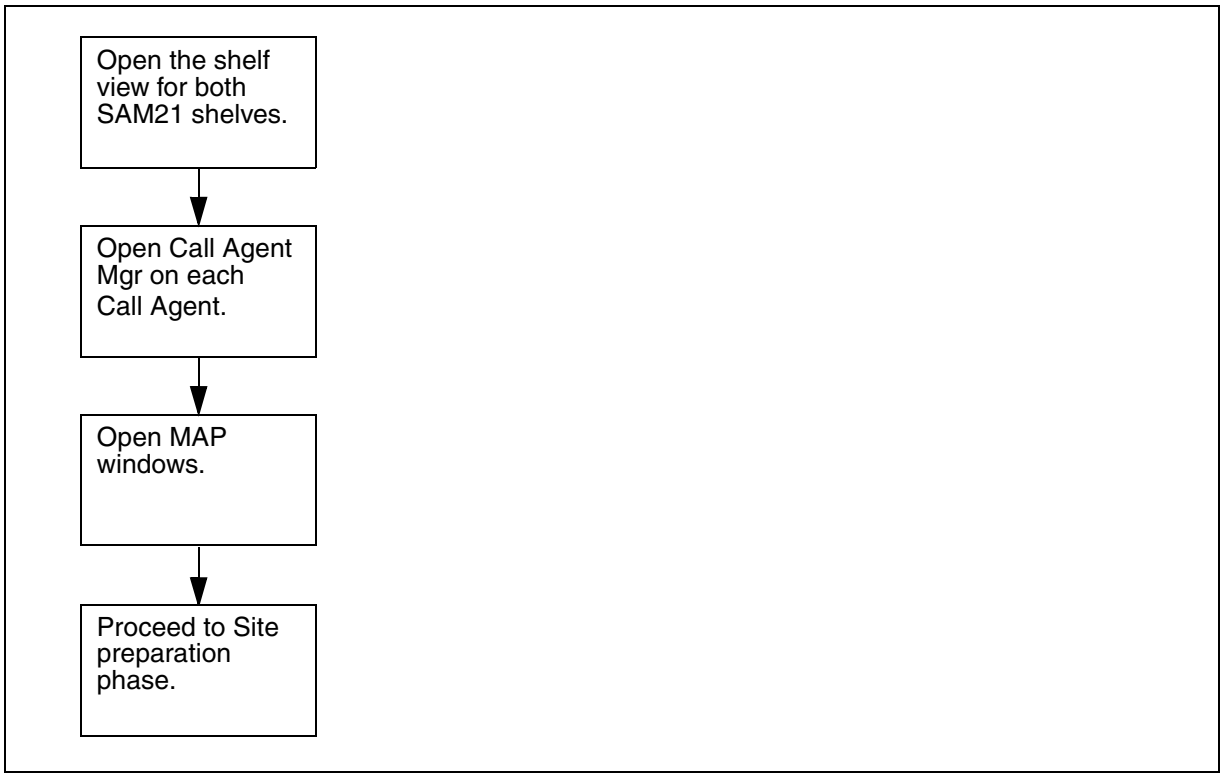
# Upgrading the CS 2000 Compact

Procedures in this section use the PassThru feature on the CS 2000 Core Manager or CBM. Refer to “Adding or removing PassThru users” in *CS 2000 Core Manager Security and Administration*, NN10170-611 or *Core Business Manager*, NN10358-611 for more information about the PassThru feature. For offices without a CS 2000 Core Manager or CBM, PassThru is not used, and direct connections to the call processing side of the CS LAN are needed.

If the PassThru usernames are not “core0usr,” “core1usr,” and “cmusr,” then substitute the office’s PassThru usernames for core0usr, core1usr, and cmusr in these procedures.

The procedures provide recommended methods for opening the interfaces required to complete an upgrade, as shown in the following figure.

**Figure 1 Interface setup**

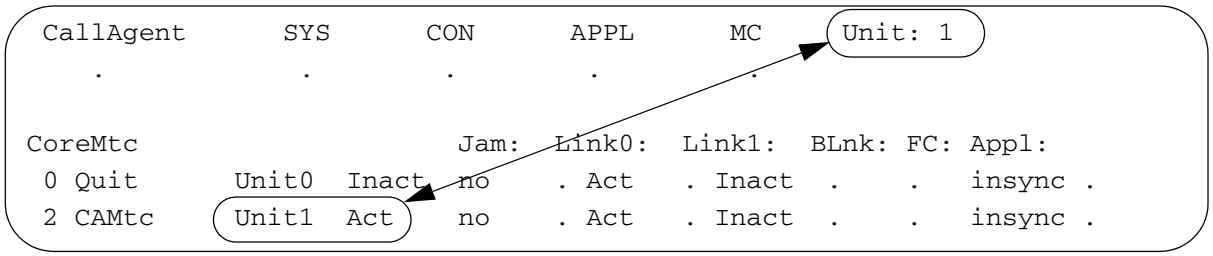


Each procedure indicates the interface used to perform the procedure or step. The following table describes the interfaces.

**Table 1 Interfaces used to perform procedures and steps**

| Interface type | Description |
|---|---|
| **ACTIVECM** | a MAP window connected to the active side session of the call processing application |
| INACTIVECM | a MAP window connected to the inactive side session of the call processing application. Actions performed at this interface are also indicated by the command prompt **`Mate>`** |
| CORE0 | a Call Agent Manager window connected to the Call Agent card identified as core0 and provides a maintenance interface. The maintenance interface is started from the **ccamtc** command. In SN05, the command was tpcmtc |
| CORE1 | a Call Agent Manager window connected to the Call Agent card identified as core1 and provides a maintenance interface. The maintenance interface is started from the **ccamtc** command. In SN05, the command was tpcmt |
| Active maintenance window (CORE0 or CORE1) | the CORE0 or CORE1 window that is connected to the active Call Agent. CORE1 is the active maintenance window for figure SN06 and newer Call Agent Manager with Message Controllers in the office on page 1124. |
| SDM | a window connected to the CS 2000 Core Manager. The **sdmmtc** program and UNIX system activities are completed from this window |

**Figure 2 SN06 and newer Call Agent Manager with Message Controllers in the office**



The following procedure indicates how to create a shell script that changes the title of an xterm window. This procedure only works on UNIX workstations.

***At an xterm window on the CS 2000 SAM21 Mgr client workstation***

**1** Use an editor to create the following file. Available editors are vi and dtpad. Save the file with a name of “xtermtitle”.

```
#!/bin/sh
# this script changes the title of an xterm
echo “\033]2;$1\007”
echo “\033]1;$1\007”
```

**2** Make the file executable.

```
UNIX> chmod +x xtermtitle
```

**3** To use the script, enter the command and the new name for the window.

```
UNIX> ./xtermtitle <window_title>
```

**window_title**
is a string like core0, core1, sam21gui, activecm, or inactivecm

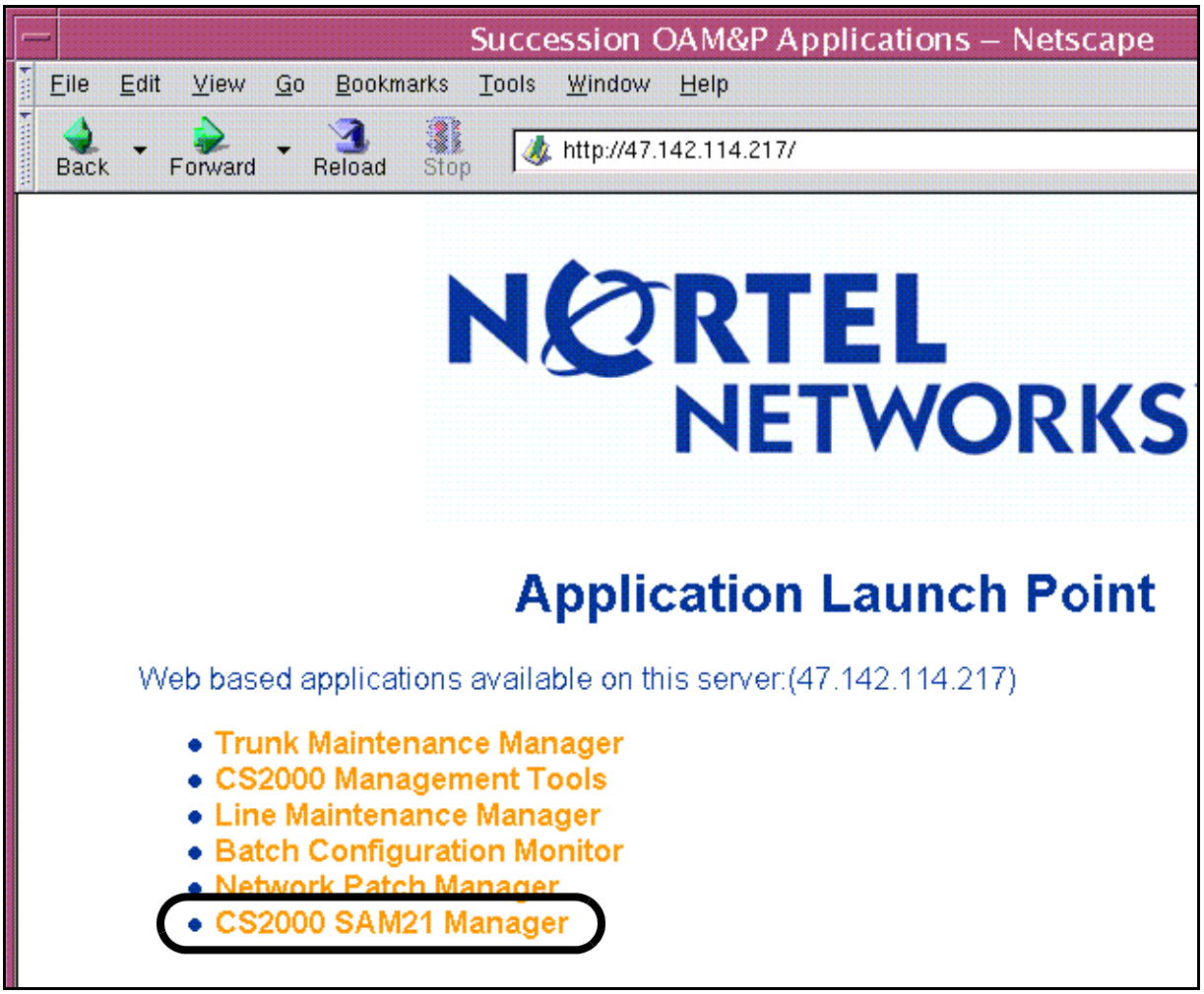
**4** This procedure is complete.

For Microsoft Windows 2000 based workstations, change the title of a command prompt window with the **title <window_name>** command.

# Open SAM21 shelf views

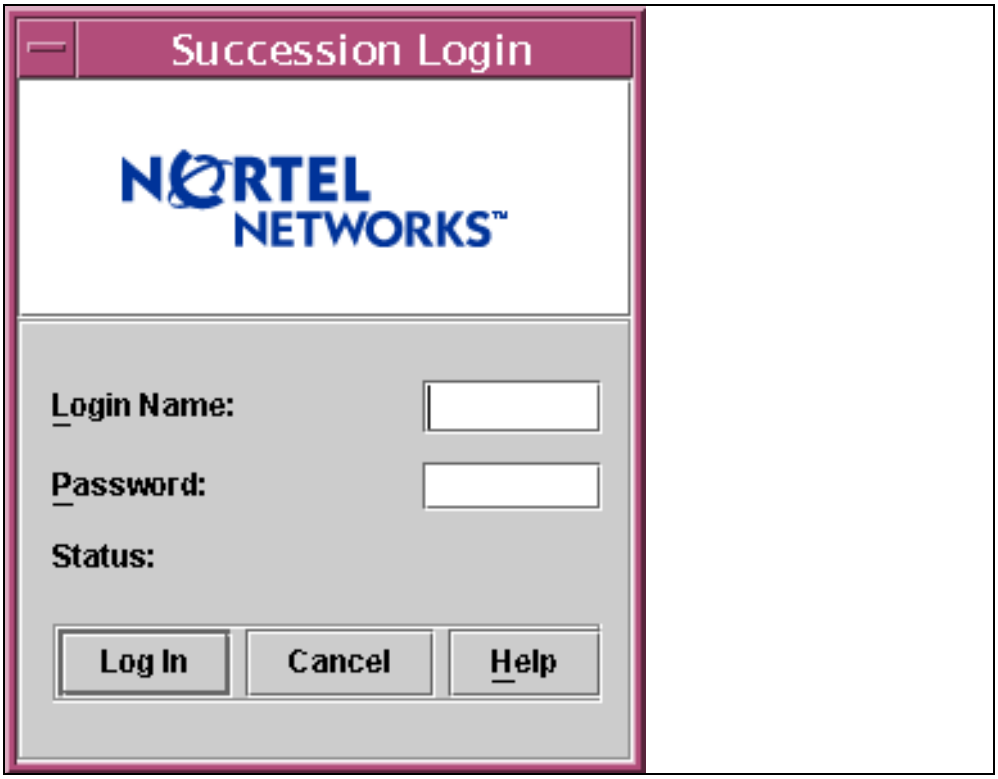
***At your workstation***

1 Open a web browser and enter the IP address or hostname of the host that provides the CS 2000 Management Tools. Click on the link for the CS 2000 SAM21 Manager.




*A login window appears.*

2 Provide the login name and password and then click Log In.




***Note:*** The login account must have mgcrw or mgcadm level permissions.

*The application starts and the Subnet View window opens.*

3 Open both Shelf View windows by double-clicking on the shelf icons from the Subnet View window.

4 Position the screens so that alarms and access to locking and unlocking cards are available.

5 This procedure is complete.

# Open a window to the CS 2000 Core Manager

***At the CS 2000 SAM21 Manager client workstation***

**1** Open an xterm window and change the title to “SDM”.

***At the SDM window***

**2** Telnet to the CS 2000 Core Manager and log in.

Log in as a user with privilege to apply filesets, read tapes from the tape device, and transfer files with FTP.

**3** This procedure is complete.

# Open Call Agent Mgr windows

The procedure requires that the PassThru feature and usernames are configured on the CS 2000 Core Manager or CBM. For this procedure and the remainder of the upgrade, the documented usernames are core0usr, core1usr, and cmusr. If the office has different PassThru usernames provisioned, substitute the different usernames. Offices that do not have a CS 2000 Core Manager or CBM require two connections, one to each Call Agent card, but will telnet directly to each Call Agent card.

***At your workstation***

**1** Open two terminal windows and change the title for one window to “CORE0” and the other window to “CORE1”.

***SDE — At the CORE0 window***

**2** Telnet to the CS 2000 Core Manager or CBM and log in as user “core0usr”.

*The CS 2000 Core Manager or CBM forwards the telnet session to the core0 Call Agent card.*

**3** Log in to the core0 Call Agent card.

***SDE — At the CORE1 window***

**4** Telnet to the CS 2000 Core Manager or CBM and log in as user “core1usr”.

*The CS 2000 Core Manager or CBM forwards the telnet session to the core1 Call Agent card.*

**5** Log in to the core1 Call Agent card.

***SDE — At the CORE0 and CORE1 windows***

**6** Start the maintenance interface.

```
[mtc@core0_ip_address mtc]$ ccamtc
[mtc@core1_ip_address mtc]$ ccamtc
```

**7** This procedure is complete.

# Open MAP windows

If the office does not have a CS 2000 Core Manager or CBM, create two telnet connections to the IP address of the call processing application instead of following this procedure. The IP address of the call processing application is the “activeirm” address reported by the **QueryIP** command at the Call Agent Manager interface.

***At your workstation***

**1** Open two terminal windows and change the title of one to “ACTIVECM” and the other to “INACTIVECM”.

***SDE — At the ACTIVECM window***

**2** Telnet to the CS 20000 Core Manager or CBM and log in as user “cmusr.”

*The CS 2000 Core Manager or CBM forwards the telnet session to the call processing application.*

**3** Log in to the call processing application.

***SDE — At the INACTIVECM window***

**4** Repeat steps 2 and 3.

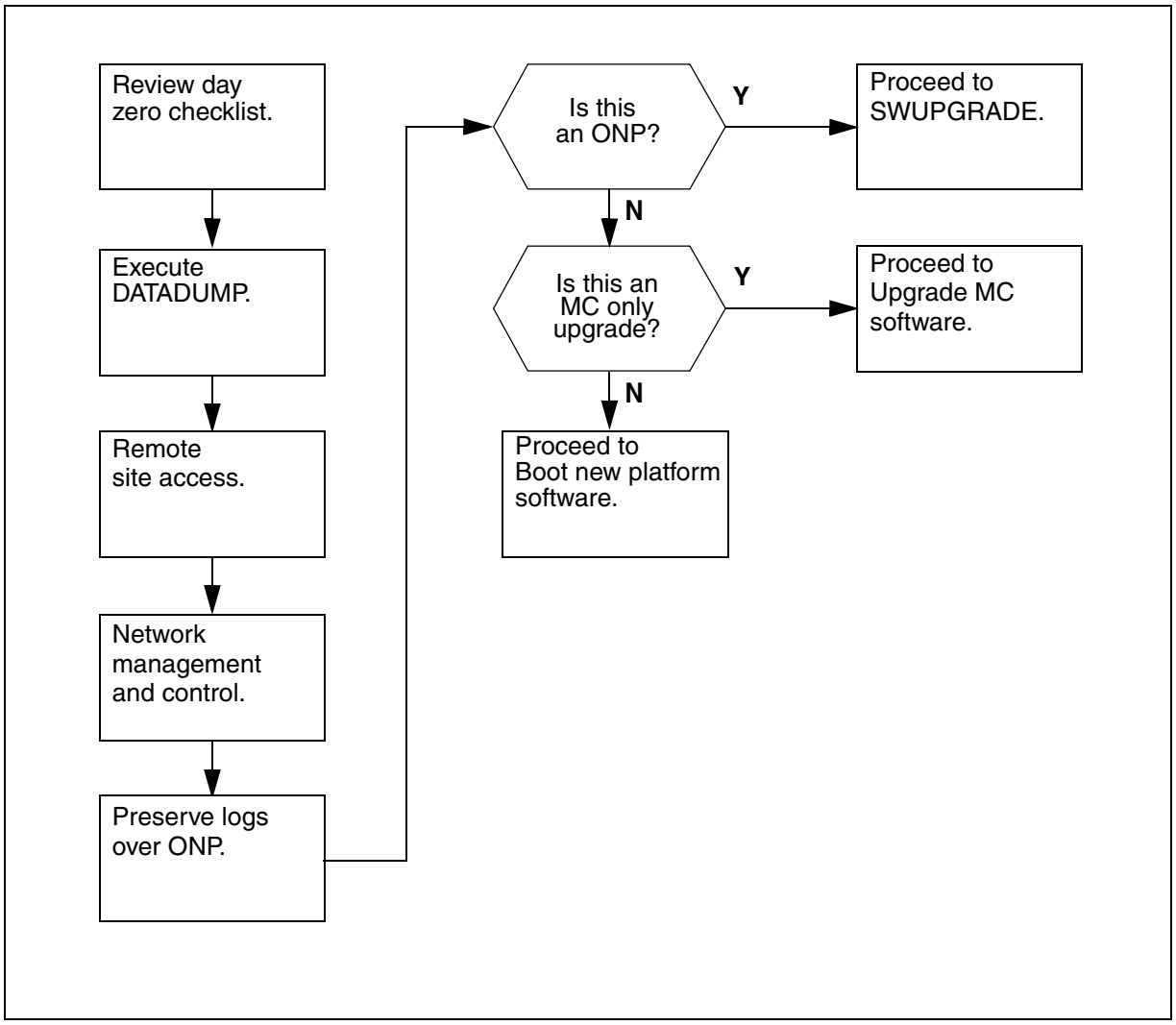
**5** This procedure is complete.

***Note:*** The INACTIVECM window does not connect to the inactive call processing application at this time. Later steps indicate when and how to connect to the inactive call processing application, when necessary.

# Site responsibilities the day of the software delivery

Complete this section on the day of the ONP. Site personnel should have the following procedures completed before the Software Delivery Applicator contacts the site to begin the scheduled ONP.

**Site responsibilities the day of the software delivery**



## Day zero checklist

***SITE — At the ACTIVECM window***

1 Verify that all pre-application activities are complete. This includes the Site preparation overview on page 370, Perform TABAUDIT on page 408, and Restore call processing application files on page 395.

2 Verify the ONP start time. Either Nortel Networks and/or the operating company established this start time during the site preparation phase. To verify this time, refer to the software delivery site-ready reports or contact your next level of support. If requesting a change to the start time contact your Nortel Networks regional customer representative.

3 Verify front-end stability by ensuring the last REx test passed.

4 Take an office IMAGE and back it up. Refer to Dump call processing application image on page 419. Store the copy of the office IMAGE for at least 30 days following the ONP.

5 Ensure you have defined and tested the Test Call Scripts. The test call plan must be ready before activation of the new software load.

6 Patches and process files downloaded for the ONP must remain where they are. Do not erase these files.

7 Check for a SOC file “<clli>_SCF” or “<clli>$SCF” in SFDEV (or download device). If a SOC file is present, copy the file to a disk drive.

***Note:*** For information on installing the RTU (right-to-use) SOC password file, refer to the *Software Optionality Control User’s Manual*, 297-8991-900.

8 Verify that SFDEV is clear of unnecessary files. (This is to clear Store File Device space for ONP work.)

9 Ensure that no peripheral hardware or software changes, including retrofits, extensions, or maintenance activities, are scheduled to take place during the ONP. Any affected hardware must be made INB (installation busy), in both the host and remote offices.

***Note:*** Recently removed hardware must have all associated software removed as well. Peripheral hardware that is not in the in-service or offline state may jeopardize the ONP.

**10** For offices equipped with a CS 2000 Core Manager or Core and Billing Manager (CBM), ensure the SuperNode Billing Application (SBA) is not undergoing backup or recovery. The SBA system must be operating in normal mode during the ONP. If necessary, refer to *CS 2000 Core Manager Fault Management*, NN10082-911 or *Core and Billing Manager 850 Fault Management*, NN10351-911for alarm clearing procedures.

**11** Set up user interfaces and ensure they are available.

**12** This procedure is complete.

# Execute DATADUMP

**ATTENTION**
Allow sufficient time to run the DATADUMP. Depending on the office, DATADUMP can require eight hours or more. Failure to allow sufficient time may impact the application start time.

***SITE — At the MAP***

**1** Record the datadump on disk or in the storefile device (SFDEV):

```
> RECORD START ONTO <device>
```

**device**
is a disk device such as SD00TEMP or is the storefile device, SFDEV

***Note:*** The name of the created file is RECORDFILE.

**2** Execute the DATADUMP:

```
> BCSUPDATE;DATADUMP
```

*Several confirmation prompts are presented. Confirm each prompt with "yes."*

```
Data Dump for CO: OFC_CLLI              Date: MAY 11, 2004  13:36:34
=============================================================================
Do you want to display INB, MB and RES trunks?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display 1MR registers?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display INB lines?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display tables?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display hardware?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
```

*The datadump runs and completes.*

3 When the DATADUMP completes, quit to the CI level:

```
> QUIT ALL
```

4 Stop the recording:

```
>RECORD STOP ONTO <device>
```

5 This procedure is complete.

## Remote site access

At the established ONP start time, the telephone operating company is responsible for providing remote site access to the Nortel Networks Applicator. If not provided to Nortel Networks in advance, be prepared to furnish all the necessary information for this task.

***SITE***

**1** Ensure there will be uninterrupted communication with the Applicator during the ONP. Nortel Networks recommends using Foreign Exchange (FX) voice and data lines for this purpose.

- Two site connections — One connection is used for the active terminal (controlling the ONP procedure) and the second is used for tracing. If IOC or IOM equipment is available, Nortel Networks recommends that one site connection reside on one unit of the device, and the other connection on the second unit.
- One reliable voice number is required.

***Note 1:*** If these services are unavailable, contact Nortel Networks support personnel to determine if the available services are sufficient.

***Note 2:*** Foreign Exchange (FX) numbers are recommended for both voice and data lines for Applicator remote site access.

**2** Ensure two usernames and passwords with at least the following settings are provided for the ONP:

- COMCLASS — ALL
- PRIVCLASS — ALL
- STACKSIZE — 10000
- PRIORITY — 4

**3**



**DANGER**

**Prolonged software upgrade time**

Failure to provide working and reliable dialup access may cause problems during the software upgrade.

Failure to provide two dialups will jeopardize the software upgrade.

If the software delivery engineer loses contact with the office during SWACT, any datakits or defender modems will require more time accessing the switch, prolong office recovery times, and extend any potential service degradation. The operating company is responsible for providing all of the required information (pin #, passcodes, destinations, etc.) to the Applicator at the start of the ONP. The operating company is also responsible for ensuring that access is completely operational before starting the ONP.

## Network management control

**ATTENTION**
If necessary, contact your Network Maintenance support for assistance with these steps.

If Network Management code blocking is active before the ONP, the code blocking must be restored after the ONP is complete.

***SITE — At the MAP***

1 Make a list of all active code controls before the ONP to aid in restoration of code blocking.

```
> MASSCALL LIST CGAP ACODE ALL
```

2 Code blocking must be restored after the ONP. Make arrangements with Network Maintenance personnel for assistance.

3 This procedure is complete.

# Preserve logs over ONP

Logs that are suppressed or have a threshold set are configured for each site. Unless these logs are datafilled in table LOGCLASS, the settings will not be restored in the new call processing software load. Follow this procedure to determine which log reports are specially configured and how to provision table LOGCLASS.

***SITE — At the MAP***

**1** Determine which log reports are specially configured:

```
> LOGUTIL
> LISTREPS SPECIAL
> QUIT
```

**2** Determine if these log reports are already datafilled in table LOGCLASS:

```
> TABLE LOGCLASS
> LIS ALL (THRESHLD NE '0')
> LIS ALL (SUPPRESS NE 'N')
```

***Note:*** The field for threshold is spelled THRESHLD. The second command lists all tuples with a threshold that does not equal zero.

**3** If the output from step 2 does not equal the output from step 1, change as necessary to match the output from the LISTREPS output:

```
> RWOK ON
> POS <log_name>
> CHA <THRESHLD or SUPPRESS> <value or Y>
> YES
```

**log_name**
is the log report name such as TRKMEM listed in the LISTREPS output

**value**
is an integer value listed in the LISTREPS output

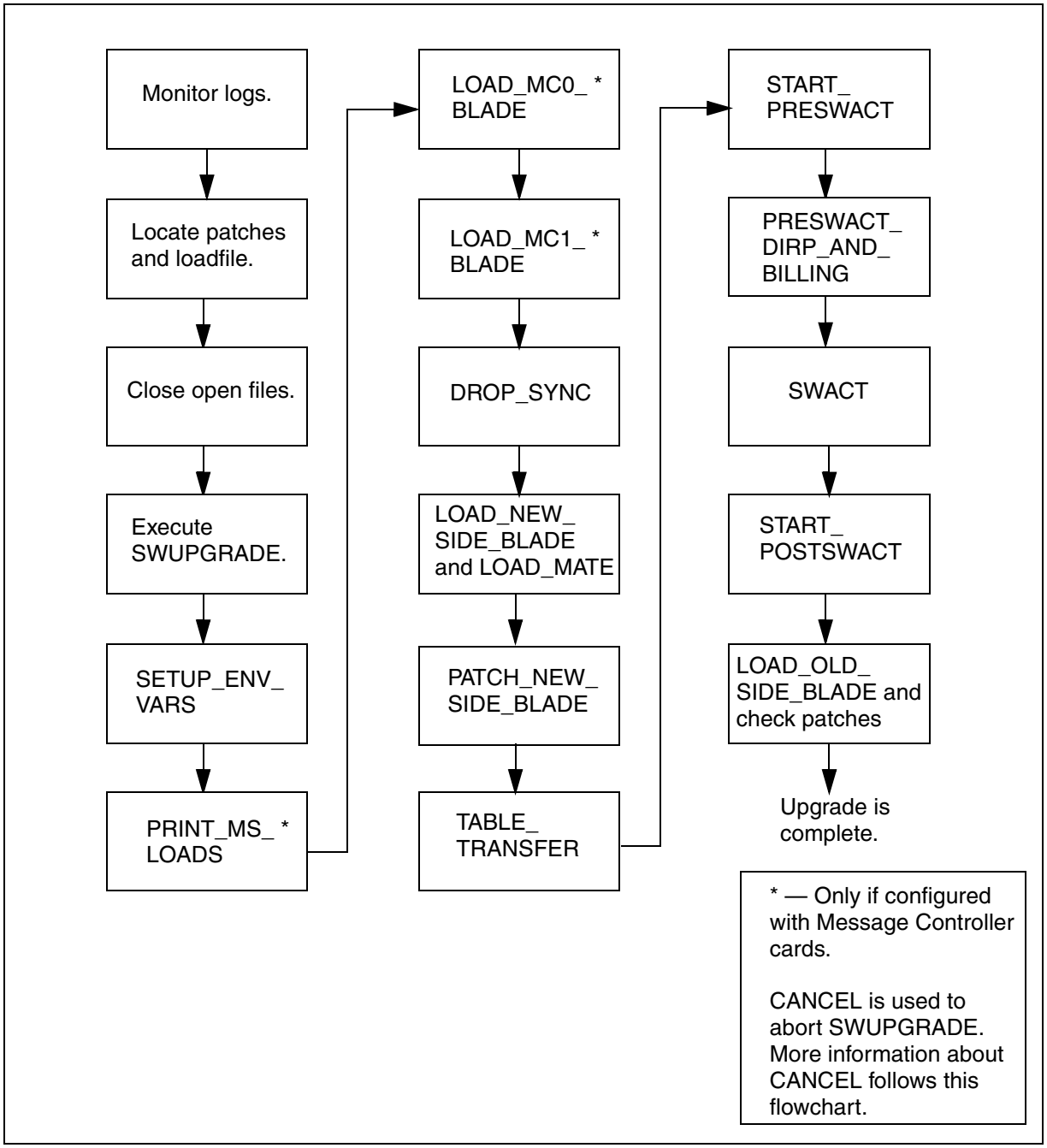
**4** Repeat step 3 for each required change and then exit the LOGUTIL level:

```
> QUIT
```

**5** This procedure is complete.

# SWUPGRADE

This section contains procedures that automate many of the upgrade tasks. Please read the important information following this flowchart.




Before proceeding with the procedures in this SWUPGRADE section of this document, complete the procedures in sections Upgrading the CS

2000 Compact on page 1123, Preparing to upgrade CS 2000 Compact on page 367, and Site responsibilities the day of the software delivery on page 1131.

## Software

TheCS2K Management Tool reads CD-ROMS and DVDs.

Software for the Call Agent platform is available on CDROM as a package for the CS 2000 Management Tools server. The software package is installed with the **platform_load_install.sh** tool on the CS 2000 Management Tools server. Software for the Message Controller cards is automatically installed in all offices even though not all offices have Message Controller cards. If the software is not installed, refer to Apply platform software for Call Agent and Message Controller on page 377.

The software image for the call processing application is taken from DVD on the CS 2000 Management Tools server, and then transferred to the Call Agent card file system. It is then imported with the IMPORT command at the MAP to make the new image available for booting. If the upgrade software load is not available on one of the disk volumes, refer to Restore call processing application files on page 395.

If the office is configured with Message Controller cards, then a Message Switch software image is required for the Message Switch. This software image is taken from DVD on the CS 2000 Management Tools server at the same time as the upgrade call processing application image. Once the Message Switch software is transferred, it is imported to one of the disk volumes. If the Message Switch software load is not available on one of the disk volumes, refer to Upgrade Peripheral Modules and Message Switch on page 373.

## CANCEL command

The CANCEL command issued on the active terminal to abort SWUPGRADE. Instructions for the rollback are printed to the device that is selected as the TRACE_DEVICE.

To ensure that the TRACE_DEVICE is prepared to receive messages, enter command **TRACECI TEST 'TESTMESSAGE'** at the active terminal. The TRACE_DEVICE is still connected if `TESTMESSAGE` is printed to it.

## Locate patches and loadfile

Call processing application patch files were loaded into the first device listed in table PADNDEV during the preparation phase. Use this procedure to verify the location of the patch files. The location is a required parameter during the SETUP_ENV_VARIABLES step of the software upgrade.

The call processing application image was retrieved from DVD, transferred, and stored during the preparation phase. Verify the location of the image.

### *SDE — At the ACTIVECM window*

1 Determine the default call processing application patch file location provisioned in table PADNDEV:

```
> TABLE PADNDEV; LIS ALL; QUIT
```

2 Make a note of the location. This value is a required parameter for the software upgrade.

3 Enter the disk utilities level and list the disk volumes:

```
> DISKUT; LV
```

4 List the contents of the volume with the upgrade call processing software image:

```
> LF <volume_name>
```

**volume_name**
is a string like SD00IMAGE

5 Make a note of the image file name. This value is a required parameter for environment variable LDMATE_IMAGE.

6 This procedure is complete.

If the CS 2000 - Compact is configured with Message Controller cards, check the Message Switch software loads and ensure that both Message Switches are running the same load and the load is specified in the *Peripheral Module Software Release Document*.

### *SDE — At the ACTIVECM window*

1 Remote login to Message Switch 0:

```
> REMLOGIN MS 0
```

*The terminal is now active on Message Switch 0.*

2 Issue the IMAGENAME command:

```
MS0> IMAGENAME
```

*The software load running in the Message Switch is displayed.*

```
MS-U BCS 55 CE built on 2004-APR-12 at 19:26:00
using mux20ce
LOAD: NIL.000
LAYER: BAS.21.0.CE
LAYER: TL.20.0.CE
```

3 Logout of the Message Switch:

```
MS0> REMLOGOUT
```

4 Ensure that the software load displayed (mux20ce in the example) is the correct Message Switch load for this release.

Use the REMLOGIN command to log into Message Switch 1, issue the IMAGENAME command, and REMLOGOUT. Ensure that the two Message Switches are running the same software load.

5



**CAUTION**

**Possible service interruption**

If the Message Switch is not loaded correctly, escalate immediately. Incorrect MS loads will cause subsequent AutoONP processes to fail and will jeopardize the software delivery application.

This procedure is complete.

# Close open files

Open files may have data in cache rather than written to storage. Follow this procedure to ensure that data is written to storage.

***SDE — At the ACTIVECM window***

**1** Determine if there are any open files:

```
> DISKUT; LV
```

```
DISKUT:
Volumes found:
--------------
NAME                    TYPE       TOTAL        FREE TOTAL  OPEN
                                  BLOCKS      BLOCKS FILES  FILES F
-------------------------------------------------------------------
SD00IMAGE                STD     1638400      269821     4     0
SD00IMAGE1               STD     1638400      718476     3     0
SD00TEMP                 STD      409600      409498     4     0
```

**2** For billing and Device Independent Recording Package (DIRP) files, rotate the volumes:

```
> MAPCI;MTC;IOD;DIRP
> ROTATE <subsystem>
> QUIT ALL
```

**subsystem**
is a billing or DIRP subsystem such as AMA

**3** For regular files, determine the name of the open file and close the file:

```
> LF <volume_name>
> FILECLOSE <file_name> <volume_name>
```

**volume_name**
is the name of the volume with open files from step 1

**file_name**
is the name of the file to close returned by the LF command

**4** For assistance with closing open files, contact Nortel Networks support personnel.

**5** This procedure is complete.

# Execute SWUPGRADE

The Automated One Night Process (AutoONP) maintains a list of steps to execute. When a step fails or requires user input, the process stops, the user responds to the problem and types **GO** to continue until all steps are executed.

Help for the SWUPGRADE level commands is available by typing **HELP** while in the SWUPGRADE level.

Step DOWNLOAD_FILES reminds the Software Delivery Engineer to retrieve the bulletins file. If the bulletins file is not available in SFDEV, the software upgrade will fail.

The number of steps in the AutoONP process is determined by the CS 2000 - Compact configuration. If the CS 2000 - Compact is configured with Message Controller cards, there are more steps.

**SWUPGRADE CA steps**

| without Message Controllers | with Message Controllers |
|---|---|
| SETUP_ENV_VARS | SETUP_ENV_VARS |
| NOTIFY_USERS | NOTIFY_USERS |
| SET_LOGIN_BANNER | SET_LOGIN_BANNER |
| DOWNLOAD_FILES | DOWNLOAD_FILES |
| READ_BULLETINS | READ_BULLETINS |
| VERIFY_DEVICES | VERIFY_DEVICES |
| PRINT_PARMS_AND_SAVE | PRINT_PARMS_AND_SAVE |
| CHECK_LOGS_1 | CHECK_LOGS_1 |
| STOP_JOURNAL_FILE | STOP_JOURNAL_FILE |
| | PRINT_MS_LOADS |
| DISABLE_PRSM_AUDIT_ACT | DISABLE_PRSM_AUDIT_ACT |
| | LOAD_MC0_BLADE |
| | LOAD_MC1_BLADE |

**SWUPGRADE CA steps**

| without Message Controllers | with Message Controllers |
|---|---|
| DROP_SYNC | DROP_SYNC |
| LOAD_NEW_SIDE_BLADE | LOAD_NEW_SIDE_BLADE |
| LOAD_MATE | LOAD_MATE |
| PATCH_NEW_SIDE_BLADE | PATCH_NEW_SIDE_BLADE |
| MATELINK_RTS | MATELINK_RTS |
| UPDATE_STEPS_AND_VARS | UPDATE_STEPS_AND_VARS |
| CHECK_NEW_LOAD | CHECK_NEW_LOAD |
| SET_DATE_AND_LOGMSG | SET_DATE_AND_LOGMSG |
| CHECK_LOGS_2 | CHECK_LOGS_2 |
| CLEAR_TRAPINFO | CLEAR_TRAPINFO |
| TRANSFER_DEVICES_INFO | TRANSFER_DEVICES_INFO |
| TRANSFER_PARM_VALUES | TRANSFER_PARM_VALUES |
| | MS_CHECK |
| DISABLE_AUTOIMAGE | DISABLE_AUTOIMAGE |
| SET_OFFICE_TUPLES | SET_OFFICE_TUPLES |
| SET_PADNDEV | SET_PADNDEV |
| SEND_PATCHES | SEND_PATCHES |
| APPLY_PATCHES | APPLY_PATCHES |
| CHECK_LOGS_3 | CHECK_LOGS_3 |
| RESTORE_PADNDEV | RESTORE_PADNDEV |
| TABLE_TRANSFER | TABLE_TRANSFER |
| TABXFR_REPORT | TABXFR_REPORT |
| CHECK_LOGS_4 | CHECK_LOGS_4 |
| START_PRESWACT | START_PRESWACT |

**SWUPGRADE CA steps**

| without Message Controllers | with Message Controllers |
|---|---|
| PRESWACT_DIRP_AND_BILLING | PRESWACT_DIRP_AND_BILLING |
| PRINT_SPMS_INDICES | PRINT_SPMS_INDICES |
| GET_FIRST_SWACT_AGREEMENT | GET_FIRST_SWACT_AGREEMENT |
| PREPARE_FOR_SWACT | PREPARE_FOR_SWACT |
| STATUSCHECK | STATUSCHECK |
| CHECK_LOGS_5 | CHECK_LOGS_5 |
| TRANSFER_TIMINGS | TRANSFER_TIMINGS |
| SWACT | SWACT |
| DISPLAY_DATE | DISPLAY_DATE |
| RECOVER_DIRP_AND_BILLING | RECOVER_DIRP_AND_BILLING |
| PERFORM_TEST_CALLS_1 | PERFORM_TEST_CALLS_1 |
| START_POSTSWACT | START_POSTSWACT |
| RESTART_OLD_LOAD | RESTART_OLD_LOAD |
| DRTIME_PRINT | DRTIME_PRINT |
| PERFORM_TEST_CALLS_2 | PERFORM_TEST_CALLS_2 |
| LOAD_OLD_SIDE_BLADE | LOAD_OLD_SIDE_BLADE |
| SYNC_SWITCH | SYNC_SWITCH |
| FINISH_POSTSWACT | FINISH_POSTSWACT |
| RESTORE_PARMS | RESTORE_PARMS |
| RESET_DEVICES | RESET_DEVICES |
| COMPLETE_NEW_LOAD_INIT | COMPLETE_NEW_LOAD_INIT |
| RESET_LOGIN_BANNER | RESET_LOGIN_BANNER |
| DUMP_NEW_LOAD | DUMP_NEW_LOAD |

**SWUPGRADE CA steps**

| without Message Controllers | with Message Controllers |
|---|---|
| RESUME_REX_TEST | RESUME_REX_TEST |
| START_JOURNAL_FILE | START_JOURNAL_FILE |
| PRINT_SWUPGRADE_REPORT | PRINT_SWUPGRADE_REPORT |
| STOP_RECORD | STOP_RECORD |
| UPGRADE_COMPLETE | UPGRADE_COMPLETE |

***SDE — At the ACTIVECM window***

1 Enter the software upgrade level:

```
> SWUPGRADE CA
```

2 Press return twice to display the current office header message. Note the office header message for environment variable INACT_LOGMSG.

3 Begin the upgrade:

```
> START
```

4 Proceed to SETUP_ENV_VARS.

## Additional information

### How to insert, delete, or modify steps

To allow customization of the AutoONP, SWUPGRADE allows the user to change the steps that are normally performed. Commands are available to insert, delete, or otherwise modify the AutoONP steps.

Use the **INSERT** command to add a new step or copy an existing step into another location in the step list. The step list is printed with command **DISP STEPS**. **REMOVE** removes any step or pause that was added. **OVERRIDE** disables the execution of a step. **PAUSE** is used to halt the AutoONP process before or after a step until **RESUME** is entered.

### Use of the BULLETINS file

The BULLETINS file is maintained by Nortel Networks Global Software Delivery and is used to provide as much automation as possible when performing the application bulletins and workarounds. Since application bulletins and workarounds will vary depending on the "from and to" software loads, it is recommended that the BULLETINS file and all bulletins and workarounds be reviewed before starting the AutoONP.

When required, bulletins and workarounds should be followed and manually executed during the AutoONP.

**ATTENTION**

The BULLETINS file is a critical file that must be located in SFDEV for execution during the AutoONP.

If this file is missing from SFDEV or if it is named incorrectly, the AutoONP will fail. For assistance with the BULLETINS file contact the Global Software Delivery hotline for your market.

Step DOWNLOAD_FILES, towards the beginning of the AutoONP process, will remind the user to download the BULLETINS file (along with other required files). If desired, print a hard copy of the BULLETINS file and review the file contents.

Step READ_BULLETINS will read (that is, execute) the BULLETINS file during the AutoONP.

### Using the CANCEL command

The CANCEL command is used to terminate or abort the software upgrade and halt the execution of the SWUPGRADE process at any time during the AutoONP. This command reverts all SWUPGRADE steps and returns the switch to its original state.

### Getting help on AutoONP steps

The SWUPGRADE increment is used to perform the AutoONP. At any time within this increment you may type HELP for a list of the commands available. Also, the HELP command has options to obtain information about a command syntax, specific step, or variable.

**HELP** displays a brief description of the SWUPGRADE increment and a list of the available CI commands. **HELP <swupgrade command>** displays a brief description and syntax of the command. **HELP STEP <step>** displays a brief description of a step's functionality. **HELP VAR <variable>** displays a brief description and the current value of the variable.

For additional information about SWUPGRADE commands, refer to section "SWUPGRADE summary" of Appendix A in *Software Delivery One Night Process Software Delivery Procedures*, 297-8991-303.

# SETUP_ENV_VARS

***SDE — At the ACTIVECM window***

**1** Set variable TRACE_USER to ME:

**TRACE_USER (no default)**
Holds the USER name on whose console output messages are printed. Changing the value of this variable changes the value of the TRACE_DEVICE variable, and causes the output to be redirected to the new USER device.

Value: <user name> or ME - a user name, such as ADMIN, or ME which indicates the current user

***Note:*** For clarity purposes, it is recommended to set this variable to a user other than the current user.

The USER must be LOGGED IN when this variable is set. The current setting is: <none>

```
> ME
```

**2** Do not change the TRACE_DEVICE variable. Press the Enter key.

**TRACE_DEVICE**
Holds the device name on which output messages are printed. Changing the value of this variable causes the output to be redirected to the new device.

Value: <trace device name> - a string, such as MAP

***Note:*** For clarity purposes, it is recommended to set this variable to a device other than the currently logged on terminal.

The current setting is: <none>

*The selected device indicates “This device is selected for TRACing.”*

**3** Do not change the PRINTER variable. Press the Enter key.

**PRINTER**
Holds the name of the printer on which output messages are recorded. The printer echoes all output sent to the trace device. Changing the value of this variable causes the recording to be directed to the new device.

Value: <printer name> or SINK where <printer name> is a device datafilled in table TERMDEV. Choosing SINK means choosing no printer output.

```
> SINK
```

4 Do not change the LOGS variable. Press the Enter key.

**LOGS**
Holds the names of the logs that are checked by the LOGS step. More than one log can be specified by entering log names separated by a blank.

**Example**
'SWERR TRAP' — Check traps and swerrs. Display a message if traps or swerrs are recorded.

The current setting is: TRAP SWERR

5 Enter the INACT_LOGMSG variable. Use the existing office header *except* update the new job order number, software level, and current date.

**INACT_LOGMSG**
Holds the log message that will be displayed on the inactive side of the switch.

**Example**
*** H1234 Office_Name SN000006 17/AUG/2003 ***

6 Enter the LDMATE_IMAGE variable:

**LDMATE_IMAGE**
Holds the volume name and filename used to load the inactive unit.

**Example**
SD00IMAGE0 CSN0007BG

***Note:*** The software checks to verify that a file with the specified name exists on the volume.

7 Enter the PADNDEVS variable. The default value is SFDEV. If the call processing application files were loaded into SFDEV, press the Enter key. Otherwise, enter up to three device names if the patches were loaded into a location other than SFDEV during procedure Transfer call processing application patch files.

8 Do not change the TABXFR_STOPIF variable. Press the Enter key.

**TABXFR_STOPIF**
Determines the threshold for the maximum number of failed tables allowed before halting TABXFR.

**9** Do not change the TABXFR_LIMIT variable. Press the Enter key.

**TABXFR_LIMIT**
Determines the threshold for the maximum number of tuple failures allowed before halting TABXFR.

**10** Do not change the TABXFR_INITIAL_PRINT variable. Press the Enter key.

**TABXFR_INITIAL_PRINT**
Determines the time interval for printing a single message containing the current table name.

**11** Set the TABXFR_INTERVAL_PRINT variable to 30 seconds:

**TABXFR_INTERVAL_PRINT**
Determines the time interval for printing regular table transfer status messages. This is particularly useful for large tables.

```
> 30 SECS
```

**12** Do not change the SPMS_OPTION variable. Press the Enter key.

**SPMS_OPTION**
Holds the date, or number of days, to generate the SPMS (Switch Performance Monitoring System) indices.

**13** Do not change the DRTIME_REPORT variable. Press the Enter key.

**DRTIME_REPORT**
Determines if the DRTIME report should be printed before SYNC. DRTIME provides statistics on the TABXFR process. Normally this information is not used unless this information is requested.

**14** Set the DUMP_NEW_LOAD variable:

**DUMP_NEW_LOAD**
Determines if an image dump of the new load should be taken.

```
> NO
```

***Note:*** If the value of this variable is set to NO, the Site is responsible for manually taking an image of the new software load immediately after the AutoONP is complete.

*The variables are printed to the terminal.*

```
WARNING: An ACTIVE VOLUME must be datafilled in table
         IMAGEDEV to use AUTODUMP.

SWUPGRADE variables for target CA:

Variable Name                                    Value
------------------------------------------------------------------------
TRACE_USER                          =   USERNAME
TRACE_DEVICE                        =   TELNSVR00018
PRINTER                             =   SINK
LOGS                                =   TRAP SWERR
INACT_LOGMSG                        =   INACT_LOGIN_MESSAGE
LDMATE_IMAGE                        =   SD00IMAGE0 CSN0007BG
PADNDEVS                            =   SFDEV
TABXFR_STOPIF                       =   1
TABXFR_LIMIT                        =   25
TABXFR_INITIAL_PRINT                =   30 SECS
TABXFR_INTERVAL_PRINT               =   30 SECS
SPMS_OPTION                         =   NONE
DRTIME_REPORT                       =   NO
DUMP_NEW_LOAD                       =   NO
```

**15** Type **GO** and press the Enter key to proceed with the upgrade. Monitor messages on the TRACE_DEVICE.

*Step NOTIFY_USERS is automatically run. The notified usernames and environment variables are printed to the terminal.*

*Step SET_LOGIN_BANNER is automatically run.*

*Step DOWNLOAD_FILES begins, reminds the SDE to download optional application and BULLETINS file and then waits for the SDE to type GO.*

**16** After downloading any required files, type **GO** and press the Enter key.

**17** If a BULLETINS files is located in SFDEV, it is read and executed during step READ_BULLETINS.

If a BULLETINS file is not found in SFDEV, the step fails. If a BULLETINS file is not needed, type **OVERRIDE READ_BULLETINS**, press the Enter key, and confirm the override.

Type **GO** and press the Enter key to continue.

*The following steps are automatically run:*

- *VERIFY_DEVICES*
- *PRINT_PARMS_AND_SAVE*
- *CHECK_LOGS1*

  ***Note:** Display the contents of all logs listed. Use the **DISPLAY LOG <log_name> ALL <ACT or INACT>** command.*

- *STOP_JOURNAL_FILE*

*If the CS 2000 - Compact is equipped with Message Controller cards, step PRINT_MS_LOADS runs. Otherwise, step DISABLE_PRSM_AUDIT_ACT runs.*

***Note:** Step DISABLE_PRSM_AUDIT_ACT has several substeps.*

## Additional information

If any variables require correction, use the **SET** command to change the variable. If the variable consists of two or more words such as SD00PATCH and SD01PATCH, use quotation marks to enclose the words.

**Example**
SET PADNDEVS ‘SFDEV SD00PATCH SD01PATCH’

Variables can be displayed at any time with the **DISP VAR** command.

**Example**
DISP VAR PADNDEVS

# PRINT_MS_LOADS

**ATTENTION**
This step only runs if the CS 2000 - Compact is configured with Message Controller cards.

***SDE — At the ACTIVECM window***

**1** Step PRINT_MS_LOADS runs.

```
Starting step PRINT_MS_LOADS.
Please note that the displayed information corresponds
to the BASE layer of the MS load.
Load in MS 0 = MS-U21BC
Load in MS 1 = MS-U21BC

Please check the above MS loads for correctness.
Step PRINT_MS_LOADS is complete.

The SWUPGRADE process has paused. Enter GO.
```

***Note:*** MS-U21xx is the correct value for upgrading to SN07.

**2** If the value reported is not correct, do not proceed. Contact Nortel Networks support personnel immediately.

**3** Type **GO** and press the Enter key.

*Step PRINT_MS_LOADS completes.*

*Step DISABLE_PRSM_AUDIT_ACT runs and completes.*

# LOAD_MC0_BLADE

**ATTENTION**
This step only runs if the CS 2000 - Compact is configured with Message Controller cards.

***SDE — At the ACTIVECM window***

**1** Step LOAD_MC0_BLADE runs.

```
Starting step LOAD_MC0_BLADE.
Upgrade load of MC  0 at the SAM21 EM GUI
by using the following manual procedure:
  1) At the MAPCI;MTC;MS map level, verify that MS 1 is the
     master MS.
  2) If MS 1 is not the master, perform a SWMAST. If
     performed, soak 10 minutes.
  3) At SAM21 EM GUI, open Card View for MC 0
    a) Under Provisioning Tab, determine IP address of
       the card.
    b) Ensure IP address in GUI matches IP address of MC 0.
  4) Under the States Tab, Lock the card.
    a) Wait for the lock icon to appear.
  5) Under the Provisioning Tab, change the boot file:
    a) Click Modify.
    b) Change boot file name to new load.
    c) Click Save.
  6) Under the States Tab, Unlock the card
    a) Wait for the lock icon to disappear.
  7) At Active CCAMTC MAP; MC level, Validate newly booted
     load.
    a) QryLd command for MC0 must indicate new MC load
       version.
  8) Soak for 10 minutes, monitoring logs.

Type GO to continue SWUPGRADE when above steps are
successfully completed.

Step LOAD_MC0_BLADE is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2** At the MAPCI;MTC;MS level, ensure that MS 1 is the master MS.

```
          MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
           .      .       .        .       .      .       ...     .       .

 MS                Message Switch   Clock   Shelf  0       Inter-MS Link 0 1
  0 Quit       MS 0        .          Slave          F                    . .
  2            MS 1        .          M Free         F                    . .
  3
  4
  5
  6 Tst_
  7 Bsy_
  8 RTS_
  9
 10 LoadMS_
```

**3** If MS 1 is not the master MS, perform a **SWMAST**. If SWMAST is performed, then soak 10 minutes before continuing.

***At the active Call Agent Manager interface (CORE0 or CORE1)***

**4** At the MCMtc level, verify that both Message Controllers are in service (.) prior to Locking Message Controller 0 in the next step.

```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
     .             .         .         .          .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit       MC0    .       . Act      . Inact    open       open
 2            MC1    .       . Act      . Inact    open       open
 3
```

**5** Exit the Call Agent Manager interface and determine the IP address of Message Controller 0:

```
>0 ALL
[mtc@hostname mtc]$ grep mc0 /etc/hosts
```

*The grep command returns the address of Message Controller 0.*

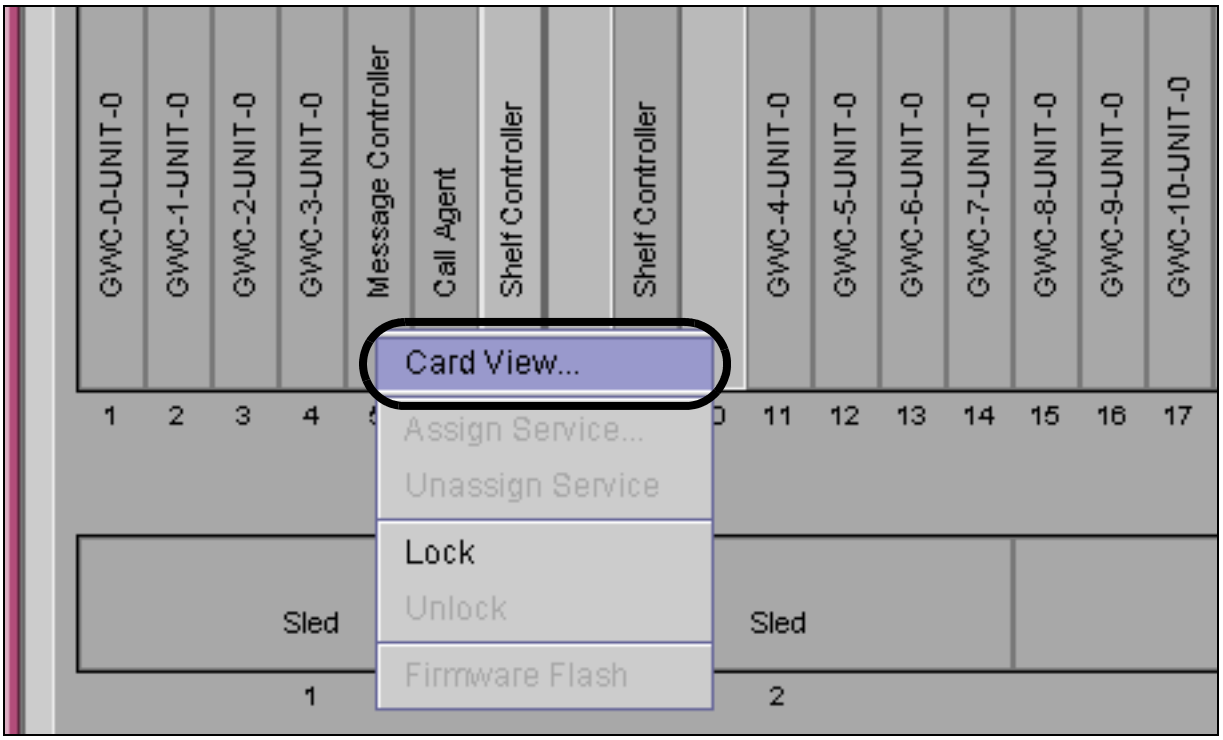
```
10.40.54.60 mc0
```

**6** Start the Call Agent Manager interface again:

```
[mtc@hostname mtc]$ ccamtc mcmtc
```

***At the CS 2000 SAM21 Manager client***

**7** From the Shelf View, right click on the card and select Card View.



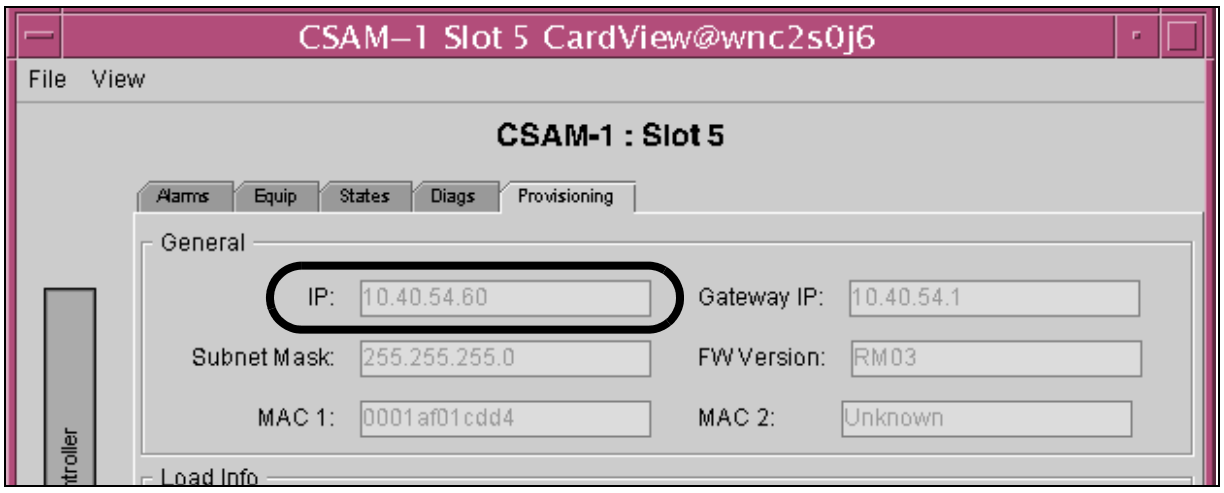

***Note:*** The Shelf View window will reflect office provisioning and the hardware configuration of the SAM21 shelf.

*The Card View window opens.*

**8** Select the Provisioning tab on the Card View window.

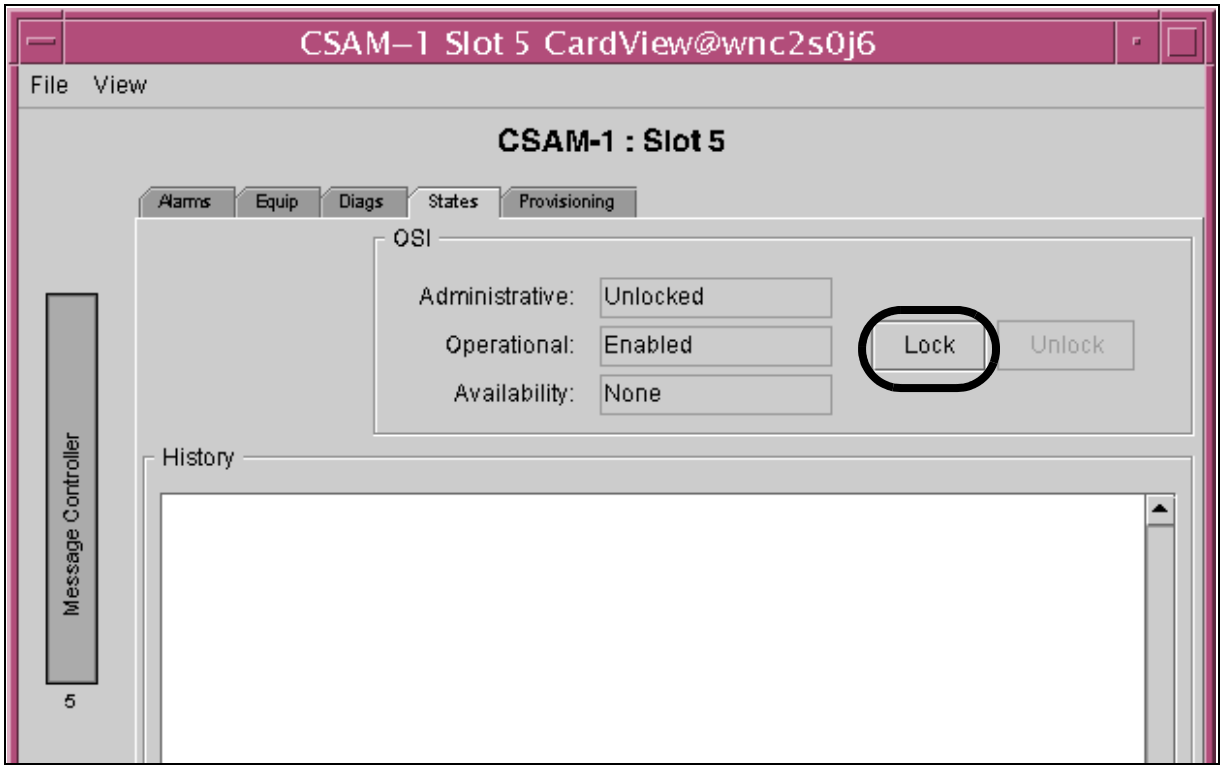
Ensure that the IP address specified in the IP field matches the IP address of Message Controller 0 from step 5. If the values do not match, open the other Shelf View from the CS 2000 SAM21

Manager and check the Message Controller provisioning for that shelf.



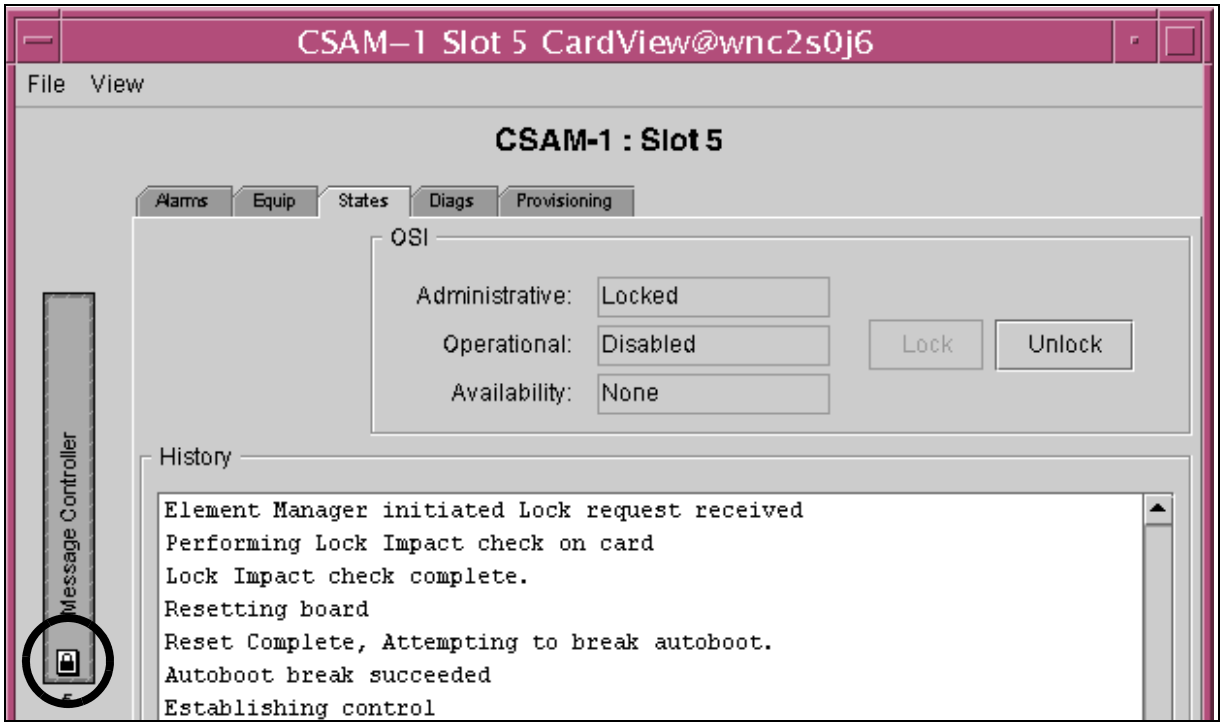

**9** Click on the States tab.

Click on the Lock button.



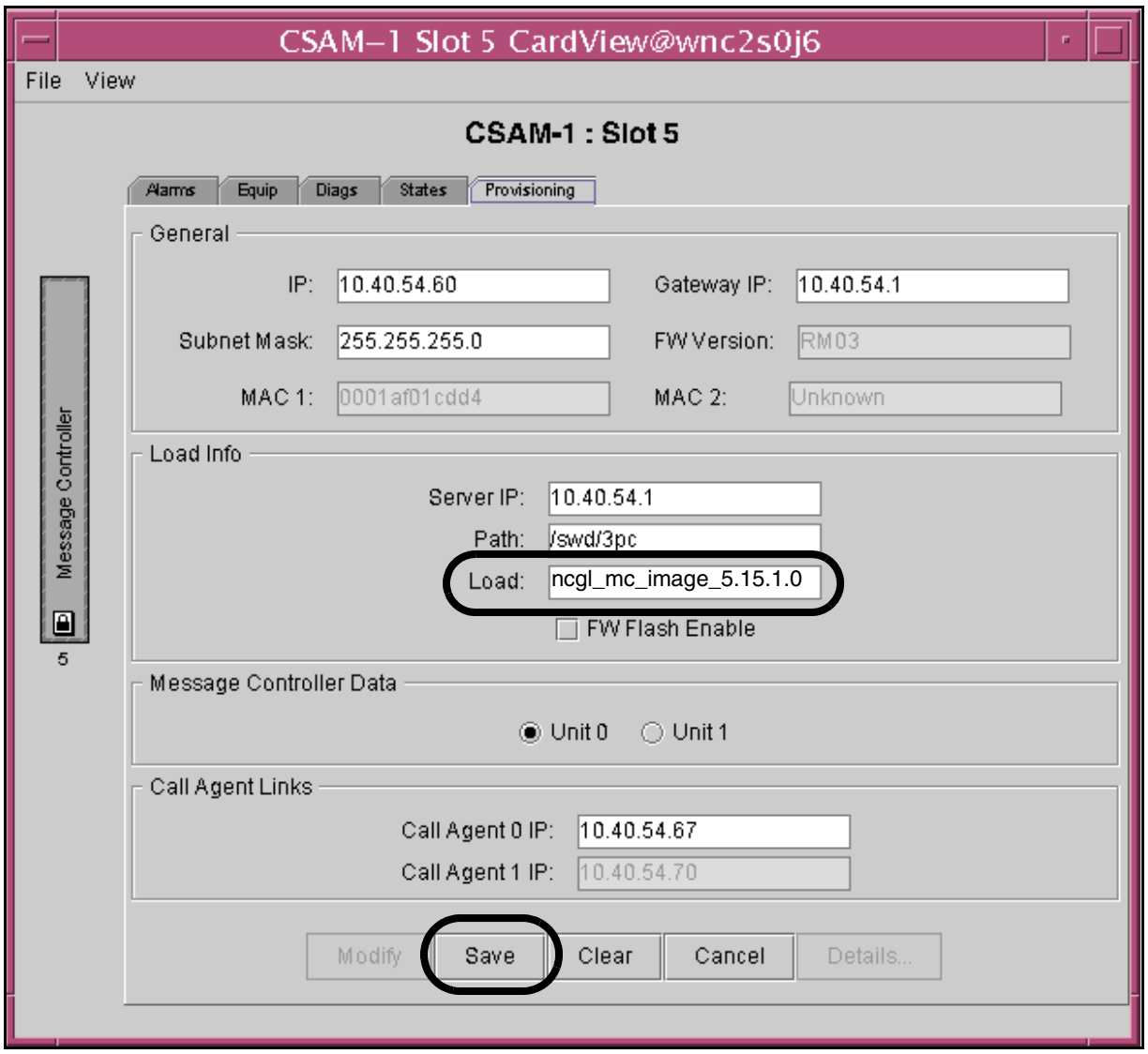

*A lock warning dialog window opens. Confirm the lock warning.*

**10** Wait for the lock icon to appear on the card icon.




*At the Call Agent Manager, a major ATM alarm is raised. The Message Controller enters the Remote Busy (R) state and is reported as out of service.*

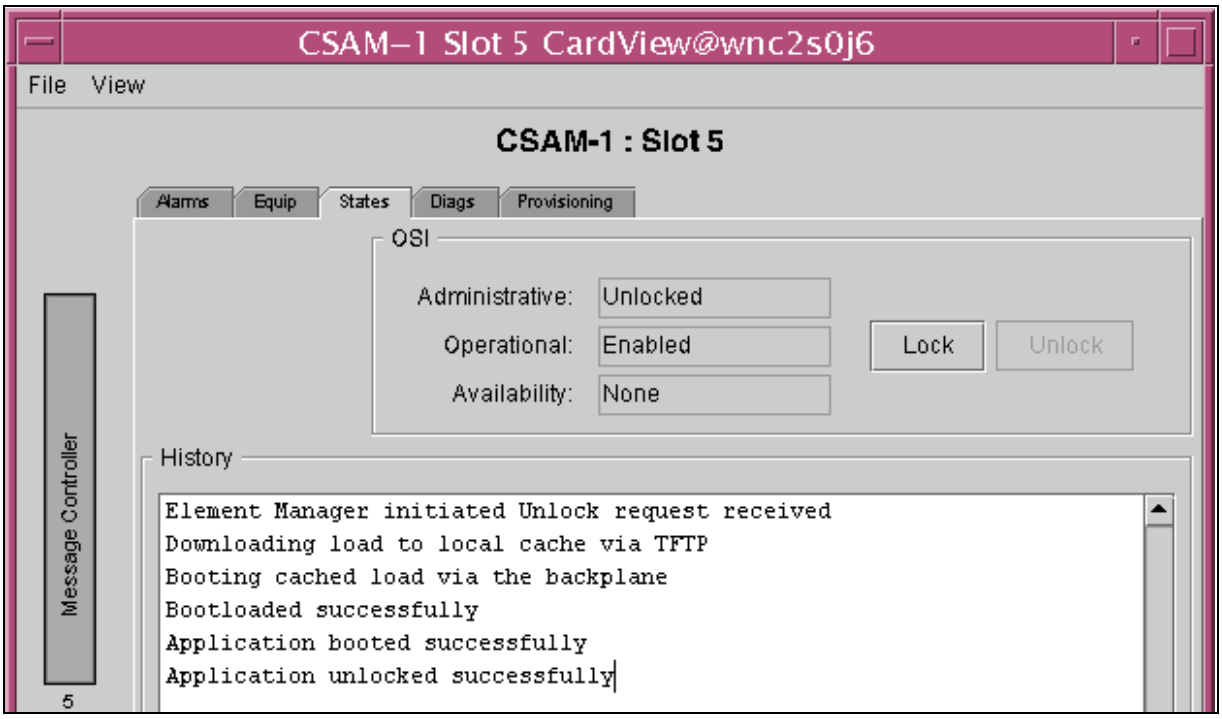
**11** Click on the Provisioning tab, change the Load value to the new software load name, and click Save.




*A warning dialog is generated indicating a load mismatch between the provisioning for the two Message Controller cards. Confirm the warning dialog by clicking OK.*

**12** Click on the States tab and click the Unlock button.

Wait for the lock icon to disappear.




*At the Call Agent Manager, the card enters the in service state (.), and the major ATM alarm clears. The Message Controller may raise a major MCTbl alarm while the Message Controller synchronizes to the NTP server.*

***At the active Call Agent Manager interface (CORE0 or CORE1)***

**13** Query the software load for Message Controller 0 and ensure that the new load is reported:

```
> MCMtc
> QryLd 0
```

```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
    .             .         .         .          .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit      MC0    .       . Act      . Inact    open       open
 2           MC1    .       . Act      . Inact    open       open
 3
 4
 5 QryLd
 6 QryHits
 7 ClrHits
 8 Trnsl
 9
10
11
12
13 LogQuery
14 Alarm
15
16           MC Load report retrieved on Thu Jun 19 13:48:45 2004:
17 Help
18 Refresh         Ramdisk: ncgl_mc_image_5.15.1.0
  mtc
Time  13:48  >
```

*Soak the load for 10 minutes while monitoring log reports.*

***SDE — At the ACTIVECM window***

**14** Type **GO** and press the Enter key to continue.

# LOAD_MC1_BLADE

**ATTENTION**
This step only runs if the CS 2000 - Compact is configured with Message Controller cards.

***SDE — At the ACTIVECM window***

**1** Step LOAD_MC1_BLADE runs.

```
Starting step LOAD_MC1_BLADE.
Upgrade load of MC 1 at the SAM21 EM GUI
by using the following manual procedure:
  1) At the MAPCI;MTC;MS map level, verify that MS 0 is the
     master MS.
  2) If MS 0 is not the master, perform a SWMAST. If
     performed, soak 10 minutes.
  3) At SAM21 EM GUI, open Card View for MC 1
    a) Under Provisioning Tab, determine IP address of
       the card.
    b) Ensure IP address in GUI matches IP address of MC 1.
  4) Under the States Tab, Lock the card.
    a) Wait for the lock icon to appear.
  5) Under the Provisioning Tab, change the boot file:
    a) Click Modify.
    b) Change boot file name to new load.
    c) Click Save.
  6) Under the States Tab, Unlock the card
    a) Wait for the lock icon to disappear.
  7) At Active CCAMTC MAP; MC level, Validate newly booted
     load.
    a) QryLd command for MC 1 must indicate new MC load
       version.
  8) Soak for 10 minutes, monitoring logs.

Type GO to continue SWUPGRADE when above steps are
successfully completed.

Step LOAD_MC1_BLADE is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2** At the MAPCI;MTC;MS level, ensure that MS 0 is the master MS.

```
          MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
           .       .        .        .        .        .        ...      .        .

 MS                  Message Switch   Clock   Shelf  0       Inter-MS Link 0 1
  0 Quit        MS 0        .          M Free          F                    . .
  2             MS 1        .          Slave           F                    . .
  3
  4
  5
  6 Tst_
  7 Bsy_
  8 RTS_
  9
 10 LoadMS_
```

**3** If MS 1 is not the master MS, perform a **SWMAST**. If SWMAST is performed, then soak 10 minutes before continuing.

***At the active Call Agent Manager interface (CORE0 or CORE1)***

**4** At the MCMtc level, verify that both Message Controllers are in service (.) prior to Locking Message Controller 1 in the next step.

```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
     .             .         .         .         .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit       MC0    .      . Act      . Inact    open       open
 2            MC1    .      . Act      . Inact    open       open
 3
```

**5** Exit the Call Agent Manager interface and determine the IP address of Message Controller 0:

```
>0 ALL
[mtc@hostname mtc]$ grep mc1 /etc/hosts
```

*The grep command returns the address of Message Controller 1.*

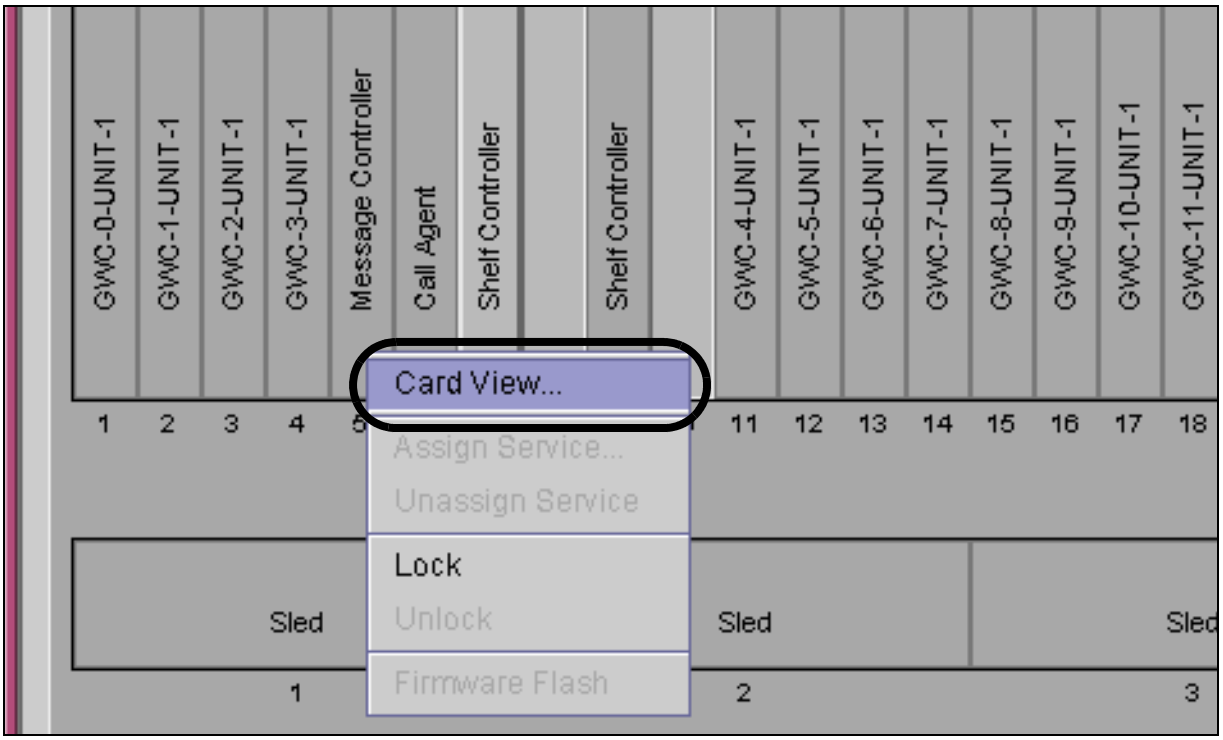
```
10.40.54.61 mc1
```

**6** Start the Call Agent Manager interface again:

```
[mtc@hostname mtc]$ ccamtc mcmtc
```

***At the CS 2000 SAM21 Manager client***

**7** From the Shelf View, right click on the card and select Card View.

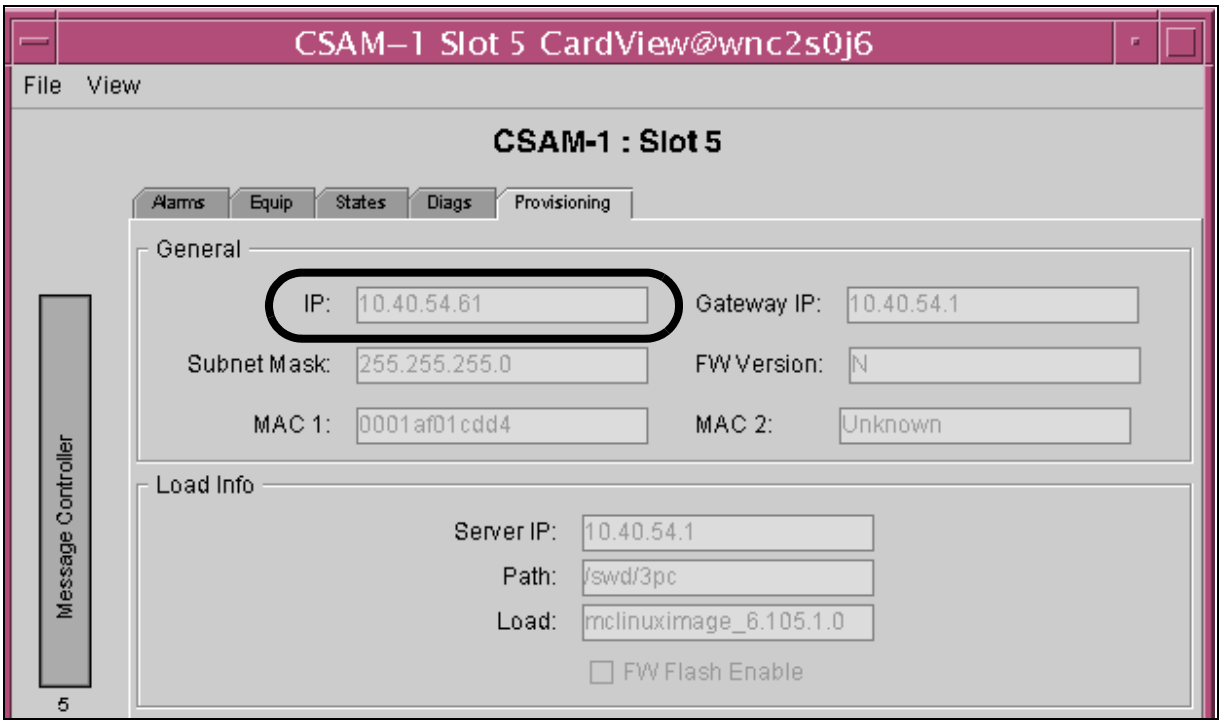



***Note:*** Message Controller 1 is located in slot 12 for some markets.

*The Card View window opens.*

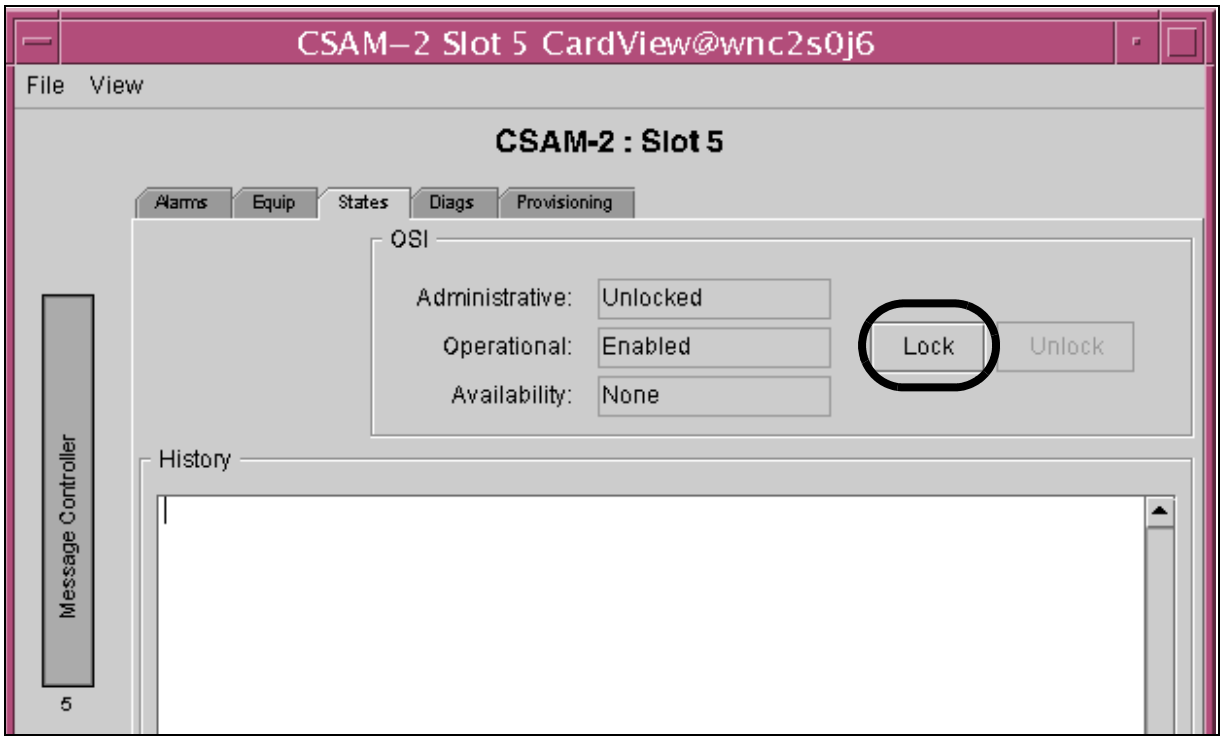
**8** Select the Provisioning tab on the Card View window.

Ensure that the IP address specified in the IP field matches the IP address of Message Controller 1. If the values do not match, open the other Shelf View from the CS 2000 SAM21 Manager and check the Message Controller provisioning for that shelf.



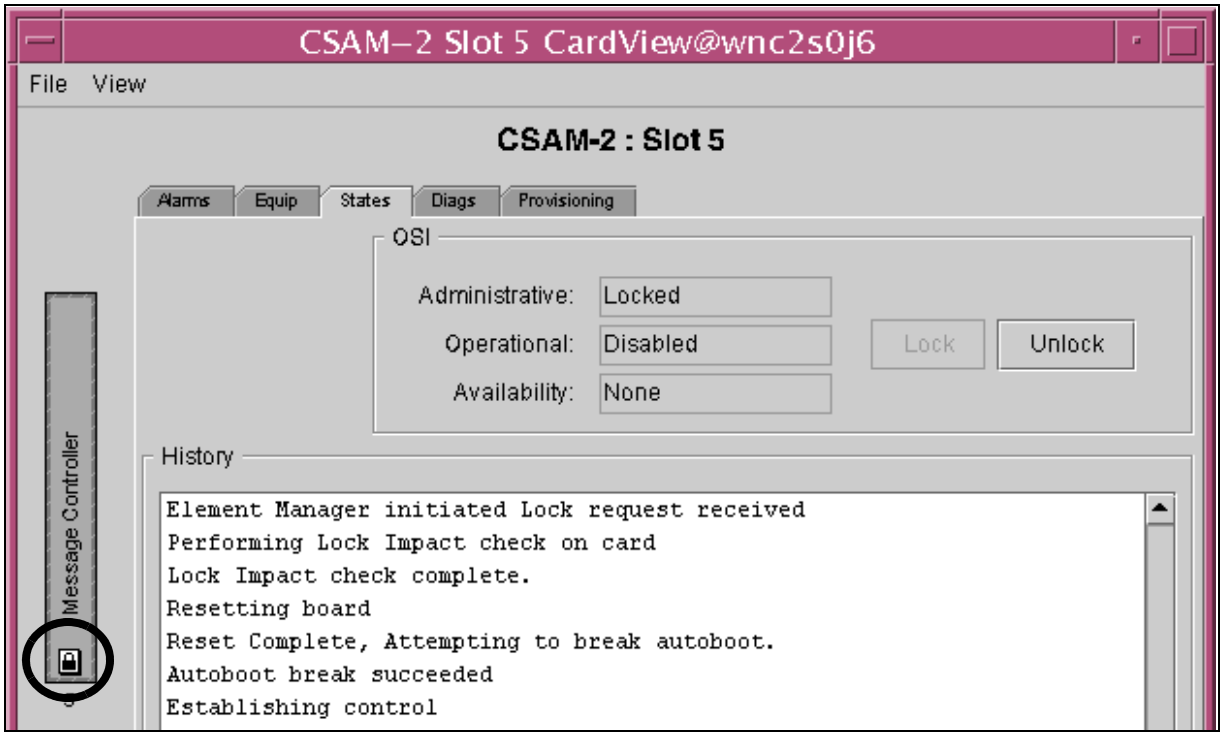
**9** Click on the States tab.

Click on the Lock button.



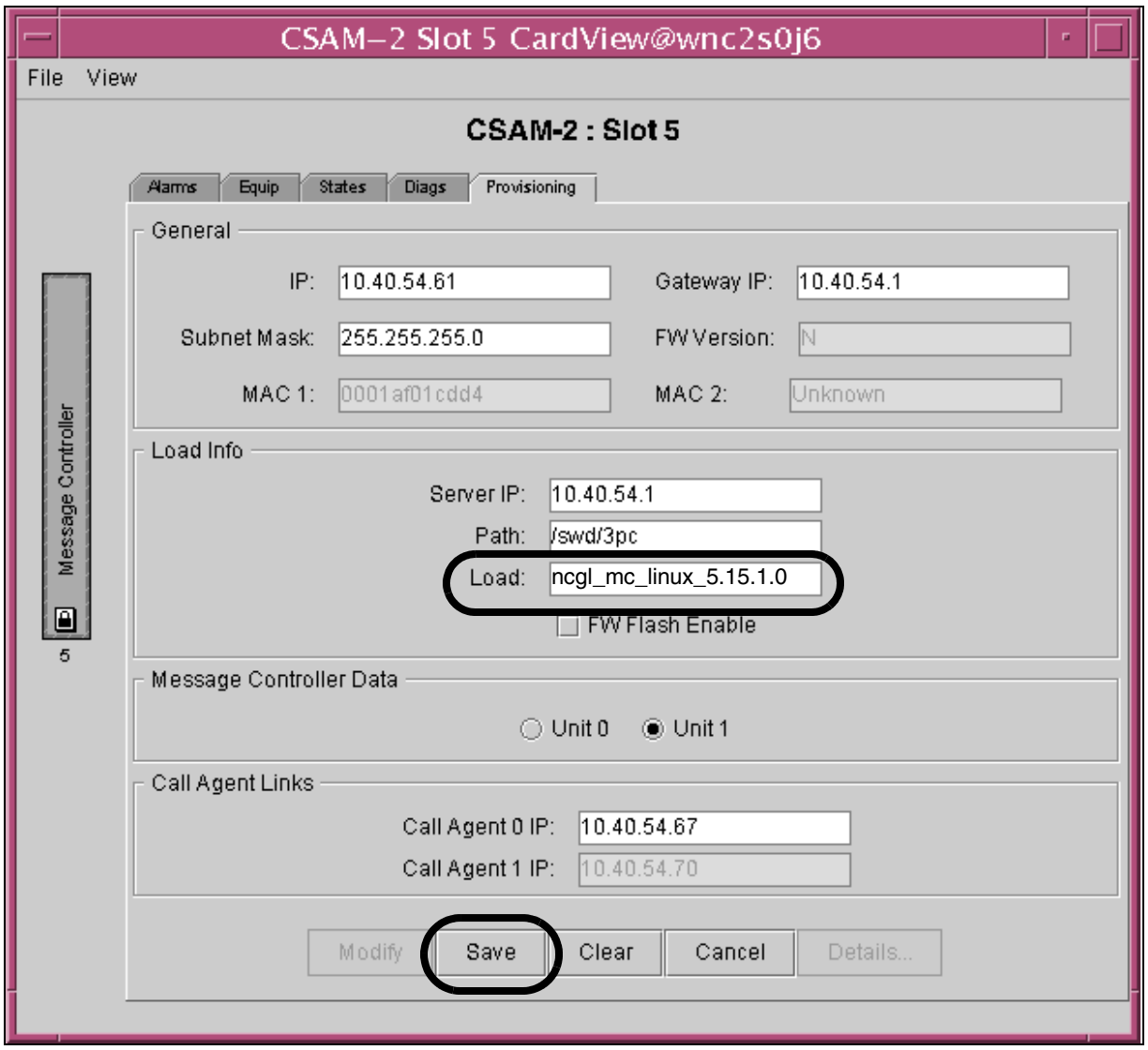

*A lock warning dialog window opens. Confirm the lock warning.*

**10** Wait for the lock icon to appear on the card icon.



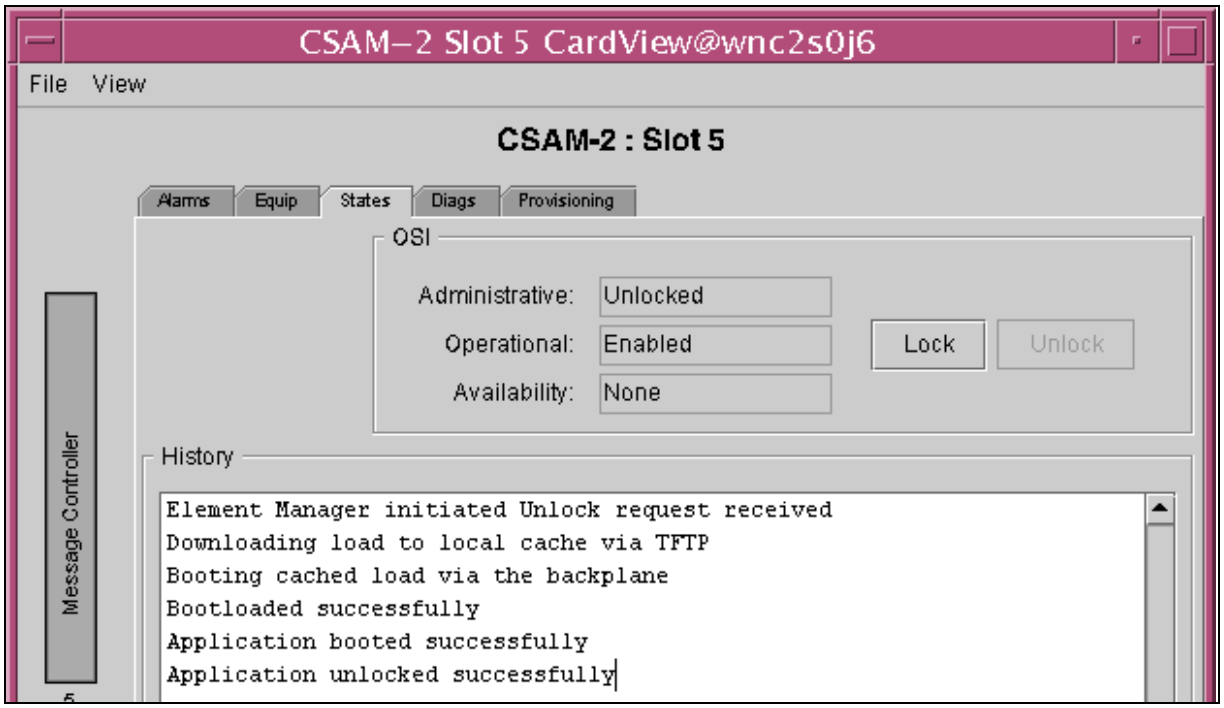

*At the Call Agent Manager, a major ATM alarm is raised, the Message Controller enters the Remote Busy (R) state and is reported as out of service.*

**11** Click on the Provisioning tab, click on Modify, change the Load value to the new software load name, and click Save.



**12** Click on the States tab and click the Unlock button.

Wait for the lock icon to disappear.




*At the Call Agent Manager, the card enters the in service state (.), and the major ATM alarm clears. The Message Controller may raise a major MCTbl alarm while the Message Controller synchronizes to the NTP server.*

***At the active Call Agent Manager interface (CORE0 or CORE1)***

**13** Query the software load for Message Controller 1 and ensure that the new load is reported:

```
> MCMtc
> QryLd 1
```

```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
    .             .         .         .          .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit      MC0    .       . Act      . Inact    open       open
 2           MC1    .       . Act      . Inact    open       open
 3
 4
 5 QryLd
 6 QryHits
 7 ClrHits
 8 Trnsl
 9
10
11
12
13 LogQuery
14 Alarm
15
16           MC Load report retrieved on Thu Jun 19 14:15:54 2004:
17 Help
18 Refresh         Ramdisk: ncgl_mc_image_5.15.1.0
  mtc
Time  13:48  >
```

*Soak the load for 10 minutes while monitoring log reports.*

***SDE — At the ACTIVECM window***

**14** Type **GO** and press the Enter key to continue.

# DROP_SYNC

Step DROP_SYNC requires jamming the inactive Call Agent from the active Call Agent Manager.

***SDE — At the ACTIVECM window***

1 Obtain approval to drop synchronization of the call processing application.

2 Type **GO** and press the Enter key to continue.

```
Starting step DROP_SYNC.
Please JAM the Inactive CA Application and confirm when complete:
At the Active TPCMTC MAP; CAMtc Level:
  1) JAM - Jam the Inactive application
Type GO to continue the SWUPGRADE when JAM is completed
Step DROP_SYNC is not complete.
The SWUPGRADE process has paused. Enter GO.
```

***SDE — At the CORE0 or CORE1 window***

3 Jam the inactive Call Agent from the active Call Agent Manager window.

```
> CoreMtc;CAMtc;Jam
```

4 Monitor the jam and verify that a JInact alarm is raised.

***SDE — At the ACTIVECM window***

5 Type **GO** and press the Enter key to continue.

6 Proceed to LOAD_NEW_SIDE_BLADE and LOAD_MATE.

## LOAD_NEW_SIDE_BLADE and LOAD_MATE

This procedure requires the SDE to perform the following actions:

- lock the inactive Call Agent card
- reprovision the platform software load
- unlock the inactive Call Agent

***SDE — At the ACTIVECM window***

**1** Review the message printed to the terminal.

```
Starting step LOAD_NEW_SIDE_BLADE.
Upgrade the New Side Call Agent load at the SAM21 EM GUI
by using the following manual procedure:
  1) At Active COREMTC MAP (ccamtc coremtc), query the Inact blade IP addr
    a) Use QueryIP command to determine the IP address of mate blade.
  2) At SAM21 EM GUI, open Card View for Inact Call Agent Card:
    a) Under the Provisioning Tab, determine IP address of the card.
    b) Ensure IP address in GUI matches inactive card IP address.
  3) Under the States Tab, Lock the card.
  4) Under the Provisioning Tab, change the boot file:
    a) Click Modify.
    b) Change boot file name to new load.
    c) Click Save.
  5) Under the States Tab, Unlock the card.
    a) Monitor the boot progress in the History pane.
  6) At Active COREMTC MAP, monitor Inact load initialization:
    a) Inact status begins with "/booting"
    b) Wait until the status becomes "/waiting"
  7) At Inactive COREMTC map (ccamtc coremtc), Validate newly booted load:
    a) Telnet/Login to the Inact Blade
    b) Under the Sys level, QryLd must indicate the new load version
Type GO to continue the SWUPGRADE when above steps are successfully complet
Step LOAD_NEW_SIDE_BLADE is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2** Perform the instructions listed in the output. Refer to the following procedures for assistance:

- Lock the inactive Call Agent — Call Agent Lock in *Upgrading the Call Agent*, NN10065-461
- Change the boot file — “Reprovision Call Agent platform load” in U*pgrading the Call Agent*, NN10065-461
- Unlock the inactive Call Agent — "Call Agent Unlock" in *Upgrading the Call Agent*, NN10065-461

**3** Type **GO** and press the Enter key.

*Step LOAD_NEW_SIDE_BLADE completes.*

*Step LOAD_MATE begins, loads the new call processing application on the inactive Call Agent, and completes. The image specified in variable LDMATE_IMAGE is loaded. Progress is displayed at the ACTIVECM window and the CORE0 and CORE1 windows.*

**4** Proceed to PATCH_NEW_SIDE_BLADE.

## PATCH_NEW_SIDE_BLADE

This step provides a prompt for the SDE to apply patches to the upgraded Call Agent platform software load. Patches for the call processing application are applied later in the upgrade. The patches must reside in the `/swd/3pc/patch` directory on the CS 2000 Core Manager or CBM.

***Note:*** The steps printed to the terminal may not be accurate. Perform the following steps to patch the new side blade.

1. At the inactive maintenance window (CORE0 or CORE1) verify that this is the inactive Call Agent.
2. Enter the Admin level and then the SWIM level.
3. At the TRANSFER level a list of available patches is displayed
   a. SELECT the patch by number
   b. FETCH INA the patch to the INACTIVE unit
4. At the PATCH level, for each patch to be applied and committed:
   a. SELECT the patch by number
   b. APPLY INA FORCE the patch to the INACTIVE unit
   c. SELECT the patch by number
   d. COMMIT INA the patch to the INACTIVE unit

Each patch is applied and committed to the inactive Call Agent unit. The Status for each patch changes from NEW to COMMITTED. Using the **COMMIT** command commits the patch to the load so that the patch is reapplied the next time the card is reset. If the patch is not committed, it will not be reapplied the next time the card is reset.

***SDE — At the ACTIVECM window***

**1** Review the message printed to the terminal.

```
Starting step PATCH_NEW_SIDE_BLADE.
If patches for the New Side Call Agent Load are available,
upgrade the load to the current patch level
using the following manual procedure:
  1) At the Inact COREMTC map (ccamtc corematc):
    a) Verify that this card is the Inact unit.
  2) At the TRANSFER map level:
    a list of available patches is displayed.
    For each patch to be transferred:
    a) SELECT the patch by number
    b) FETCH the patch to BOTH units
  3) At the PATCH map level:
    For each patch to be applied and committed:
    a) SELECT the patch by number
    b) APPLY INA - apply the patch on Inactive only
    c) SELECT the patch by number
    d) COMMIT INA - commit the patch on Inactive only
Type GO to continue the SWUPGRADE when above steps are successfully comple
Step PATCH_NEW_SIDE_BLADE is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2** Refer to Patching the CS 2000 Compact on page 1778 for assistance with the platform software patching procedure.

**3** After patching is complete, or if no patches are available, type **GO** and press the Enter key.

*Step PATCH_NEW_SIDE_BLADE completes.*

*Step MATELINK_RTS runs and completes. This step verifies the communication path between the active call processing application and the upgraded, inactive call processing application.*

*Step UPDATE_STEPS_AND_VARS runs and completes. This step automatically provisions environment variables and updates the list of steps on the inactive call processing application. The active and inactive call processing application data for the ONP is synchronized.*

*Step CHECK_NEW_LOAD runs and completes. This step verifies that the inactive call processing application on the inactive Call Agent has no datafill. The software verifies that this load has no datafill by checking that table TERMDEV has a single tuple.*

*Step SET_DATE_AND_LOGMSG runs and completes. This step sets the inactive side time and date from the active side. The login message is set from variable INACT_LOGMSG.*

*Step CHECK_LOGS_2 runs and completes. This step displays the count of logs in the LOGUTIL buffer since the start of the process. The log report types displayed are determined by the variable LOGS.*

*Step CLEAR_TRAPINFO runs and completes. This steps clears all traps on the upgraded inactive call processing application. By clearing the traps now, it is easier to differentiate between old and new traps that are caused by subsequent steps.*

*Step TRANSFER_DEVICES_INFO runs and completes. This step copies data from variable VERIFY_DEVICES on the active call processing application to the inactive call processing application.*

*If the CS 2000 - Compact is configured with Message Controllers, step MS_CHECK runs. This step checks that the software load in the Message Switch is the correct load for the upgraded call processing application load.*

*Step DISABLE_AUTOIMAGE runs and completes. This step disables the automatic image dump process since the automatic image dump process could interfere with the ONP.*

*Step SET_OFFICE_TUPLES runs and completes. This step retains the current state of office parameters NODEREXCONTROL, LCDREX_CONTROL, and GUARANTEED_TERMINAL_CPU_SHARE and then sets both NODEREXCONTROL and LCDREX_CONTROL to OFF. GUARANTEED_TERMINAL_CPU_SHARE is set to its maximum value.*

*Step SET_PADNDEV runs and completes. This step saves the tuples in table PADNDEV, deletes all the tuples, and then adds tuples according to variable PADNDEVS.*

*Step SEND_PATCHES runs and completes. This step copies the patch files for the upgraded inactive call processing application from the location specified by variable PADNDEVS to the inactive call processing application.*

*Step APPLY_PATCHES runs and completes. The patches that were copied in step SEND_PATCHES are applied.*

*Step CHECK_LOGS_3 runs and completes. This step displays the count of log reports stored in the LOGUTIL buffer.*

*Step RESTORE_PADNDEV runs and completes. This step restores table PADNDEV to contain the exact tuples it contained before step SET_PADNDEV.*

**4** Proceed to TABLE_TRANSFER.

# TABLE_TRANSFER

This step copies table provisioning data from the active call processing application to the undatafilled, inactive call processing application.

Step TABLE_TRANSFER is automated. Manual intervention is needed only if some of the table data fails to transfer. The table transfer stops according to variables STOPIF and LIMIT.

For any failed tables, compare the old, active side data to the new, inactive side data to identify and correct any tuples. If necessary, contact your translations engineer or Nortel Networks support personnel for assistance.

For some offices, it may be necessary or preferred to change office variables and parameters on the inactive side after this step completes. One possible parameter to change is field LOG_OFFICE_ID in table OFCVAR. Change this parameter after TABLE_TRANSFER completes and before step START_PRESWACT. Use the procedure below for logging into the inactive call processing application.

**ATTENTION**

If it is necessary to access the inactive call processing application to correct a problem, use the following procedure.

If it is necessary to abort the upgrade at this point, issue the CANCEL command at the ACTIVECM window.

### *At the INACTIVECM window*

1 Log in to the active call processing application by telnetting to the CS 2000 Core Manager as user cmusr.

2 Enter the mate input/output level and log in to the inactive call processing application:

```
>MATEIO;MATELOG ME;SLEEP 240 MINS
```

***Note 1:*** The `Mate>` prompt indicates that the command is sent to the inactive call processing application.

***Note 2:*** If the **MATELOG ME** command fails, enter **MATELINK RTS** and retry the **MATELOG ME** command.

```
>mateio
MATEIO -- MATECOM link not available. Attempt RTS.
>matelink rts
RTS PASSED
```

3 At the Mate> prompt, log in to the inactive call processing application:

**Mate> username password**

4 Use the table editor to correct any datafill problems.

5 Use the LOGOUT command at the Mate> prompt to exit the inactive call processing application:

**Mate> LOGOUT**

***Note:*** Do not log out of the active call processing application. Verify that the prompt is the Mate> prompt.

***At the ACTIVECM window***

6 Type **GO** and press the Enter key to continue.

*Step TABXFR_REPORT runs and completes. This step prints a report of all table failures to the trace device.*

*Step CHECK_LOGS_4 runs and completes.*

7 Proceed to START_PRESWACT.

## START_PRESWACT

Step START_PRESWACT has several sub steps. If any sub step fails to complete, make corrections according to the error message and continue the START_PRESWACT step by typing **GO** and pressing the Enter key. START_PRESWACT re-executes the failed step and continues.

Read the following notes while step START_PRESWACT executes:

START_PRESWACT sub step TABLE_DELTA displays the changes, additions, and deletions between the old and new call processing application software loads for the following tables:

- OFCENG
- OFCSTD
- OFCVAR
- OFCOPT
- DATASIZE
- TCAPTRID
- OPTCTL

For any tables with differences, compare the OLD/NEW and ADDED tuples to identify and correct any errors.

> ***Note:*** Errors stop sub step TABLE_DELTA from completing with the message "`TABLE_DELTA not complete`." The software also provides informative messages such as "Table ATTCONS Checksum incorrect, keys match." The informative messages do not stop the step from completing and do not require any manual action. At a convenient point during the upgrade, compare the old and new loads to understand and validate the differences.

If office parameter changes were made after step TABLE_TRANSFER on the inactive call processing application, then TABLE_DELTA displays the change.

Proceed to PRESWACT_DIRP_AND_BILLING.

# PRESWACT_DIRP_AND_BILLING

***SDE — At the ACTIVECM window***

**1** Step PRESWACT_DIRP_AND_BILLING runs and completes, but pauses the process. The CS 2000 - Compact requires no manual action for DIRP and billing.

```
Starting step PRESWACT_DIRP_AND_BILLING.

       MTD Billing subsystem information
       ---------------------------------
MAPCI:
MTC:
IOD:
DIRP:
MTD  TapeName  Status    IOC.CARD/PORT

        TRANSFERING table DIRPPOOL to inactive side.
        ----------------------------------------.
ACT - WARNING: If any DIRP actions other than those described in this step
               occur between now and SWACT, the user may need to manually
               correct any discrepancies in table DIRPPOOL.
D/R DART#     689 ->              DIRPPOOL : Restored       7 , Failed   0

        To prepare DIRP billing subsystems for the SWACT, please follow
        instructions in the NTP 'One Night Process Software Dellivery Pro-
cedure's.
        This verifies that all DIRP billing subsystems have been properly
        prepared for the upcoming SWACT and DIRP information is readily
available
       for timely restoration to minimize the loss of existing data, should
DIRP
        file storage devices become corrupted during the transition.

        These measures may include, but are not limited to:

           - DIRP rotation of disk primary billing.
           - DIRP rotation of tape primary billing.
           - close existing DPP billing file and open a new one.
           - prepare tape billing standby volumes.
           - prepare tape parallel standby volumes.
           - copy unprocessed disk billing file to backup tape.
           - copy disk parallel files to backup.
           - match DIRPPOOL volumes between active and inactive.
Step PRESWACT_DIRP_AND_BILLING is complete.
The SWUPGRADE process has paused. Enter GO.
```

2 Type **GO** and press the Enter key to confirm PRESWACT_DIRP_AND_BILLING.

*Step PRINT_SPMS_INDICES runs and completes.*

3 Step GET_FIRST_SWACT_AGREEMENT begins and pauses the process. The SDE must receive agreement from the customer to proceed with the SWACT.

***Note:*** If a delay of longer than 15 minutes is expected before the SWACT, the SDE should wait until all preparations are made before continuing.

```
Starting step GET_FIRST_SWACT_AGREEMENT.
NORESTARTSWACT will be used for initiating a CC Warm SWACT.
Do you wish to proceed with the preparation for the CC warm swact?
Step GET_FIRST_SWACT_AGREEMENT is complete.
The SWUPGRADE process has paused. Enter GO.
```

4 Type **GO** and press the Enter key to confirm GET_FIRST_SWACT_AGREEMENT.

5 Step PREPARE_FOR_SWACT begins.

```
Starting step PREPARE_FOR_SWACT.
DISPLAY_NOP_USERS                executing
SESSION  STATE  APPL.   ID      NODE
   0     IDLE
   1     IDLE
         2     IDLE
         3     IDLE
         4     IDLE
         5     IDLE
         6     IDLE
         7     IDLE
         8     IDLE
         9     IDLE
        10     IDLE
        11     IDLE
        12     IDLE
        13     IDLE
        14     IDLE
DISPLAY_NOP_USERS                      complete
        Please perform the following:
           - Remind the Telco personnel to inform 'active' NOP users
             listed above (if any) to log out of their session(s)
             before the S/W upgrade can continue.
           - Remind the Telco personnel to contact the high profile
             customers to ensure that they are not in emergency call
             processing mode and inform them of the approximate SWACT
             time.
           - Disable all polling and periodic testing. There is to
             be no activity on the Core, MS and CLOCK until cleared
             by the software delivery engineer.

             WARNING: FAILURE TO COMPLY MAY RESULT IN A SYSTEM RESTART.

           - Ensure no further activity is performed on the DPP,
             including DPP polling or disk backup, and inform the
             downstream processing center.
           - Dump all special logs so they can be restored onto the
             new load after postswact has completed.

Step PREPARE_FOR_SWACT is complete.
The SWUPGRADE process has paused. Enter GO.
```

6 Type **GO** and press the Enter key to confirm PREPARE_FOR_SWACT.

*Step STATUSCHECK runs and completes.*

*Step CHECK_LOGS_5 runs and completes.*

*Step TRANSFER_TIMINGS runs and completes.*

7 Proceed to SWACT.

# SWACT

***SDE — At the ACTIVECM window***

**1** Review the instructions for step SWACT.

```
Starting step SWACT.
Confirm that the Inactive CA Application is NOT JAMmed,
-or- RELEASE the JAM and confirm when complete:
At the Active TPCMTC MAP; CAMtc Level:
       1) RELJAM - Release the Jam on the Inactive application
Type GO to confirm, and to continue the SWUPGRADE
Step SWACT is not complete.
The SWUPGRADE process has paused. Enter GO.
```

***SDE — At the CORE0 or CORE1 window***

**2** Confirm that inactive Call Agent is not jammed or release the jam.

***SDE — At the ACTIVECM window***

**3** Type **GO** and press the Enter key to continue with the SWACT.

*The process performs final checks and pauses for a final NORESTARTSWACT confirmation.*

```
Beginning SWACT checks:
All the SWACT checks have finished successfully.

The VR_PRESWACT_TRANSFER step completed successfully.
All INSV and ISTB series 1 PMs will have execs loaded after the SWACT.

****************** FINAL SWACT CONFIRMATION *****************
Do you wish to proceed with the NORESTARTSWACT CC warm swact?
Step SWACT is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**4** Receive final agreement from the telephone operating company personnel to proceed with the SWACT. Type **GO** and press the Enter key once confirmation is received.

5 Monitor the messages printed to the terminal and verify that activity does switch at the CORE0 or CORE1 windows.

```
Starting step SWACT.
After the completion of the CC warm swact, please log
both the TRACE user and the ACT user
onto the new active side and enter SWUPGRADE;GO.
All Pre-SWACT checks completed. Starting Warm SWACT now.
********        The cursor will not be returned  ********
********       unless a critical failure occurs. ********
******** Now monitoring Warm SWACT messages.********

Pre-initialization done

Communication established

Exchange of data with the mate done

Transfer of data done (FASPECT)

Data estimation done

Store allocated on active CC

Store allocated on inactive CC

AMA processing completed

         SWACT Inactive Procs running, this may take a few minutes

Before_callp_stopped procs completed

Call processing in PM stopped

Call processing I/O in CC stopped

Call data extracted

Data transfer completed
```

*Activity switches to the upgrade call processing application. The connection at the ACTIVECM window is dropped.*

6 Log in to the upgraded call processing application by telnetting to the CS 2000 Core Manager or CBM as user cmusr from the ACTIVECM and INACTIVECM windows.

***Note:*** The switch provides a prompt to perform test calls after step RECOVER_DIRP_AND_BILLING.

**7** Continue the software upgrade.

```
> SWUPGRADE;GO
```

**8**

**ATTENTION**

Instruct the operating company to perform a 911 test call. If the test call fails to complete, contact Nortel Networks Emergency Recovery immediately. **Do not continue.** If the test call is successful, continue with the software upgrade and ensure the following actions take place:

— system recovery of all DIRP and billing subsystems

— system recovery of any critical alarms

— operating company begins test calls

— system logs are monitored for office stability

*Tracing begins and the software upgrade continues.*

*Step DISPLAY_DATE completes.*

*Step RECOVER_DIRP_AND_BILLING begins.*

```
2002/07/08 09:52 INACT_LOGMSG
>SWUPGRADE;GO
SWUPGRADE:
This device is selected for TRACEing
Variable TRACE_DEVICE has been set to TELNSVR00001.

Starting step DISPLAY_DATE.
Date: 2002/07/08, Time: 10:18:17
Finished step DISPLAY_DATE.

Starting step RECOVER_DIRP_AND_BILLING.

 To recover DIRP billing subsystems after the SWACT, please follow
 instructions in the NTP 'One Night Process Software Delivery Procedures'.

 This verifies that all DIRP billing subsystems have properly recovered
 from the SWACT.

 Check these devices for proper operation.

 The DIRP increment of the IOD MAPCI level provides a QUERY command to
 verify the resulting disposition of these subsystems (i.e. QUERY AMA)
 and the DPP increment of the IOD MAP level allows the applicator to
 display the alarm status for the DPP active and standby units (command
 ERRMAP ALARMS) and also provides the ability to list DPP active files
        (command LSTACT).
Step RECOVER_DIRP_AND_BILLING is complete.
The SWUPGRADE process has paused. Enter GO.
```

Determine the next action.

| If | Do |
|---|---|
| reversion to the old call processing application load is required | Type **CANCEL**, press the Enter key, and refer to "Revert and Abort" in *Upgrading the Call Agent*, NN10065-461 |
| reversion is not required | step 9 |

**9** No manual action is required for step RECOVER_DIRP_AND_BILLING. Type **GO** and press the Enter key.

*Step RECOVER_DIRP_AND_BILLING completes.*

*Step PERFORM_TEST_CALLS_1 begins.*

**10** Have telephone operating company personnel perform test calls while the software upgrade process pauses 20 seconds.

```
Starting step PERFORM_TEST_CALLS_1.
   AMAB has been added to the LOGS variable for
   automatic monitoring during the execution of the
   test calls for possible AMA test call failures.

        Please perform the test calls that were identified ahead of
        time and documented in the test file scripts.

        WARNING: If an abort becomes necessary due to critical test
                 failures, refer to the 'Revert to the old load'
                 procedure described in the ONP MOP.

        The AutoONP process will continue in 20 seconds.

Finished step PERFORM_TEST_CALLS_1.
```

**11** Determine the next action.

| If | Do |
|---|---|
| reversion to the old call processing application load is required | Type **CANCEL**, press the Enter key, and refer to “Revert and Abort” in *Upgrading the Call Agent,* NN10065-461 |
| reversion is not required | proceed to START_POSTSWACT on page 1192 |

# START_POSTSWACT

Step START_POSTSWACT is automated and runs many substeps. The automated process stops at step PERFORM_TEST_CALLS_2.

***SDE — At the ACTIVECM window***

**1** Monitor the progress of step START_POSTSWACT.

*Step START_POSTSWACT completes.*

*Step RESTART_OLD_LOAD runs and completes. This step performs a restart on the old call processing application software to verify that the old call processing software can accept activity in the event of software reversion.*

*Step PERFORM_TEST_CALLS_2 begins.*

```
Finished step START_POSTSWACT.

Starting step RESTART_OLD_LOAD.
Finished step RESTART_OLD_LOAD.

Starting step DRTIME_PRINT.
A DRTIME PRINT was not requested.
Finished step DRTIME_PRINT.

Starting step PERFORM_TEST_CALLS_2.
        If not already done, please perform test calls.
        WARNING: If an abort becomes necessary due to critical test
                 failures, refer to the 'Revert to the old load'
                 procedure described in the ONP MOP.
Step PERFORM_TEST_CALLS_2 is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2**

**ATTENTION**

Do not proceed to step LOAD_OLD_SIDE_BLADE until the test calls complete successfully. Once the old side Call Agent card is locked, normal abort is not supported.

Receive confirmation from the telephone operating company to proceed with the software upgrade.

Have operating company personnel perform test calls.

| If | Do |
|---|---|
| reversion is required | Type **CANCEL**, press the Enter key, and refer to “Revert and Abort” in *Upgrading the Call Agent*, NN10065-461 |
| reversion is not required | step 3 |

3 Type **GO** and press the Enter key to continue the upgrade.

4 Proceed to LOAD_OLD_SIDE_BLADE.

# LOAD_OLD_SIDE_BLADE

***SDE — At the ACTIVECM window***

**1** Review the instructions printed to the terminal.

```
Starting step LOAD_OLD_SIDE_BLADE.
ACT - WARNING: The revert to the old load is not possible after the
ACT - WARNING: Old Side Call Agent card has been Locked.
Are you ready to continue?.
Type GO to continue the SWUPGRADE.
Step LOAD_OLD_SIDE_BLADE is not complete.
The SWUPGRADE process has paused. Enter GO.
```

Type **GO** and press the Enter key.

**2** Review the instructions printed to the terminal.

```
Starting step LOAD_OLD_SIDE_BLADE.
Upgrade the Old Side Call Agent load at the SAM21 EM GUI
by using the following manual procedure:
  1) At Active COREMTC MAP (ccamtc coremtc), query the Inact blade IP addr
     a) Use QueryIP command to determine IP address of mate blade.
       2) At SAM21 EM GUI, open Card View for Inact Call Agent Card:
          a) Under the Provisioning Tab, determine IP address of the card.
          b) Ensure IP address in GUI matches inactive card IP address.
       3) Under the States Tab, Lock the card
       4) Under the Provisioning Tab, change the boot file:
          a) Click Modify.
          b) Change boot file name to new load.
          c) Click Save.
       5) Under the States Tab, Unlock the card
          a) Monitor the boot progress in the History pane.
       6) At Active COREMTC MAP, monitor Inact load initialization:
          a) Inact status begins with "/booting"
          b) Wait until the status becomes "/waiting"
      7) At Inact COREMTC map (ccamtc coremtc), Validate newly booted load
          a) Telnet/Login to the Inact Blade
         b) Under the Sys level, QryLD must indicate the new load version
Type GO to continue the SWUPGRADE when above steps are successfully com-
pleted
Step LOAD_OLD_SIDE_BLADE is not complete.
The SWUPGRADE process has paused. Enter GO.
```

For assistance, refer to the following procedures:

- “Call Agent Lock” in *Upgrading the Call Agent,* NN10065-461
- “Reprovision Call Agent platform load” in *Upgrading the Call Agent*, NN10065-461
- "Call Agent Unlock" in *Upgrading the Call Agent*, NN10065-461

***Note:*** If CallAgent C_MisM alarm is active at the CORE0 or CORE1 window, patch the platform software:

1. At the inactive maintenance window (CORE0 or CORE1) verify that this is the inactive Call Agent.
2. Enter the Admin level and then the SWIM level.
3. At the TRANSFER level a list of available patches is displayed
   a. SELECT the patch by number
   b. FETCH INA the patch to the INACTIVE unit
4. At the PATCH level, for each patch to be applied and committed:
   a. SELECT the patch by number
   b. DISADMIN the patch and follow any special instructions
   c. APPLY INA the patch to the INACTIVE unit
   d. SELECT the patch by number
   e. COMMIT INA the patch to the INACTIVE unit

**3** Type **GO** and press the Enter key to complete step LOAD_OLD_SIDE_BLADE.

*Step LOAD_OLD_SIDE_BLADE completes.*

**4** Continue to procedure FINISH_POSTSWACT on page 1196.

# FINISH_POSTSWACT

*The events in the following procedure occur after Step LOAD_OLD_SIDE_BLADE completes.*

***SDE — At the ACTIVECM window***

**1** *Step SYNC_SWITCH begins.*

```
Starting step SYNC_SWITCH.
SWUPGRADE has now reached the SYNC_SWITCH step.
Are you ready to SYNC the switch?
Step SYNC_SWITCH is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2** Type **GO** and press the Enter key.

*Step SYNC_SWITCH completes. Optionally, monitor the synchronization from the CORE0 or CORE1 windows.*

*Step FINISH_POSTSWACT runs and completes. This step executes any remaining POSTSWACT steps. Several reports about the software upgrade are printed to the terminal. If a step fails to complete, follow the instructions given; type **GO** and press the enter key to continue.*

*Step RESTORE_PARMS runs and completes. This step restores the office parameters NODEREXCONTROL, LCDREX_CONTROL, GUARANTEED_TERMINAL_CPU_SHARE, and DUMP_RESTORE_IN_PROGRESS that were saved in step PRINT_PARMS_AND_SAVE.*

*Step RESET_DEVICES runs and completes. This step verifies that all devices used during the software upgrade are set to their original values.*

*Step COMPLETE_NEW_LOAD_INIT runs and completes. This step prints messages as a reminder to SITE that need to be performed after POSTSWACT is complete.*

```
Starting step COMPLETE_NEW_LOAD_INIT.

        1) Re-input any data changes made prior to the software
           update but not captured on journal file, if any.

        2) Notify NOP end users to log back in.

        3) Reassign all current PROFILE information (LOGIN or
           RESTART) in SFDEV.

        4) Restore any special logs (listreps special).

        5) Reassign any temporary log ROUTING setup via LOGUTIL.

        6) Reassign any changes in the INTEG level of the MAP
           (for example, UPTH, BUFFSEL, FILTER and others).

        7) If Network Management code blocking was removed earlier, have
           Network Maintenance personnel restore code blocking active.

Step COMPLETE_NEW_LOAD_INIT is complete.
The SWUPGRADE process has paused. Enter GO.
```

***SITE — At the ACTIVECM window***

**3** Perform any actions specified in step COMPLETE_NEW_LOAD_INIT.

***SDE — At the ACTIVECM window***

**4** Type **GO** and press the Enter key to complete step COMPLETE_NEW_LOAD_INIT.

*Step COMPLETE_NEW_LOAD_INIT completes.*

*Step RESET_LOGIN_BANNER runs and completes. This step erases the software upgrade banner.*

*Step DUMP_NEW_LOAD runs and completes.*

*Step RESUME_REX_TEST runs and completes.*

*Step START_JOURNAL_FILE runs and completes.*

*Step PRINT_SWUPGRADE_REPORT runs and completes. This step prints the start and stop time for each step in the software upgrade.*

*Step STOP_RECORD runs and completes.*

*Step UPGRADE_COMPLETE begins.*

```
Starting step UPGRADE_COMPLETE.
   Process complete. You may now QUIT out of the SWUPGRADE increment.
Finished step UPGRADE_COMPLETE.

SWUPGRADE Process complete - all steps have been executed.
>QUIT
CI:
```

**5** Type **QUIT** and press the Enter key.

**6** The Call Agent software upgrade is complete.

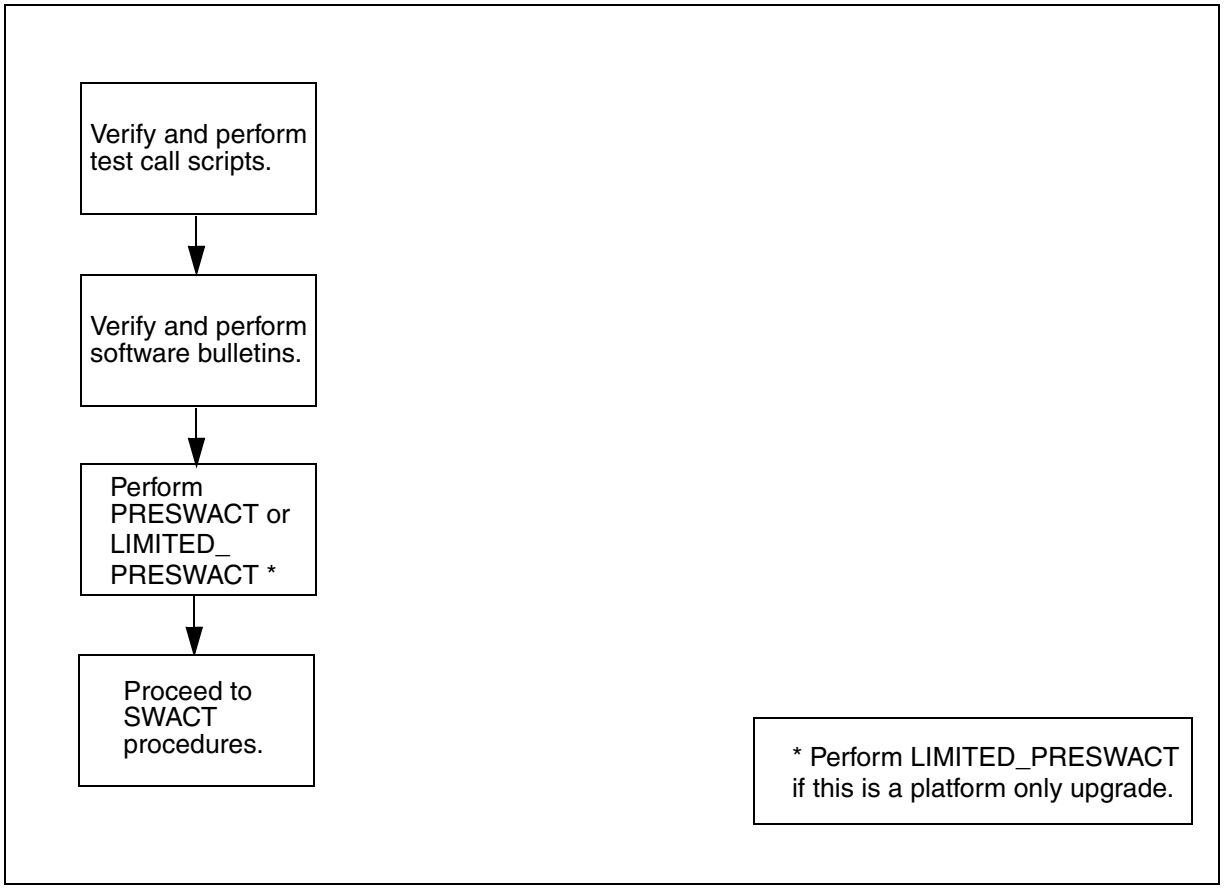
# PRESWACT/LIMITED_PRESWACT

These procedures do not apply to the automated upgrade with the SWUPGRADE tool.

**ATTENTION**
Operating company site personnel should complete test call scripts at this point of the procedure. Any calling irregularities must be identified and addressed to avoid unnecessary troubleshooting after the Switch of Activity (SWACT).

Perform procedures in this section to verify software stability and prepare for the SWACT.

## PRESWACT



## Verify and perform test calls

***SITE — At the ACTIVECM window***

**1** Make sure all emergency services are functioning.

**2** Refer to the Test Call Scripts and perform the required test calls.

**3** This procedure is complete.

Determine the next action.

| If | Do |
|---|---|
| abort is required | proceed to “ABORTSWACT” in *Upgrading the Call Agent,* NN10065-461 |
| abort is not required | continue |

# Verify and perform software bulletins

***SDE — At the ACTIVECM window***

**1** At this time, verify and perform any applicable software delivery bulletins and notices before proceeding.

**2** This procedure is complete.

# Perform LIMITED_PRESWACT

This procedure is used for a platform only MR upgrade. For an ONP, Nortel Networks supports the SWUPGRADE process.

LIMITED_PRESWACT executes a series of steps required before the office switch of activity (SWACT). If a step fails to complete, LIMITED_PRESWACT stops and gives additional information. Whenever LIMITED_PRESWACT stops, use the information given to investigate and correct the problem. All LIMITED_PRESWACT steps must be completed before SWACT.

***At the MAP***

**1** Execute LIMITED_PRESWACT:

```
> BCSUPDATE; LIMITED_PRESWACT
```

*The LIMITED_PRESWACT command presents a warning:*

```
Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
```

**2** Confirm the warning with a **Y**.

*A series of steps execute and complete. LIMITED_PRESWACT stops at step MATE_RESART_RELOAD:*

```
MATE_RESTART_RELOAD                executing
There are users still logged on the Inactive. Do
you wish to continue?
MATE_RESTART_RELOAD                not complete
ACT - Error: Restart aborted. Type
LIMITED_PRESWACT to continue
Investigate and correct if needed.
```

**3** Reenter LIMITED_PRESWACT to continue:

```
> LIMITED_PRESWACT
```

*Another warning is printed:*

```
MATE_RESTART_RELOAD                executing
There are users still logged on the Inactive. Do
you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
```

**4** Confirm the warning with a **Y**.

*The inactive unit indicates* `/restart` *at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated as follows:*

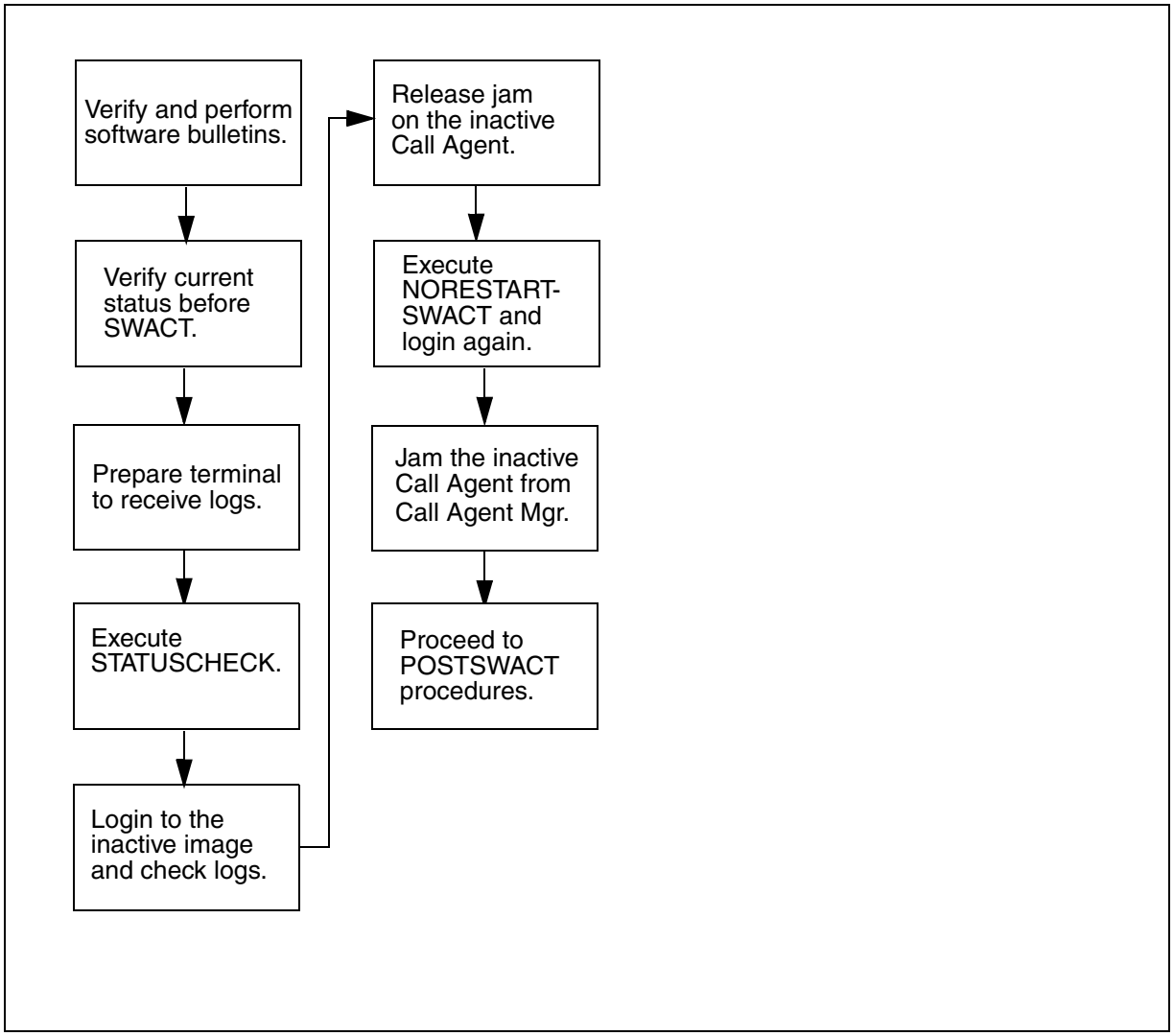
```
Total execution time for all complete procedures
00:07:31.362
All LIMITED_PRESWACT steps completed
successfully.
```

**5** This procedure is complete.

# SWACT

Perform procedures in this section to execute a switch of activity (SWACT) to the new software.

## SWACT



# Verify and perform software bulletins

***SDE — At the ACTIVECM window***

**1** At this time, verify and perform any applicable software delivery bulletins and notices before proceeding.

**2** This procedure is complete.

# Verify correct status before SWACT

***SITE — At the ACTIVECM window***

**1**

> **ATTENTION**
> Do not proceed until operating company personnel and Nortel Networks support personnel agree to proceed.

Contact high-profile customers and customers with essential services to verify they are not in emergency call processing mode.

***Note:*** These customers include, but are not restricted to, the police and emergency bureaus, hospitals, and radio stations.

**2** Contact dynamic network control (DNC) users, if any, and make sure they log out.

**3** Disable all polling and periodic testing.

***Note:*** Polling or periodic testing on the Call Agent or clock can cause a system restart. Cease all polling and periodic testing until the software delivery engineer lifts this restriction.

**4** Take REGISTER readings as required by the Service Provider.

**5** Dump Switch Performance Monitoring System (SPMS) register information to a printer.

**6** This procedure is complete.

# Prepare terminal to receive logs

***SDE — At the ACTIVECM window***

**1** Stop the log device.

```
> LOGUTIL;STOP
> DELDEVICE <device>
```

**device**
is the device name to which logs are routed

**2** Add log reporting to the device.

```
> ADDREP <device> SWCT
```

**3** Begin logging to the device.

```
> START
```

or

```
> STARTDEV <device>
```

if the device is not the screen terminal

**4** Exit the log utilities level.

```
> LEAVE
```

**5** This procedure is complete.

# Run STATUSCHECK

***SDE — At the ACTIVECM window***

**1** Run the status check.

```
> BCSUPDATE;SWACTCI;STATUSCHECK
```

***Note 1:*** STATUSCHECK may cause a restart on the inactive side.

***Note 2:*** The Service Provider is responsible for changing device states on the active side, as required, during this upgrade process and restoring them on completion of the process. The software delivery engineer is responsible for the device states on the inactive side.

**2** Verify the status check passes and both sides match.

**3** This procedure is complete.

# Check logs inactive

***SDE — At the INACTIVECM window***

**1** Enter the BCS update level.

```
Mate> BCSUPDATE
```

**2** Check the logs.

```
Mate> LOGCHECK
```

**3**

**ATTENTION**
Do not proceed until all log activity is explained.

Print trap information for the inactive side if a trap is detected while running the LOGCHECK command.

```
Mate> TRAPINFO
```

If a trap occurred, capture the full trap information.

```
Mate> TRAPINFO <trap_no>
```

**trap_no**
is the number of the trap

**4**

**ATTENTION**
Determine the significance of any traps. Do not proceed until all traps are understood.

Clear the trap information.

```
Mate> TRAPINFO CLEAR
```

Confirm the command.

**5** This procedure is complete.

# Release jam on the inactive Call Agent

***At the active Call Agent Manager***

**1** Enter the RelJam command:

```
> CoreMtc
> CAMtc
> RelJam
```

```
 CallAgent       SYS       CON       APPL              Unit: 0
    .             .         .       simplx
                                       M
CAMtc                        Jam:  Link0:  Link1: BLnk: FC: Appl:
 0 Quit       Unit0  Act     no     . Inact . Act     .    .   nosync .
 2 Jam        Unit1  Inact   no     . Inact . Act     .    .   nosync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh    RelJam:   Release jam on the inactive unit.
  mtc
Time  10:38  >
```

**2** This procedure is complete.

# Execute NORESTARTSWACT

**CAUTION**
**Possible loss of service**
NORESTARTSWACT does not check if the inactive Call Agent is unjammed. If the inactive Call Agent is jammed and a NORESTARTSWACT is requested, service is affected. Verify that the inactive Call Agent is not jammed.

**CAUTION**
**Possible loss of service**
Use the Call Agent Manager to verify that the inactive Call Agent does not have any critical alarms. A critical alarm causes the NORESTARTSWACT to fail.

***At the MAP***

**1** Check status:

```
> BCSUPDATE;SWACTCI;STATUSCHECK
```

*Success is indicated as follows:*

```
SWACTCI:
Checking Nodes Status
STATUSCHECK successful
```

**2** Execute the NORESTARTSWACT:

```
> NORESTARTSWACT
```

***Note 1:*** Only simple two-port and echo calls that are in a stable talking state (that is, not in a transition state such as dialing) survive a CC WarmSWACT. Survival means that the call is kept up until the next signaling message is received (usually, for example, a terminate message, but on any other message as well, such as an attempt to use the conference feature).

***Note 2:*** Attendant Consoles will be in night service after the SWACT if the INSV field is set to Y in table ATTCONS (Attendant Consoles).

*Progress is printed and the process stops to verify that the inactive Call Agent is not jammed:*

```
Beginning SWACT checks:
All the SWACT checks have finished successfully.
The VR_PRESWACT_TRANSFER step completed
successfully.
All INSV and ISTB series 1 PMs will have execs
loaded after the SWACT.
Device Checking Status:
NOMATCH option is set to OFF <default setting>.
Device matching during CC WARM SWACT Enabled.
Do you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
>
```

**3** Confirm the warning with a **Y** if the only alarm is an APPL simplx.

*The final progress follows. Activity also switches at the Call Agent Manager.*

```
Please confirm ("YES", "Y", "NO", or "N"):
>Y
All Pre-SWACT checks completed. Starting Warm
SWACT now.
*****   The cursor will not be returned  *****
*****  unless a critical failure occurs. *****
***** Now monitoring Warm SWACT messages.*****

Pre-initialization done
Communication established
Exchange of data with the mate done
Transfer of data done (FASPECT)
Data estimation done
```

**4** The telnet sessions to the active and inactive call processing applications are lost. Reestablish the connection. Refer to the Upgrading the CS 2000 Compact in this Upgrades document for procedures.

5 This procedure is complete.

**ATTENTION**
**ABORT PROCEDURE**

Reversion to the previous software release is possible until procedure Lock the inactive Call Agent. If this is a PCL upgrade with the SWUPGRADE tool, reversion is started with the CANCEL command. If this is a platform only MR upgrade, refer to “ABORTSWACT” in *Upgrading the Call Agent*, NN10065-461.

# Jam the inactive Call Agent

***At the active Call Agent Manager***

**1** Enter the Jam command:

```
> CoreMtc
> CAMtc
> Jam
```

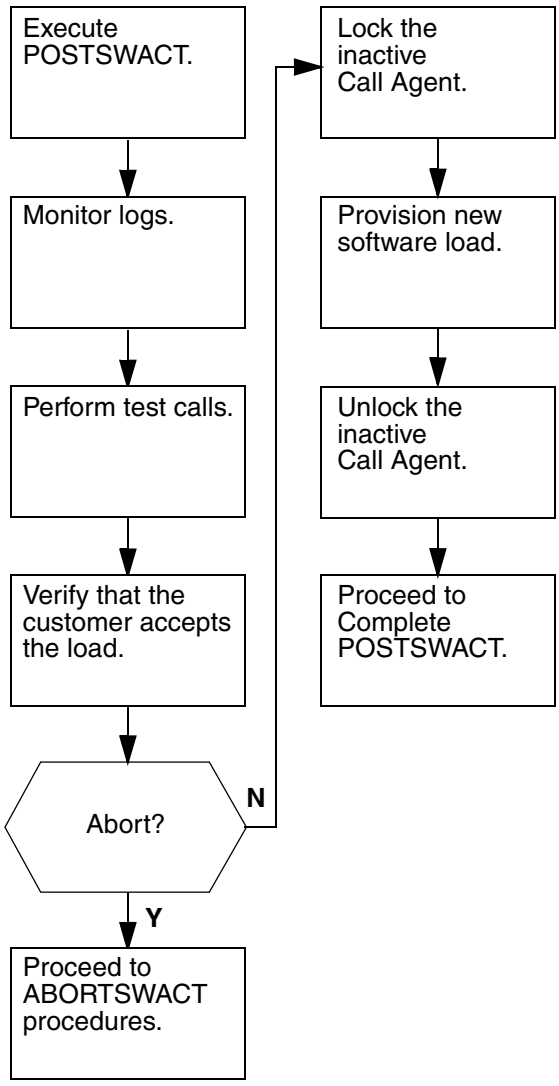
```
 CallAgent       SYS       CON       APPL              Unit: 1
  JInact          .         .       simplx
                                      M
CAMtc                        Jam:  Link0:  Link1:  BLnk: FC: Appl:
 0 Quit       Unit0  Inact  yes    . Inact . Act     .    .   nosync .
 2 Jam        Unit1  Act    no     . Inact . Act     .    .   nosync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16           Jam:      Jam the inactive unit, to prevent it taking activity.
17 Help                 Parms: [FORCE]
18 Refresh                 FORCE     - bypass system stability checks
  mtc
Time  10:38  >
```

**2** This procedure is complete.

# Start POSTSWACT

Perform the procedures in this section to verify the stability of the new platform software load.

### Start POSTSWACT procedure



# Execute POSTSWACT

***At the MAP***

**1** Execute POSTSWACT:

```
> BCSUPDATE;POSTSWACT
```

*POSTSWACT begins, steps execute, and complete. POSTSWACT stops at step BEGIN_TESTING:*

```
REACTIVATE_TRIGASGN                executing
REACTIVATE_TRIGASGN                   complete

DIRP_RECOVERY                      executing
DIRP_RECOVERY                      complete
...
BEGIN_TESTING                      executing
BEGIN_TESTING                      complete
Enter Postswact after office testing has been
completed
```

**2** Proceed to Monitor logs on page 1217 and Test calls and acceptance on page 1219 before reentering the **POSTSWACT** command on page 1226.

# Monitor logs

***At the inactive MAP***

1 Log in to the mate image, refer to How to log in to the mate image.

2 Review previous log reports:

```
> LOGUTIL;OPEN SWCT;BACK ALL
```

3 Set the terminal to receive logs:

```
> LOGUTIL;START;QUIT
```

or

```
> STARTDEV <device>
```

**device**
is a different terminal device

4 Let logs run for 30 minutes and then run LOGCHECK:

```
> LOGUTIL;STOP;QUIT
> BCSUPDATE;LOGCHECK;QUIT
```

5 When LOGCHECK completes. Set the terminal to receive logs again.

6 This procedure is complete.

## How to log in to the mate image

***At the MAP***

1 Use MATELINK, MATIO, and MATELOG to log in.

```
> MATELINK RTS
> MATEIO
> MATELOG ME; SLEEP <nn> MINS
```

**nn**
is the number of minutes to sleep. Allow at least 30 minutes.

2

**ATTENTION**
While logged into the inactive call processing application, the system prompt changes to `Mate>`.

Log in to the inactive call processing application with a username and password.

3 This procedure is complete.

## Test calls and acceptance

***At the MAP***

1 Make sure all emergency services are functioning.

2 Refer to the Test Call Scripts and perform the required test calls.

3 Confirm that the customer accepts the new load.

4 This procedure is complete.

Determine the next action.

| If | Do |
|---|---|
| abort is required | proceed to “ABORTSWACT” in *Upgrading the Call Agent*, NN10065-461 |
| abort is not required | set the boot file pointer, as described below, and then proceed to Lock the inactive Call Agent on page 1220 |

Take an image dump.

Set the boot file pointer to the new software load if this was not done when the software was transferred to storage.

***At the MAP***

1 Dump the new call processing application image.

```
> AUTODUMP MANUAL
```

*or*

```
> DUMP MANUAL image_name disk_vol ACTIVE UPDATE
```

2 Enter the ITOCCI level.

```
> ITOCCI
```

3 Set the boot file pointer to the new software load.

```
> SA CM image_name
```

**image_name**
is the name of the new call processing application image from step 1

4 This procedure is complete.

# Lock the inactive Call Agent

**ATTENTION**

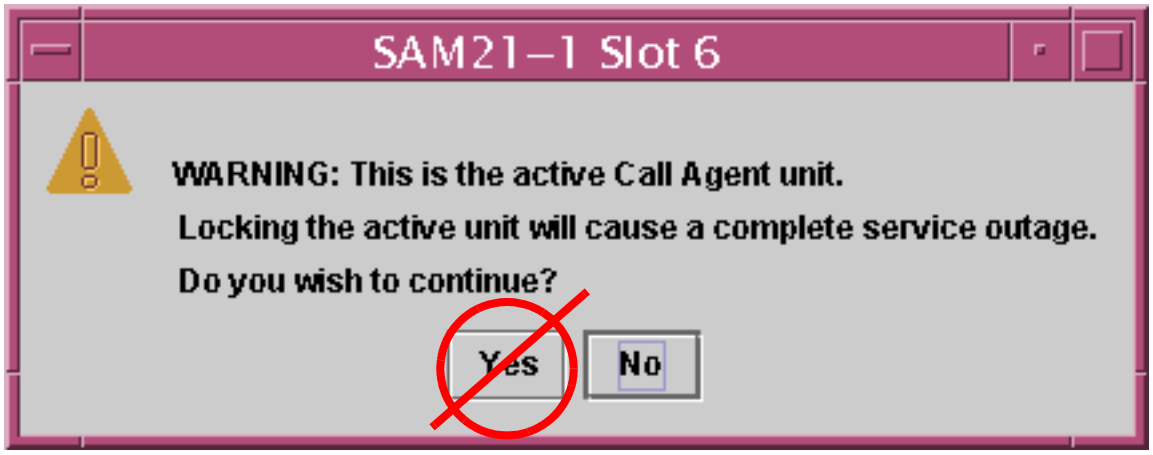
Verify that the customer accepts the new load.

ABORTSWACT is no longer available after this procedure. ABORTSWACT is the preferred method to revert a platform only upgrade. Reversion is still possible after this procedure, but requires assistance from Nortel Networks support personnel.

**CAUTION**
**Possible service interruption**
Do not lock the active Call Agent.

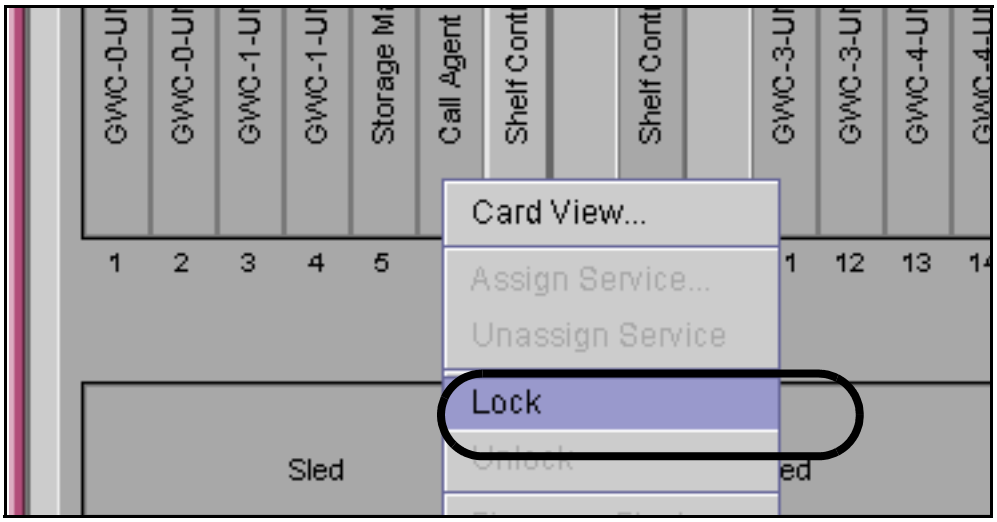
The CS 2000 SAM21 Manager client responds to an active Call Agent lock with the prompt shown in figure Call Agent lock warning. Do not click Yes. The inactive Call Agent is located in the other SAM21 shelf and a lock request does not provide a prompt when the Call Agent is inactive.

**Call Agent lock warning**



***At the CS 2000 SAM21 Manager client***

**1** From the Shelf View, right click on the card and select Lock from the context menu.




***Note:*** Lock is also available from the States tab of the Card View window.

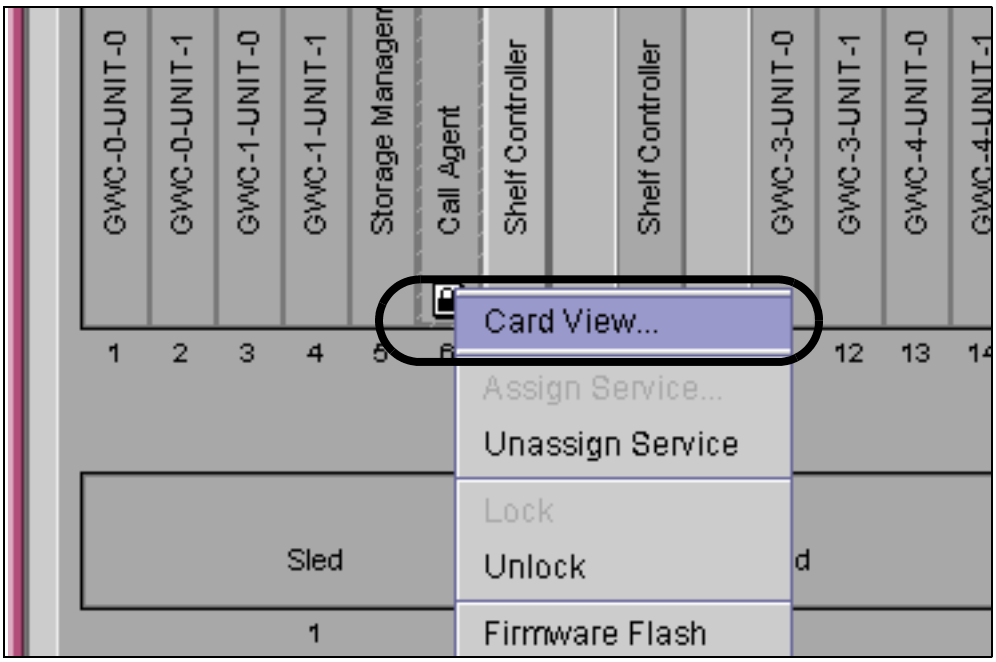
**2** Wait for the lock icon to appear on the selected card.

**3** This procedure is complete.

## Provision new software load

***At the CS 2000 SAM21 Manager client***

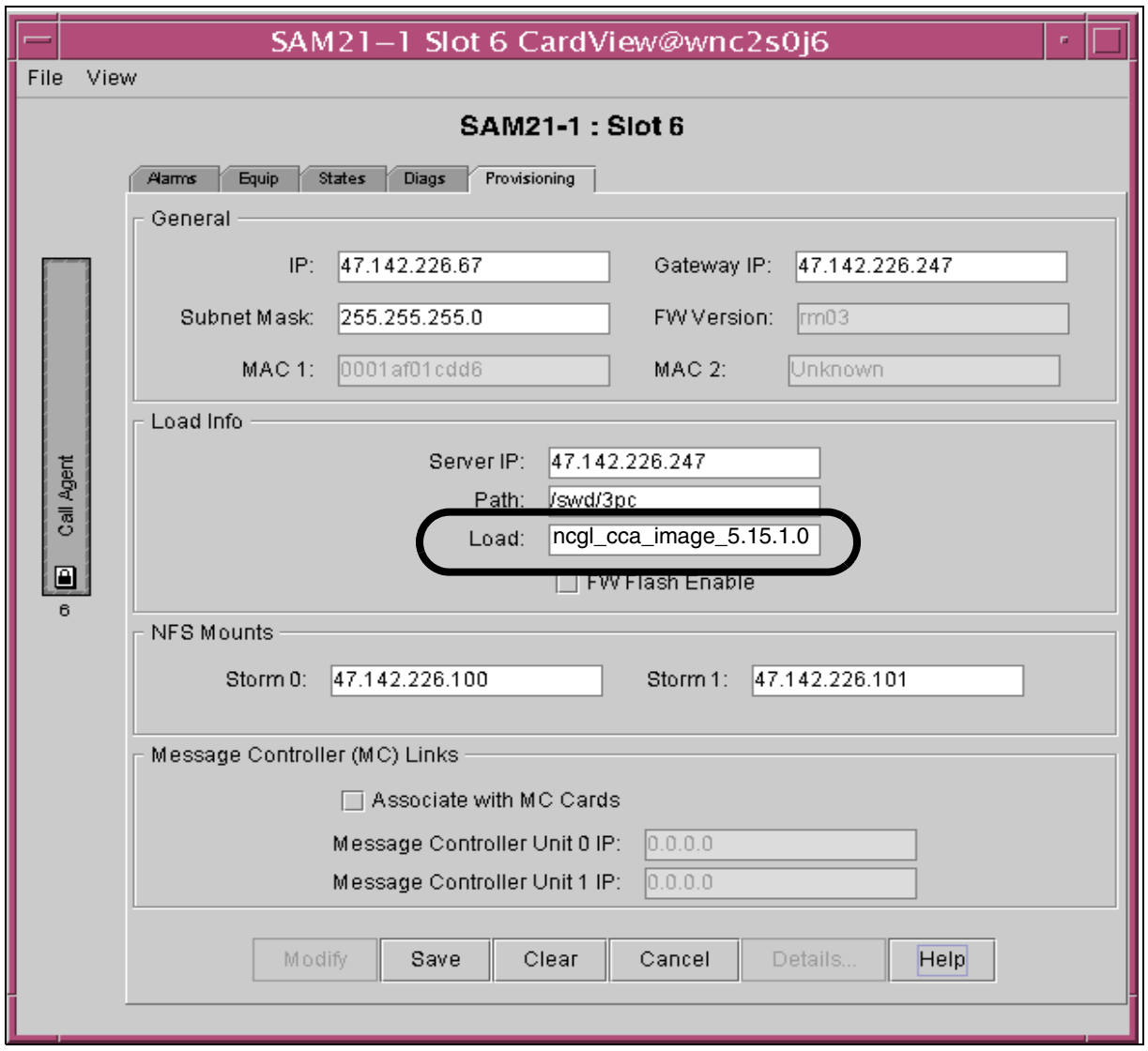
**1** From the Shelf View, right click on the card and select Card View from the context menu to open the Card View window.




**2** Click the Provisioning tab from the Card View window.

**3** Click the Modify button.

4 Enter the new load file name in the load field.




***Note:*** Click the firmware flash enable (FW Flash Enable) checkbox if the *SAM21 Platform Base Release Notes*, SAM2006 indicate a firmware upgrade is available. However, there is no consequence if the checkbox is enabled and firmware is not available. If a firmware flash upgrade is available, verify that “Firmware flash: succeeded” is reported in the History area of the States tab.

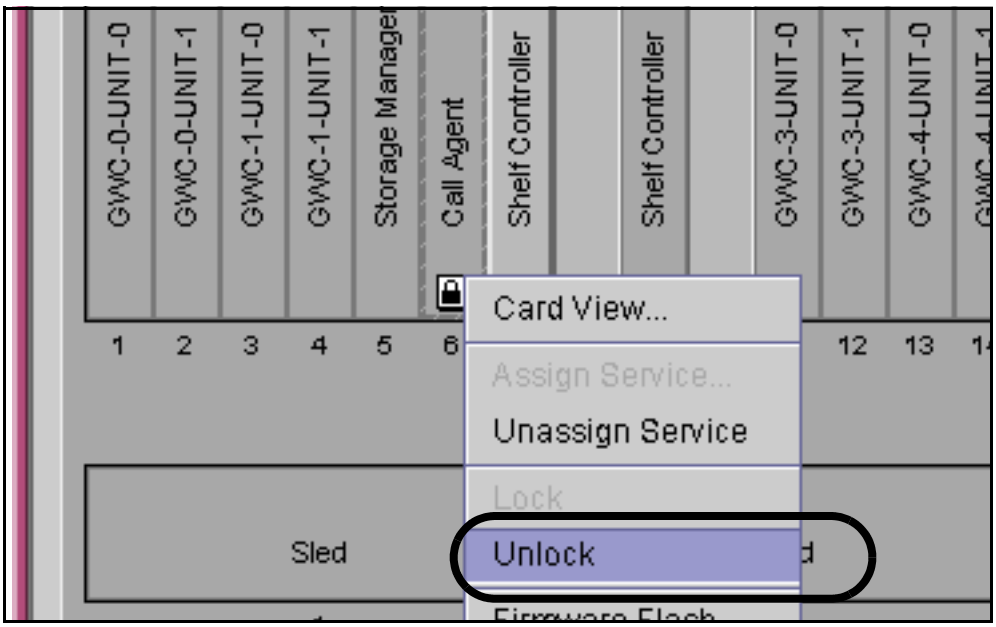
5 Click the Save button.

6 This procedure is complete.

# Unlock the inactive Call Agent

***At the CS 2000 SAM21 Manager client***

**1** From the Shelf View, right click on the card and select Unlock from the context menu.




***Note:*** Unlock is also available from the States tab of the Card View window.

The card resets, downloads software, and reboots.

**2** Wait for the lock icon to disappear.

***At the active Call Agent Manager***

**3** Verify that the call processing application loads successfully and waits for synchronization.

```
CoreMtc                 Jam:    Link0:  Link1:   BLnk: FC: Appl:
 0 Quit    Unit0 Inact yes      . Act   . Inact    S    S   nosync /waiting
 2 CAMtc   Unit1 Act   no       . Act   . Inact    S    S   nosync
```

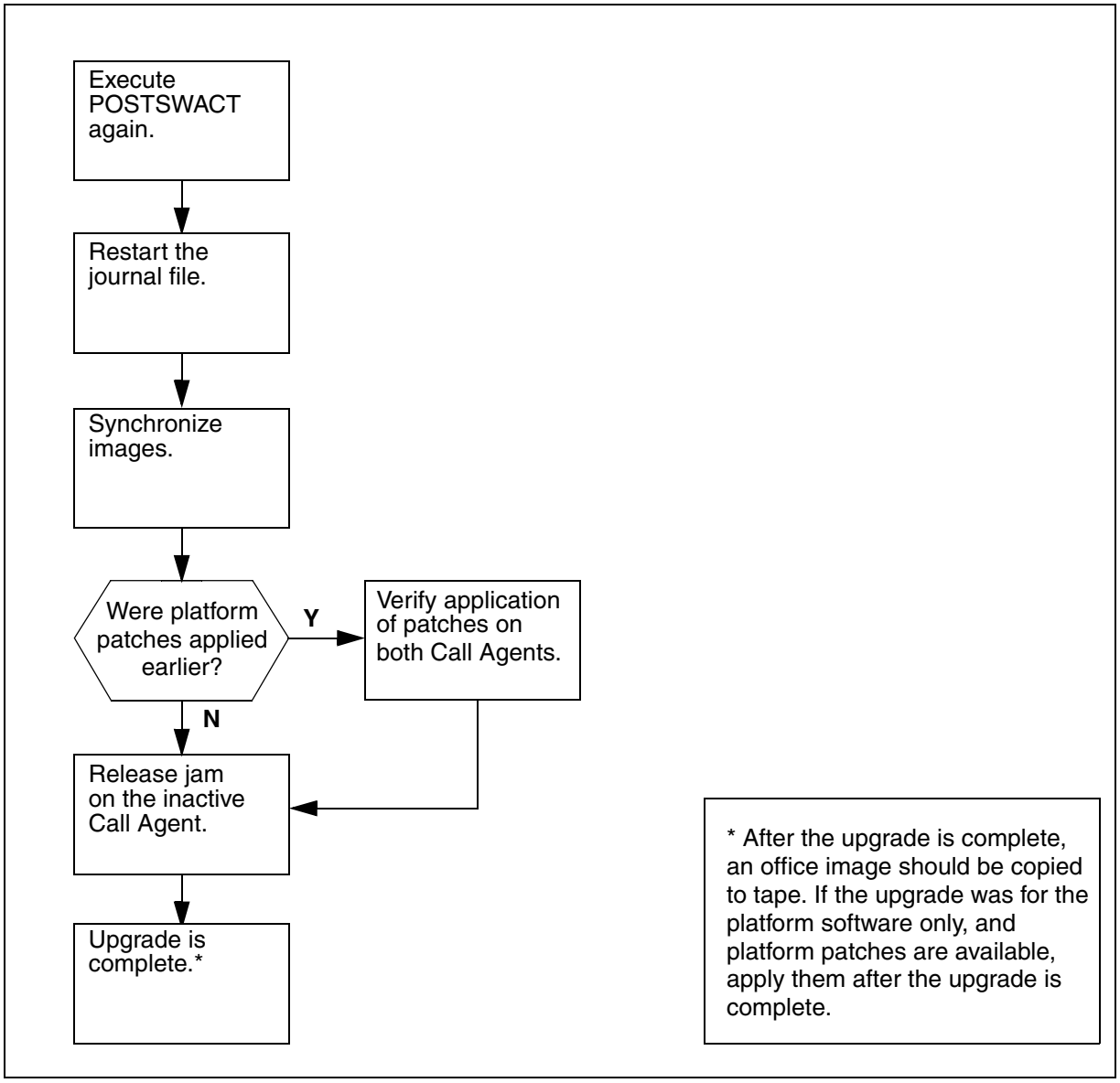
***Note:*** The figure above is used only to show the waiting flag. Disregard the values for activity and jam state.

**4** This procedure is complete.

# Complete POSTSWACT

Perform the procedures in this section to commit the new load. If a revert was required, the procedures in this section complete the reversion.

### Complete POSTSWACT procedure



# Execute POSTSWACT again

***At the MAP***

1 Execute POSTSWACT:

```
> BCSUPDATE;POSTSWACT
```

2 Confirm the prompt to XA_UNSPLIT:

```
> Y
```

3 Clean up SFDEV by erasing any application-related files, such as FEATDATA, SITEINFO, and DIRP_INAC.

Have telephone operating company personnel perform the following procedure.

***At the MAP***

1 Verify passwords for users ADMIN and OPERATOR.

2 Reassign all current PROFILE information (LOGIN or RESTART) in SFDEV.

3 Reassign any temporary log ROUTING setup using LOGUTIL.

4 If table PADNDEV was altered, restore the original values.

5 This procedure is complete.

# Restart journal file

***At the MAP***

1 Access the DIRP level of the MAP:

```
> MAPCI;MTC;IOD;DIRP
```

2 Start the journal file:

```
> JF START
```

3 This procedure is complete.

# Synchronize images

Perform this procedure only if XA_UNSPLIT was rejected during POSTSWACT.

***SDE — At the active maintenance window (CORE0 or CORE1)***

**1** Enter the CoreMtc level.

```
> CoreMtc
```

**2** Enter the Appl level.

```
> Appl
```

**3** Enter the Sync command.

```
> Sync
```

```
 CallAgent       SYS       CON       APPL              Unit: 0
    .             .         .       simplx
                                      M
Appl                         Jam:  Link0:  Link1:  BLnk: FC: Appl:
 0 Quit       Unit0  Act     no     . Inact . Act     S    NA  nosync .
 2 ImgTst     Unit1  Inact   no     . Act   . Inact   S    NA  nosync .
 3 Sync
 4 DpSync
 5
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh    Sync:     Synchronize the applications.
  mtc
Time  12:27  >
```

**4** This procedure is complete.

# Verify platform patches

Perform this procedure only if platform patches were applied earlier to the first Call Agent.

***At the active Call Agent Manager***

1. If platform patches are available, platform patches may need to be applied to this Call Agent unit:
2. At the TRANSFER level (**ccamtc transfer** ) a list of available patches is displayed. For each patch:
   - **a** SELECT the patch by number
   - **b** FETCH INA the patch to the INACTIVE unit
3. At the PATCH level, for each patch to be applied and committed:
   - **a** SELECT the patch by number
   - **b** DISADMIN the patch and follow any special instructions
   - **c** APPLY INA the patch to the INACTIVE unit
   - **d** SELECT the patch by number
   - **e** COMMIT INA the patch to the INACTIVE unit
4. Verify that the reported load information is the same for both Call Agents.
5. This procedure is complete.

# Release jam on the inactive Call Agent

***At the active Call Agent Manager***

**1** Enter the RelJam command:

```
> CoreMtc
> CAMtc
> RelJam
```

```
 CallAgent       SYS       CON       APPL              Unit: 1
    .             .         .         .

CAMtc                       Jam:  Link0:  Link1:  BLnk: FC: Appl:
 0 Quit       Unit0  Inact  no    . Inact . Act    .    .   insync .
 2 Jam        Unit1  Act    no    . Inact . Act    .    .   insync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh   RelJam:   Release jam on the inactive unit.
  mtc
Time  10:38  >
```

**2** This procedure is complete.

The upgrade is complete. Backup the image taken during procedure Test calls and acceptance on page 1219. For the details of how to make the backup, refer to section Backup image on page 421.

# Upgrading Multiservice Switch 15000/Media Gateway 15000 in Succession Networks (UA-IP)

## HSM overview

This section describes Nortel Networks Multiservice Switch/Media Gateway hitless software migration (HSM) and its associated processes. While an HSM must be preceded by pre-migration checks and followed by post-migration checks, these checks are not described in this overview. For information on pre-migration checks, see HSM (Command Console) pre-work on page 1236. For information on post-migration checks, see Verify the success of HSM on page 1287.

## What happens to the node during a hitless software migration

Nortel Networks Multiservice Switch 15000/20000 and Media Gateway 15000/20000 nodes support hitless software upgrades in Succession

PT-IP, PT-AAL2, IAC, or IAW solutions. Nortel Networks Multiservice Switch 15000 and Media Gateway 15000 nodes support hitless software upgrades in Succession UA-IP solution. During a hitless software migration, the Multiservice Switch 15000/20000 or Media Gateway 15000/20000 shelf logically splits into two shelves: the service shelf and the migration shelf. The service shelf contains the active FPs and is controlled by the active CP. The migration shelf contains the standby FPs and is controlled by the standby CP. The standby cards that are being loaded with the new version of software are referred to as the migrating cards.

During the migration, the active CP and FPs continue to operate using the old version of software while a new version of software is being loaded and provisioned on the migrating CP and FPs. The active cards remain active until the migrating cards have finished migrating to the new software and are ready to take over.

When the migration shelf is ready, the migration shelf will become the active shelf without operator intervention. This is called migration switchover. The CP and FPs in the former service shelf then reset and are loaded with the new version of software.

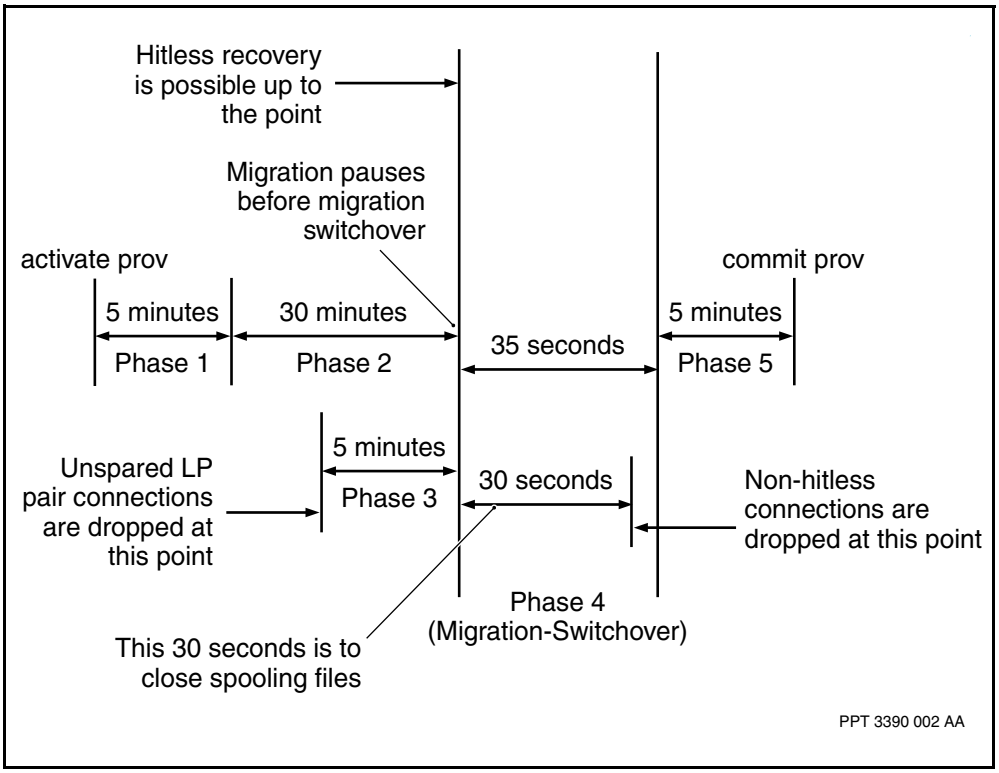
If a problem is detected by the system, the process pauses automatically allowing the operator to stop migration or fix the problem and continue.

The five phases of a hitless software migration are as follows:

- Phase 1 - Preparation of the CP on page 1232
- Phase 2 - CP migration on page 1233
- Phase 3 - FP migration on page 1234
- Phase 4 - Migration switchover on page 1234
- Phase 5 - Post migration on page 1235

Refer to the figure Hitless software migration phases on page 1232 for more information about the phases.

**Figure 1 Hitless software migration phases**




## Phase 1 - Preparation of the CP

### Procedure 1 Preparing the CP

***As the hitless migration begins, the following occurs:***

**1** The edit view is saved in a temporary file.

**2** Hitless CP switchover is disabled.

**3** The card availability status of the standby CP is set to migrating. The standby CP resets to load new software.

4 The system responds to the **activate prov** command indicating that a software migration activation is to be performed.

5 Certain operator commands are automatically disabled.

6 The **Prov Migration** component is created and a SET warning alarm is issued against this component indicating that a software migration is being performed.

***Note:*** The disabled operator commands remain disabled by the system until after the migration switchover or hitless recovery.

## Phase 2 - CP migration

### Procedure 2 CP migration

***After the system raises the SET warning alarm to complete phase 1, the following occurs:***

1 The LED of the migrating CP eventually changes to fast, pulsing green.

2 The new provisioning view migrates to the migrating CP.

3 Committed formats of the migrated view are saved on the migrating CP.

4 The active CP splits the physical shelf into two logical shelves: the service shelf and the migration shelf. The active CP also prepares for the FP migrations according to the following criteria:

- For FPs in a one-for-one sparing model, one FP remains under the control of the active CP in the service shelf while the second FP goes under the control of the migrating CP. The second FP's card availability is set to migrating and is reset to load new software. At this point, equipment protection is disabled.
- For FPs that do not fit the previous criteria, the FPs remain under the control of the active CP in the service shelf. These FPs are reloaded with new software after the migration switchover occurs.

5 Provisioning data is delivered within the migrating CP.

6 Applications that run on the CP are initialized.

***Note:*** Disk synchronization occurs in the background during this phase. This phase is not complete until disk synchronization is complete.

## Phase 3 - FP migration

### Procedure 3 FP migration

***After the system initializes the CP applications to complete phase 2, the following occurs:***

1. The migrating FPs load new software and start up in migration mode.
2. The LEDs of the migrating FPs eventually change to fast, pulsing green or to solid green.
3. Provisioning data is delivered on the migrating FPs.
4. The migrating FPs are loaded with dynamic data for services, such as ATM and IP. The automatic pause condition exists when a fault scenario occurs on the migration shelf such that an application cannot achieve its expected switchover behavior. The software migration pauses before the migration switchover. The **Prov Migration** component is operationally disabled and an appropriate alarm is raised against it. The operator must either issue a **continue -force prov** command to continue with the migration switchover, or **stop prov** to stop the software migration.

   After a **continue -force prov** command is issued, the system does not pause again. If you are in an SN07 to SN07 migration, and the system has paused prior to migration switchover, the expected pause at migration switchover does not occur.

## Phase 4 - Migration switchover

### Procedure 4 Migration switchover

***After the system notifies the active CP that phase 3 is complete, the following occurs:***

1. Migration switchover begins when the CPs close all spooled files. For example, alarms and security logs.
2. All processors in the service and migration shelves are notified to switchover.
3. Processors within the service shelf reset to load new software.
4. The CP and FPs in the migration shelf become the service shelf. FPs providing services, such as ATM and IP, re-establish signalling and routing functions. The CP and FPs with the new software start providing service.
5. Any sparing panels are switched over.

6 Final port initialization is completed.

7 The shelf becomes one when all CPs and FPs are running the new software. The shelf is no longer logically split.

## Phase 5 - Post migration

### Procedure 5 Post-migration

***After all CPs and FPs are running the new software and phase 4 is complete, all alarms are cleared and the following occurs:***

1 The restarting CP and FPs load new firmware, new software, and their provisioning data is activated.

2 FP applications initialize with provisioning data and re-establish services, such as ATM and IP. Dynamic service data is loaded from the active FPs.

3 Network management connectivity is re-established.

4 Equipment protection and inter-card APS are re-established.

5 The operator commands which are disabled during the software migration are now available.

6 The operator must complete provisioning by confirming the provisioning changes. This phase is completed once the operator commits the new provisioning view.

# HSM (Command Console) pre-work

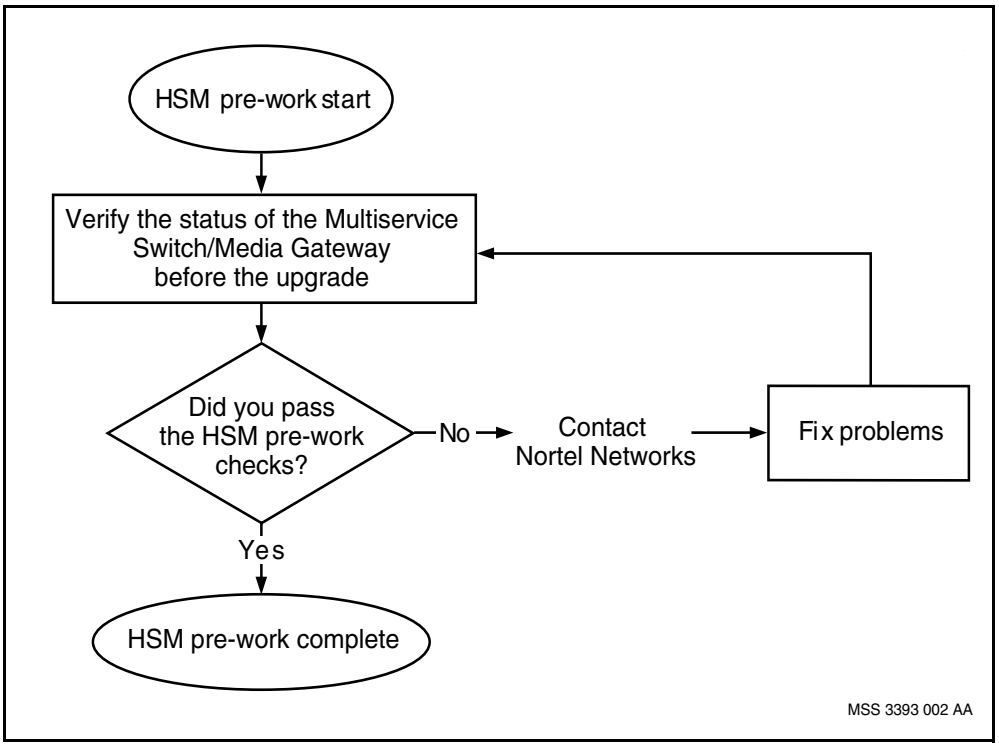
Complete the HSM pre-work before you proceed with a software upgrade.

## Prerequisites

- Complete Downloading and backing up node software on page 446.

  The task flow shows the sequence of procedures you need to perform prior to performing the HSM.

### HSM pre-work task flow



## Verify the status of the node before the upgrade

Verify the status of Multiservice Switch 15000/Media Gateway 15000/20000 nodes before upgrading to ensure that the nodes do not have any alarms raised, and that they are configured correctly. Record the current status, so you can compare it to the node status following the upgrade to verify that the upgrade proceeded correctly.

***Note:*** The following pre-checks apply to Multiservice Switch 15000/Media Gateway 15000 nodes in a UA-IP solution. Solutions using AAL2, SPVCs for VoIP, ASPEN signalling and/or electrical TDM cards will require additional pre-checks of the related components.

## Prerequisites

- Save the information gathered in the following procedure to verify the success of the upgrade. To save the information to a file if you are using Nortel Networks Preside Multiservice Data Manager (MDM), select Command Console, select **Log to File** from the File menu and set the options in the Log to File dialog as required. If you are not using Command Console, use the standard UNIX logging functionality.
- If any of the components displayed in the following procedure are not enabled or have alarms, investigate the cause and correct the problem before proceeding with the hitless software migration. The node that you are upgrading and all of the nodes connected to it must be free of alarms.

1 Verify that the disk and file systems are synchronized:

**display FileSystem syncStatus**

2 Verify that the syncProgress between the disk and the file system is 100%:

**display FileSystem syncProgress**

3 Ensure that network synchronization on the system is enabled, unlocked, synchronized, and free of alarms:

**display NetworkSynchronization**

4 Ensure that there is no provisioning activity occurring on the control processors by verifying that the *provisioningActivity* value is none:

**display prov provisioningActivity**

5 Ensure that there is no provisioning activity occurring on the control processors by verifying that the *standbyCpActivity* value is none:

**display prov standbyCpActivity**

6 Ensure that there is no provisioning activity occurring on the control processors by verifying that the s*tandbyCpActivityProgress* value is n/a:

**display prov standbyCpActivityProgress**

7 Ensure that there is no provisioning activity occurring on the control processors by verifying that there is either no value for the *provisioningSession* or the value is the same as the value for Preside MDM server session:

**display prov provisioningSession**

***Note:*** To find the value of the Preside MDM session, issue the **me** command. An empty value or a value the same as your session is the expected response.

8 Ensure that there is no provisioning activity occurring on the control processors by verifying that the *editViewAddedComponents* value is 0:

**display prov editViewAddedComponents**

9 Ensure that there is no provisioning activity occurring on the control processors by verifying that the *editViewDeletedComponents* value is 0:

**display prov editViewDeletedComponents**

10 Ensure that there is no provisioning activity occurring on the control processors by verifying that the e*ditViewChangedComponents* value is 0:

**display prov editViewChangedComponents**

11 Verify the status of the node's fabrics before migration:

**display shelf fabriccard/* osistate**

For both fabrics, the osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. Both fabrics must be enabled and free of alarms.

The following shows sample output when you verify the status of the fabrics before migration:

```
> display shelf fabriccard/* osistate

Shelf FabricCard/*
-------------------------------------------------------------------------
|FabricCard|osiAd|osiO|osiUs|osiAai |osiProc|osiCntr|osiAlar|osiS|osiUn
|          | min |per | age |   l   |       |   l   |   m   |tby | knw
-------------------------------------------------------------------------
|x         |unlck|ena |activ|       |       |       |       |nSet|false
|y         |unlck|ena |activ|       |       |       |       |nSet|false
```

**12** Verify that all logical processors on the system are enabled, unlocked, and free of alarms:

**display Lp/* osistate**

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the logical processors must be enabled and free of alarms.

The following shows sample output for this command:

```
> display Lp/* osistate

Lp/*
+==+-----+----+-----+-------+-------+-------+-------+----+-----
|Lp|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|  | min |per | age |   l   |       |   l   |   m   |tby | knw
+==+-----+----+-----+-------+-------+-------+-------+----+-----
| 0|unlck|ena |activ|       |       |       |       |serv|false
| 8|unlck|ena |activ|       |       |       |       |serv|false
| 9|unlck|ena |activ|       |       |       |       |serv|false
|14|unlck|ena |activ|       |       |       |       |serv|false
```

**13**



**CAUTION**
**Possibility of non-hitless software migration**
Any card that does not have equipment protection enabled will undergo a non-hitless software upgrade during the migration and experience an outage. If there is a card that has equipment protection configured on it, but has a value of *nset* or |:N equipment protection displayed in the *osiStby* column, that protection pair will also undergo a service outage.

Investigate why that value is being displayed and correct the problem before proceeding with a hitless software migration.

Verify that the equipment protection has been configured properly and all spared cards are ready to take over:

**display Shelf Card/* SparedServices**

All cards configured with equipment protection should have a value of *serv*. All standby function processors should have a value of *hot* indicating *hot standby*.

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty.

The following shows sample output when you verify that the equipment protection is configured properly, and all spared cards are ready to take over:

```
> display Shelf Card/* SparedServices

Shelf Card/* SpServ
-------------------------------------------------------------------
|Card|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|    | min |per | age |   l   |       |   l   |   m   |tby | knw
-------------------------------------------------------------------
|   0|unlck|ena |activ|       |       |       |       |hot |false
|   1|unlck|ena |activ|       |       |       |       |serv|false
|   8|unlck|ena |activ|       |       |       |       |serv|false
|   9|unlck|ena |activ|       |       |       |       |hot |false
|  14|unlck|ena |activ|       |       |       |       |serv|false
|  15|unlck|ena |activ|       |       |       |       |hot |false
```

**14** Verify that all logical processors using the dual LP sparing model are enabled, unlocked and free of alarms:

**display Dlep/* osistate**

The following shows sample output for this command:

```
> display Dlep/* osistate

Dlep/*
-------------------------------------------------------------------
|Dlep|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|    | min |per | age |   l   |       |   l   |   m   |tby | knw
-------------------------------------------------------------------
|   6|unlck|ena |activ|       |       |       |       |nSet|false
```

**15** If the node is connected with GigE to a Passport 8600 node, verify that all the Ethernet ports configured on the system are enabled, unlocked and free of alarms:

**display Lp/* Ethernet/* osistate**

The following shows sample output for this command:

```
> display Lp/* Ethernet/* osistate

Lp/* Eth/*
+==+===+-----+----+-----+-------+-------+-------+-------+----+-----
|Lp|Eth|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|  |   | min |per | age |   l   |       |   l   |   m   |tby | knw
+==+===+-----+----+-----+-------+-------+-------+-------+----+-----
|14|  0|unlck|dis |idle |depend |       |       |crit   |nSet|false
|14|  1|unlck|ena |busy |       |       |       |       |nSet|false
|15|  0|unlck|ena |busy |       |       |       |       |nSet|false
|15|  1|unlck|ena |busy |       |       |       |       |nSet|false
|15|  3|unlck|ena |busy |       |       |       |       |nSet|false
```

**16** Verify that all the *Sonet* ports configured on the system are enabled, unlocked, and free of alarms:

**display Lp/* Sonet/* osistate**

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *SONET* ports must be enabled and free of alarms.

The following shows sample output for this command:

```
5> display Lp/* Sonet/* osistate
Lp/* Sonet/*

-------------------------------------------------------------
|Lp |Sonet|osi   |osi |osi  |osi  |osi  |osi |osi  |osi  |osi
|   |     |Admin |Oper|Usage|Avail|Proc |Cntr|Alarm|Stby |Unknw
|-------------------------------------------------------------
|2  | 1   |unlck |ena |busy |     |     |    |     |nSet |false
|2  | 2   |unlck |ena |busy |     |     |    |     |nSet |false
|3  | 1   |unlck |ena |busy |     |     |    |     |nSet |false
|3  | 2   |unlck |ena |busy |     |     |    |     |nSet |false
|8  | 0   |unlck |ena |busy |     |     |    |     |nSet |false
```

**17** Verify that there are no shelf hardware failures.

**display sh hardware**

```
d sh hardware

Shelf
   hardwareFailures =
ok   2004-09-09 20:03:32.53

2> h sh hard
Shelf
   Attribute     hardwareFailures (hwFailures)
       Access     Read:  passive     Write: not allowed
       Criticality      none
       Type   SET OF Enumeration
       Values
 card,powerConverter,coolingUnit,terminatorCard,fan,

 powerSupply,fabricCard,macAddressCard,alarmBitsCard
       Default
```

**18** Display the *Laps* components to identify any *Laps* components that have any faults or a manual override associated with them.

***Note:*** Use the -noTabular option to view the following hidden attributes: *osiUnknw, osiStby, osiAlarm, osiCntrl, osiProc, osiAvail, mmAlarm, pfAlarm* and *timeUntilRestore*.

**display Laps/***

The *Laps* component should be unlocked, enabled, working, and protected.

Acceptable values for the operational attribute *NearEndRequest* (*neReq*) are "NoRequ" (noRequest) and "doNotR" (doNotRevert).

The following shows a sample output for this command:

display Laps/*

| Laps | osiAdmin | osiOper | osiUsage | neRxLine | neReq | neReqChan | feReq | feReqChan | sdOnLines | switchovers |
|---|---|---|---|---|---|---|---|---|---|---|
| 200 | unlck | ena | busy | protec | doNotR | workin | noRequ | protec | | 1 |
| 201 | unlck | ena | busy | protec | doNotR | workin | noRequ | protec | | 1 |
| 202 | unlck | ena | busy | protec | doNotR | workin | noRequ | protec | | 1 |
| 203 | unlck | ena | busy | protec | doNotR | workin | noRequ | protec | | 1 |
| 600 | unlck | ena | busy | workin | noRequ | protec | noRequ | protec | | 4 |
| 601 | unlck | ena | busy | workin | **lockou** | protec | noRequ | protec | | 2 |
| 602 | unlck | ena | busy | protec | **manual** | workin | doNotR | workin | | 1 |

**19** For each *Laps* component listed in the output, whose values for neReq are "lockou" (lockoutOfProtection) or "manual", remove this state of line automatic protection switching (LAPS):

**clear Laps/<laps_inst>**

In the sample command output for step 18, the clear command would be needed for *Laps*/601 and *Laps*/602.

**20** Verify that the *lop, ais, rfi, slm, txAis,* and *txRdi* attributes of the *Laps Sts* components have a value of *off*:

**display Laps/* Sts/0**

The osiAdmin column should contain only *unlck* values. All of the attributes from *lop* to *txRdi* should have a value of *off*.

The following shows sample output for this command:

```
> display Laps/* Sts/0

Laps/* Sts/0
   Use -noTabular to see the many hidden attributes.
----------------------+-------------------------------------------
|Laps |osiAd|osiO|osiUs|snmpOp|lop|ais|rfi|slm|txA|txR|  pefs   |  pc
|     | min |per | age |erStat|   |   |   |   |is |di |         |
|     |     |    |     |  us  |   |   |   |   |   |   |         |
-----------------------------------------------------------------------
|  800|unlck|ena |busy |up    |off|off|off|off|off|off|      215|
|  802|unlck|ena |busy |up    |off|off|off|off|off|off|      279|
|  803|unlck|ena |busy |up    |off|off|off|off|off|off|      279|
```

**21** Verify that the *Laps* components are enabled, unlocked, and free of alarms:

**display Laps/* osistate**

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the Laps components must be enabled and free of alarms.

The following shows sample output for this command:

```
> display Laps/* osistate

Laps/*
-------------------------------------------------------------------------
|Laps |osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|     | min |per | age |   l   |       |   l   |   m   |tby | knw
-------------------------------------------------------------------------
|  800|unlck|ena |busy |       |       |       |       |nSet|false
|  802|unlck|ena |busy |       |       |       |       |nSet|false
|  803|unlck|ena |busy |       |       |       |       |nSet|false
```

**22** If *DS3* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

**display lp/* ds3/* osistate**

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *DS3* components must be enabled and free of alarms.

The following shows sample output for this command:

```
> display lp/* ds3/* osistate

Lp/* DS3/*
-------------------------------------------------------------------------
|Lp|DS3|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|  |   |  min |per | age |   l   |       |   l   |   m   |tby | knw
-------------------------------------------------------------------------
|10|  0|unlck|ena |busy |       |       |       |       |nSet|false
|10|  1|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|unlck|ena |busy |       |       |       |       |nSet|false
```

**23** If *DS1* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

**display lp/* ds3/* ds1/* osistate**

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *DS1* components must be enabled and free of alarms.

The following shows sample output for this command:

```
> display lp/* ds3/* ds1/* osistate

Lp/* DS3/* DS1/*
-------------------------------------------------------------------------
|Lp|DS3|DS1|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|  |   |   |  min |per | age |   l   |       |   l   |   m   |tby | knw
-------------------------------------------------------------------------
|14|  0|  1|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  2|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  3|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  4|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  5|unlck|ena |busy |       |       |       |       |nSet|false
```

**24** If *DS3 DS1 Chan* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

**display lp/* ds3/* ds1/* chan/* osistate**

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *DS3 DS1 Chan* components must be enabled and free of alarms.

The following shows sample output for this command:

```
> display lp/* ds3/* ds1/* chan/* osistate

Lp/* DS3/* DS1/* Chan/*
-------------------------------------------------------------------------
|Lp|DS3|DS1|Chan|osi   |osi |osi  |osi   | osi  |osi  |osi   |osi |osi
|  |   |   |    |Admin|Oper|Usage|Avail| Proc |Cntrl|Alarm|Stby|Unkn
-------------------------------------------------------------------------
|14|  0|  1|   0|unlck|ena |busy |     |      |     |     |nSet|fals
|14|  0|  2|   0|unlck|ena |busy |     |      |     |     |nSet|fals
|14|  0|  3|   0|unlck|ena |busy |     |      |     |     |nSet|fals
|14|  0|  4|   0|unlck|ena |busy |     |      |     |     |nSet|fals
```

**25** If *DS3 IMA* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

**display lp/* ds3/* ima/* osistate**

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *DS3 IMA* components must be enabled and free of alarms.

The following shows sample output for this command:

```
> display lp/* ds3/* ima/* osistate

Lp/* DS3/* Ima/*
-------------------------+-------+-------+-------+-------+----+-----
|Lp|DS3|Ima|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|  |   |   | min |per | age |   l   |       |   l   |   m   |tby | knw
--------------- +----+-----+-------+-------+-------+-------+----+----
|14|  0|  0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  1|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  2|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  1|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  2|unlck|ena |busy |       |       |       |       |nSet|false
```

**26** If *DS3 IMA LINK* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

**display lp/* ds3/* ima/* lk/* osistate**

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *DS3 IMA* components must be enabled and free of alarms.

The following shows sample output for this command:

```
> display lp/* ds3/* ima/* lk/* osistate

Lp/* DS3/* Ima/* Lk/*
+==+===+===+==+-----+----+-----+-----+----+-----+-----+----+-----
|Lp|DS3|Ima|Lk|osiAd|osiO|osiUs|osi  |osi |osi  |osi  |osiS|osiUn
              | min |per | age |Avail|Proc|Cntrl|Alarm|tby | knw
+==+===+===+==+-----+----+-----+-----+----+-----+-----+----+-----
|14|  0|  0| 1|unlck|ena |busy |     |    |     |     |nSet|false
|14|  0|  0| 2|unlck|ena |busy |     |    |     |     |nSet|false
|14|  0|  0| 3|unlck|ena |busy |     |    |     |     |nSet|false
|14|  0|  0| 4|unlck|ena |busy |     |    |     |     |nSet|false
|14|  0|  0| 5|unlck|ena |busy |     |    |     |     |nSet|false
|14|  0|  0| 6|unlck|ena |busy |     |    |     |     |nSet|false
|14|  0|  0| 7|unlck|ena |busy |     |    |     |     |nSet|false
|14|  0|  0| 8|unlck|ena |busy |     |    |     |     |nSet|false
|14|  0|  1| 1|unlck|ena |busy |     |    |     |     |nSet|false
|14|  0|  1| 2|unlck|ena |busy |     |    |     |     |nSet|false
```

**27** Verify that all *ATM interfaces* configured on the system are enabled, unlocked, and free of alarms:

**display AtmIf/* osistate**

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *ATM interfaces* must be enabled and free of alarms.

The following shows sample output for this command:

```
6> display AtmIf/* osistate
AtmIf/*
-------------------------------------------------------------------
|   AtmIf|osiAdmin|osiOper|osiUsage|osiAvail|osiProc|osiCntrl|osiAlarm|osiStby|osiUnknw
-------------------------------------------------------------------
|   201 |unlck|ena|busy||  |        |                              |nSet  |false
|   202 |unlck|ena|busy||  |        |                              |nSet  |false
|   800 |unlck|ena|busy||  |        |                              |nSet  |false
|   801 |unlck|ena|busy||  |        |                              |nSet  |false
|   802 |unlck|ena|busy||  |        |                              |nSet  |false
|   803 |unlck|ena|busy||  |       |                              |nSet|false
|   813 |unlck|ena|busy||  |         |                                   |nSet  |false
```

**28** Verify that all *UNI signalling* components are enabled and unlocked:

**display atmif/* uni sig/(operatingMode = normal) osistate**

The osiAdmin column should contain only *unlck* values. All of the *UNI Signalling* components must be enabled.

The following shows sample output for this command:

```
> display atmif/* uni sig/(operatingmode = normal) osistate

AtmIf/* Uni Sig
-------------------------------------------------------------------
|AtmIf|osiAd|osiO|osiUs|Response
|     | min |per | age |
-------------------------------------------------------------------
|  215|unlck|ena |activ|
```

**29** Verify that the *ILMI* channel osistate for the *AtmInterface* is enabled and unlocked:

**display atmif/* uni ilmi/(operatingMode = addressRegEnabled) osistate**

The osiAdmin column should contain only *unlck* values. All of the *ILMI* components must be enabled.

***Note:*** If *ILMI* is not configured, disabled is a valid osiState.

The following shows sample output for this command:

```
10> display atmif/* uni ilmi/(operatingMode = addressRegEnabled)
osistate

AtmIf/* Uni Ilmi
-------------------------------------------------------------------
AtmIf|osiAd|osiO|osiUs|Response
     | min |per | age |
-------------------------------------------------------------------
   45|unlck|dis |idle |
   48|unlck|dis |idle |
   49|unlck|dis |idle |
   55|unlck|dis |idle |
   59|unlck|ena |activ|
   63|unlck|ena |activ|
  100|unlck|ena |activ|
  101|unlck|ena |activ|
  212|unlck|dis |idle |
```

**30** Verify that all *PNNI signalling* components are enabled and unlocked:

**display AtmIf/* Pnni Sig osistate**

The osiAdmin column should contain only *unlck* values. All of the *PNNI Signalling* components must be enabled.

The following shows sample output for this command:

```
10> display AtmIf/* Pnni Sig osistate

AtmIf/* Pnni Sig
-------------------------------------------------------------------------
AtmIf|osiAdmin|osiOper|osiUsage|Response
-------------------------------------------------------------------------
   201|unlck|ena|activ|
   202|unlck|ena|activ|
```

**31** Verify that the *Atmmpe* components are unlocked, enabled, and active:

**display Atmmpe/* osistate**

The following shows sample output for this command:

```
> display Atmmpe/* osistate

AtmMpe/*
+======+=====+====+=====+----------------------------------------
|AtmMpe|osiAd|osiO|osiUs|Response
|      | min |per | age |
+======+=====+====+=====+----------------------------------------
|   800|unlck|ena |activ|
|   810|unlck|ena |activ|
|   900|unlck|ena |activ|
|  1000|unlck|ena |activ|
|  1001|unlck|ena |activ|
|  1100|unlck|ena |activ|
|  1101|unlck|ena |activ|
|  1400|unlck|ena |activ|
|  1401|unlck|ena |activ|
|  1402|unlck|ena |activ|
|  1420|unlck|ena |activ|
|  1421|unlck|ena |activ|
|  1422|unlck|ena |activ|
|  1500|unlck|ena |activ|
|  1501|unlck|ena |activ|
|  1502|unlck|ena |activ|
|  1520|unlck|ena |activ|
|  1521|unlck|ena |activ|
|  1522|unlck|ena |activ|
```

**32** Verify that the *Ac* components are unlocked, enabled, and active:

**display Atmmpe/* Ac/* osistate**

The following shows sample output for this command:

```
> display Atmmpe/* Ac/* osistate

AtmMpe/* Ac/*
+======+===+-----+----+-----+-------------------------------------
|AtmMpe|Ac |osiAd|osiO|osiUs|Response
|      |   | min |per | age |
+======+===+-----+----+-----+-------------------------------------
|   800|  1|unlck|ena |activ|
|   800|  2|unlck|ena |activ|
|   800|  3|unlck|ena |activ|
|   810|  1|unlck|ena |activ|
|   900|  1|unlck|ena |activ|
|  1000|  1|unlck|ena |activ|
|  1001|  1|unlck|ena |activ|
|  1100|  1|unlck|ena |activ|
|  1101|  1|unlck|ena |activ|
|  1400|  1|unlck|ena |activ|
|  1401|  1|unlck|ena |activ|
|  1402|  1|unlck|ena |activ|
|  1420|  1|unlck|ena |activ|
|  1421|  1|unlck|ena |activ|
|  1422|  1|unlck|ena |activ|
|  1500|  1|unlck|ena |activ|
|  1501|  1|unlck|ena |activ|
|  1502|  1|unlck|ena |activ|
|  1520|  1|unlck|ena |activ|
```

**33** If the Multiservice Switch 15000/Media Gateway 15000/20000 node is connected with GigE to a Passport 8600, node verify that all *LanApplications* components are enabled and unlocked:

**display La/* osistate**

The following shows sample output for this command:

```
> display La/* osistate

La/*
+===+-----+----+-----+-------------------------------------
|La |osiAd|osiO|osiUs|Response
|   | min |per | age |
+===+-----+----+-----+-------------------------------------
|  0|unlck|ena |busy |
|140|unlck|dis |idle |
|141|unlck|ena |busy |
|150|unlck|ena |busy |
|151|unlck|ena |busy |
|153|unlck|ena |busy |
```

**34** Verify that all *VirtualRouter* components are unlocked, enabled and active:

**display Vr/* osistate**

The following shows sample output for this command:

```
> display Vr/* osistate

Vr/*
-------------------------------------------------------------------------
|       Vr        |osiAd|osiO|osiUs|Response
|                 | min |per | age |
-------------------------------------------------------------------------
|0                |unlck|ena |activ|
|VOIP             |unlck|ena |activ|
```

**35** Verify that all *ProtocolPorts* components are unlocked, enabled and active:

**display Vr/* Pp/* osistate**

The following shows sample output for this command:

```
> display Vr/* Pp/* osistate

Vr/* Pp/*
+================+====================+-----+----+-----
|       Vr        |          Pp          |osiAd|osiO|osiUs
|                 |                      | min |per | age
+================+====================+-----+----+-----
|0                |ATMMPE                |unlck|ena |activ
|0                |OAMENET0              |unlck|ena |activ
|VOIP             |8600_1A               |unlck|dis |idle
|VOIP             |8600_1B               |unlck|ena |activ
|VOIP             |8600_2A               |unlck|ena |activ
|VOIP             |8600_2B               |unlck|ena |activ
|VOIP             |9K_1_CC               |unlck|ena |activ
|VOIP             |9K_1_OAM              |unlck|ena |activ
|VOIP             |9K_2_CC               |unlck|ena |activ
|VOIP             |9K_2_OAM              |unlck|ena |activ
|VOIP             |9K_3_CC               |unlck|ena |activ
|VOIP             |9K_3_OAM              |unlck|ena |activ
|VOIP             |9K_4_CC               |unlck|ena |activ
|VOIP             |9K_4_OAM              |unlck|ena |activ
|VOIP             |ADTECH#8              |unlck|ena |activ
|VOIP             |NSTA12_IPMCONN        |unlck|ena |activ
|VOIP             |NSTA12_MG             |unlck|ena |activ
|VOIP             |NSTA12_SG             |unlck|ena |activ
|VOIP             |PP_D6_1000_CC         |unlck|ena |activ
|VOIP             |PP_D6_1001_CC         |unlck|ena |activ
|VOIP             |PP_D7_800_CC          |unlck|ena |activ
```

**36** Verify that all Ip components are unlocked, enabled and active:

**display Vr/* Ip osistate**

The following shows sample output for this command:

```
 > display Vr/* Ip osistate

 Vr/* Ip
 ------------------------------------------------------------------------
 |       Vr        |osiAd|osiO|osiUs|Response
 |                 | min |per | age |
 ------------------------------------------------------------------------
 |0                |unlck|ena |activ|
 |VOIP             |unlck|ena |activ|
```

**37** If the Multiservice Switch 15000/Media Gateway 15000/20000 node is connected with GigE to a Passport 8600 node, verify that all *Ospf* components are unlocked, enabled, and active:

**display Vr/* Ip Ospf osistate**

The following shows sample output for this command:

```
 > display Vr/* Ip Ospf osistate

 Vr/* Ip Ospf
 ------------------------------------------------------------------------
 |       Vr        |osiAd|osiO|osiUs|Response
 |                 | min |per | age |
 ------------------------------------------------------------------------
 |VOIP             |unlck|ena |activ|
```

**38** If the Multiservice Switch 15000/Media Gateway 15000/20000 is connected with GigE to a Passport 8600, verify that the state of the *Ospf neighbor* components is "full":

**display Vr/* Ip Ospf Nbr/* state**

The following shows sample output for this command:

```
> display Vr/* Ip Ospf Nbr/* state

Vr/* Ip Ospf Nbr/*,*
-------------------------------------------------
|       Vr        |    address    |address|state
|                 |               |LessInd|
|                 |               |  ex   |
-------------------------------------------------
|1                |14.22.8.2      |      0|full
|1                |14.22.9.2      |      0|full
|1                |18.22.65.1     |      0|full
```

**39** Verify that the static routes are up.

The ""osiOper" (operational state) of all static routes are *ena* (enabled). In addition, if a protected default route (addr = 0.0.0.0 and mask = 0.0.0.0), the "protL" (protection level) must be "cardPro" (card protected).

**display Vr/* Ip static routeEntry/* operationalState, protectionLevel**

The following shows sample output for this command:

```
> display Vr/* Ip static routeEntry/* operationalState,protectionLev

Vr/* Ip Static Route/*,*,*
-------------------------------------------------------------------
|       Vr       |     addr      |     mask      |tos|osiO|protL
|                |               |               |   |per |
-------------------------------------------------------------------
|VOIP            |0.0.0.0        |0.0.0.0        |  0|ena |cardPro
|VOIP            |10.0.32.0      |255.255.240.0  |  0|ena |notApp
```

**40** Verify that all *Nexthop* components under static routes have an operational status of enabled:

**display Vr/VoIP Ip static route/* nexthop/* operationalState**

The following shows sample output for this command:

```
Vr/VOIP Ip Static Route/*,*,* Nh/*
-----------------------------------------------------------
|     addr       |     mask       |tos|       Nh        |osiO
|                |                |   |                 |per
-----------------------------------------------------------
|0.0.0.0         |0.0.0.0         |  0|10.48.0.97       |ena
|0.0.0.0         |0.0.0.0         |  0|10.48.0.129      |dis
|10.0.16.0       |255.255.240.0   |  0|10.48.0.2        |ena
|10.0.32.0       |255.255.240.0   |  0|10.48.0.10       |ena
|10.15.1.0       |255.255.255.0   |  0|10.48.1.65       |dis
|10.16.16.0      |255.255.240.0   |  0|10.48.0.2        |ena
|10.16.32.0      |255.255.240.0   |  0|10.48.0.10       |ena
```

**41** Verify that all *Vsp* components are unlocked, enabled and active:

**display Lp/* Vsp osistate** (for VSP3 - NTHW84xx)
and/or
**display Dlep/* Vsp osistate** (for VSP3-0 - NTHW77xx)

The following shows sample output for the second command:

```
> display Dlep/* Vsp osistate

Dlep/* Vsp
-----------------------------------------------------------------
|Dlep|osiAd|osiO|osiUs|Response
|    | min |per | age |
-----------------------------------------------------------------
|   6|unlck|ena |activ|
```

**42** Verify that all *ProcessingModule* components are unlocked, enabled and active:

**display Lp/* Vsp PModule/* osistate** (for VSP3 - NTHW84xx) and/or
**display Dlep/* Vsp PModule/* osistate** (for VSP3-0 - NTHW77xx)

The following shows sample output for the second command:

```
> display Dlep/* Vsp Pm/* osistate

Dlep/* Vsp PModule/*
-------------------------------------------------------------------
|Dlep|PModule|osiAd|osiO|osiUs|Response
|    |       | min |per | age |
-------------------------------------------------------------------
|   6|      1|unlck|ena |activ|
|   6|      2|unlck|ena |activ|
|   6|      3|unlck|ena |activ|
|   6|      4|unlck|ena |activ|
|   6|      5|unlck|ena |activ|
|   6|      6|unlck|ena |activ|
|   6|      7|unlck|ena |activ|
|   6|      8|unlck|ena |activ|
|   6|      9|unlck|ena |activ|
|   6|     10|unlck|ena |activ|
|   6|     11|unlck|ena |activ|
|   6|     12|unlck|ena |activ|
|   6|     13|unlck|ena |activ|
|   6|     14|unlck|ena |activ|
|   6|     15|unlck|ena |activ|
|   6|     16|unlck|ena |activ|
|   6|     17|unlck|ena |activ|
|   6|     18|unlck|ena |activ|
|   6|     19|unlck|ena |activ|
|   6|     20|unlck|ena |activ|
|   6|     21|unlck|ena |activ|
|   6|     22|unlck|ena |activ|
|   6|     23|unlck|ena |activ|
```

**43** Verify that all *Nsta* components are unlocked, enabled and active:

**display Nsta/* osistate**

The following shows sample output for this command:

```
> display Nsta/* osistate

Nsta/*
-------------------------------------------------------------------
|Nsta |osiAd|osiO|osiUs|Response
|     | min |per | age |
-------------------------------------------------------------------
|   12|unlck|ena |activ|
```

**44** Verify that all *TDMAccessGroup* components are unlocked, enabled and active:

**display Nsta/* vgs tag/* osistate**

The following shows sample output for this command:

```
> display Nsta/* vgs tag/* osistate

Nsta/* Vgs Tag/*
-------------------------------------------------------------------------
|Nsta |  Tag   |osiAd|osiO|osiUs|Response
|     |        | min |per | age |
-------------------------------------------------------------------------
|   12|     111|unlck|ena |idle |
|   12|     122|unlck|ena |idle |
|   12|     133|unlck|dis |idle |
```

**45** Verify that all *Aal1Ces* components are unlocked and enabled:

**display Aal1Ces/* osistate**

The following shows sample output for this command:

```
> display Aal1Ces/* osistate

Aal1Ces/*
--------------+----+-----+-------+-------+-------+-------+----+-----
|Aal1Ces|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|       | min |per | age |   l   |       |   l   |   m   |tby | knw
--------------+----+-----+-------+-------+-------+-------+----+-----
|  10011|unlck|ena |activ|       |       |       |       |nSet|false
|  10012|unlck|ena |activ|       |       |       |       |nSet|false
|  10013|unlck|ena |activ|       |       |       |       |nSet|false
|  10014|unlck|ena |activ|       |       |       |       |nSet|false
|  10021|unlck|ena |activ|       |       |       |       |nSet|false
|  10022|unlck|ena |activ|       |       |       |       |nSet|false
|  10023|unlck|ena |activ|       |       |       |       |nSet|false
|  10024|unlck|ena |activ|       |       |       |       |nSet|false
|  10031|unlck|ena |activ|       |       |       |       |nSet|false
|  10032|unlck|ena |activ|       |       |       |       |nSet|false
|  10033|unlck|ena |activ|       |       |       |       |nSet|false
|  10034|unlck|ena |activ|       |       |       |       |nSet|false
|  10041|unlck|ena |activ|       |       |       |       |nSet|false
```

**46** Verify that all *IpMConn* components are unlocked, enabled and active:

**display Nsta/* vgs IpMConn osistate**

The following shows sample output for this command:

```
> display Nsta/* vgs IpMConn osistate

Nsta/* Vgs IpMConn
-------------------------------------------------------------------
|Nsta |osiAd|osiO|osiUs|Response
|     | min |per | age |
-------------------------------------------------------------------
|   12|unlck|ena |activ|
```

**47** Verify that all *ControlConnection* components are unlocked, enabled and active:

**display Nsta/* vgs Ctrl/* osistate**

The following shows sample output for this command:

```
> display Nsta/* vgs Ctrl/* osistate

Nsta/* Vgs Ctrl/*
-------------------------------------------------------------------------
|Nsta |Ctrl|osiAd|osiO|osiUs|Response
|     |    | min |per | age |
-------------------------------------------------------------------------
|   12|mg  |unlck|ena |activ|
|   12|sg  |unlck|ena |activ|
```

**48** Verify that all *vt1dot5* components are unlocked and enabled:

**display Laps/* Sts/* vt1dot5/* osistate**

The following shows sample output for this command:

```
> display Laps/* Sts/*  vt1dot5/* osistate

Laps/* Sts/* Vt1dot5/*,*
-----------------------------------------------------------------------
|Laps |Sts|l|m|osiAd|osiO|osiUs|osi  |osi |osi  |osi  |osiS|osiUn
|     |   | | | min |per | age |Avail|Proc|Cntrl|Alarm|tby | knw
-----------------------------------------------------------------------
|  120|  0|1|1|unlck|ena |busy |     |    |     |     |nSet|false
|  120|  0|1|2|unlck|ena |busy |     |    |     |     |nSet|false
|  120|  0|1|3|unlck|ena |busy |     |    |     |     |nSet|false
|  120|  0|1|4|unlck|ena |busy |     |    |     |     |nSet|false
|  120|  0|2|1|unlck|ena |busy |     |    |     |     |nSet|false
|  120|  0|2|2|unlck|ena |busy |     |    |     |     |nSet|false
|  120|  0|2|3|unlck|ena |busy |     |    |     |     |nSet|false
```

**49** Verify that all *vt1dot5 DS1* components are unlocked and enabled:

**display Laps/* Sts/* vt1dot5/* ds1/* osistate**

The following shows sample output for this command:

```
> display Laps/* Sts/* vt1dot5/* ds1/* osistate

Laps/* Sts/* Vt1dot5/*,* DS1
--------------------------------------------------------------------------
|Laps |Sts|l|m|osiAd|osiO|osiUs|osi  |osi |osi  |osi  |osiS|osiUn
|     |   | | | min |per | age |Avail|Proc|Cntrl|Alarm|tby | knw
--------------------------------------------------------------------------
| 1300|  0|1|1|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|1|2|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|1|3|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|1|4|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|2|1|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|2|2|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|2|3|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|2|4|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|3|1|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|3|2|unlck|ena |busy |     |    |     |     |nSet|false
```

**50** Verify that all *vt1dot5 DS1 Chan* components are unlocked and enabled:

**display Laps/* Sts/* vt1dot5/* ds1/* chan/* osistate**

The following shows sample output for this command:

```
> display Laps/* Sts/* vt1dot5/* ds1/* chan/* osistate

Laps/* Sts/* Vt1dot5/*,* DS1 Chan/*
--------------------------------------------------------------------------
|Laps |Sts|l|m|Chan|osiAd|osiO|osiUs|osi  |osi |osi  |osi  |osiS|osiUn
|     |   | | |    | min |per | age |Avail|Proc|Cntrl|Alarm|tby | knw
--------------------------------------------------------------------------
| 1300|  0|1|1|   0|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|1|2|   0|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|1|3|   0|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|1|4|   0|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|2|1|   0|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|2|2|   0|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|2|3|   0|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|2|4|   0|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|3|1|   0|unlck|ena |busy |     |    |     |     |nSet|false
| 1300|  0|3|2|   0|unlck|ena |busy |     |    |     |     |nSet|false
```

**51** Verify that all *CasDefn* components are unlocked, enabled and active:

**display Nsta/* vgs casdefn/* osistate**

The following shows sample output for this command:

```
> display Nsta/* vgs casdefn/* osistate

Nsta/* Vgs CasDefn/*
--------------------------------------------------------------------------
|Nsta |CasDefn|osiAd|osiO|osiUs|Response
|     |       | min |per | age |
--------------------------------------------------------------------------
|   12|      0|unlck|ena |activ|
```

**52** Verify that all *IsdnUserAdaption* components are unlocked, enabled and active:

**display Nsta/* vgs iua/* osistate**

The following shows sample output for this command:

```
> display Nsta/* vgs iua/* osistate

Nsta/* Vgs Iua
----------------------------------------------------------------------
|Nsta |osiAd|osiO|osiUs|Response
|     | min |per | age |
----------------------------------------------------------------------
|    2|unlck|ena |activ|
|   11|unlck|ena |activ|
```

**53** Verify that all *Q921* components are unlocked, enabled and active:

**display Nsta/* vgs q921/* osistate**

The following shows sample output for this command:

```
> display Nsta/* vgs q921/* osistate

Nsta/* Vgs Q921/*
------------------------------------------------------------------------
|Nsta |Q921|osiAd|osiO|osiUs|Response
|     |   | min |per | age |
------------------------------------------------------------------------
|   12|  22|unlck|ena |activ|
```

**54** If the node being migrated relies on OAM Ethernet connectivity, verify that the active control processor has Ethernet connections with a value of up:

**display Lp/0 Oamenet/0 activeStatus**

The following shows sample output for this command:

```
> display Lp/0 Oamenet/0 activeStatus
Lp/0 OamEnet/0
   activeStatus = available
```

***Note:*** If the Multiservice Switch 15000/Media Gateway 15000 node is using in-band OAM, only the gateway node needs Ethernet connectivity. You may have an Ethernet connection to a remote node for emergency access.

**55** If the node being migrated relies on OAM Ethernet connectivity, verify that the standby control processor has Ethernet connections with a value of up:

**display Lp/0 Oamenet/0 standbyStatus**

The following shows sample output for this command:

```
> display Lp/0 Oamenet/0 standbyStatus
Lp/0 OamEnet/0
   standbyStatus = available
```

**56** Optionally, display, ping, and record information about the IP accessibility of the node to verify the reachability of the node:

**list ac ipaccess/***

The following shows sample output for this command:

```
> list ac ipaccess/*
Ac IpAccess/10.0.0.0
Ac IpAccess/47.0.0.0
```

**57** Verify and record information about the IP reachability of the first Preside MDM server from the node:

**ping -trace -ip(<MDM1 IP>) Vr/0 Ip Icmp**

The following shows sample output for this command:

```
> ping -trace -ip(10.47.0.3) Vr/0 Ip Icmp
Vr/0 Ip Icmp
   IP Trace Route for 10.47.0.3:
   Path taken:
     Hop 1:   10.47.0.3       (time = 1ms)
```

**58** Verify and record information about the IP reachability of the second Preside MDM server from the node:

**ping -trace -ip(<MDM2 IP>) Vr/0 Ip Icmp**

In conjunction with step 57, ensure that both Preside MDM servers are connected to this node with as diverse paths as possible, and that each server is accessible.

The following shows sample output for this command:

```
ping -tr -ip(10.47.0.2) Vr/0 Ip Icmp
Vr/0 Ip Icmp
   IP Trace Route for 10.47.0.2:
   Path taken:
     Hop 1:   10.47.0.2       (time = 1ms)
```

### Variable values

| Variable | Value |
|---|---|
| <laps_inst> | The instance value of the *Laps* component whose manual overrides you want to remove. This instance value is an integer between 0 and 15999. |

# HSM (Command Console) activation

Perform the HSM by setting the application version list, setting the patchlist, if required, and activating the provisioning changes. When the activation completes, the node will be running the new software.

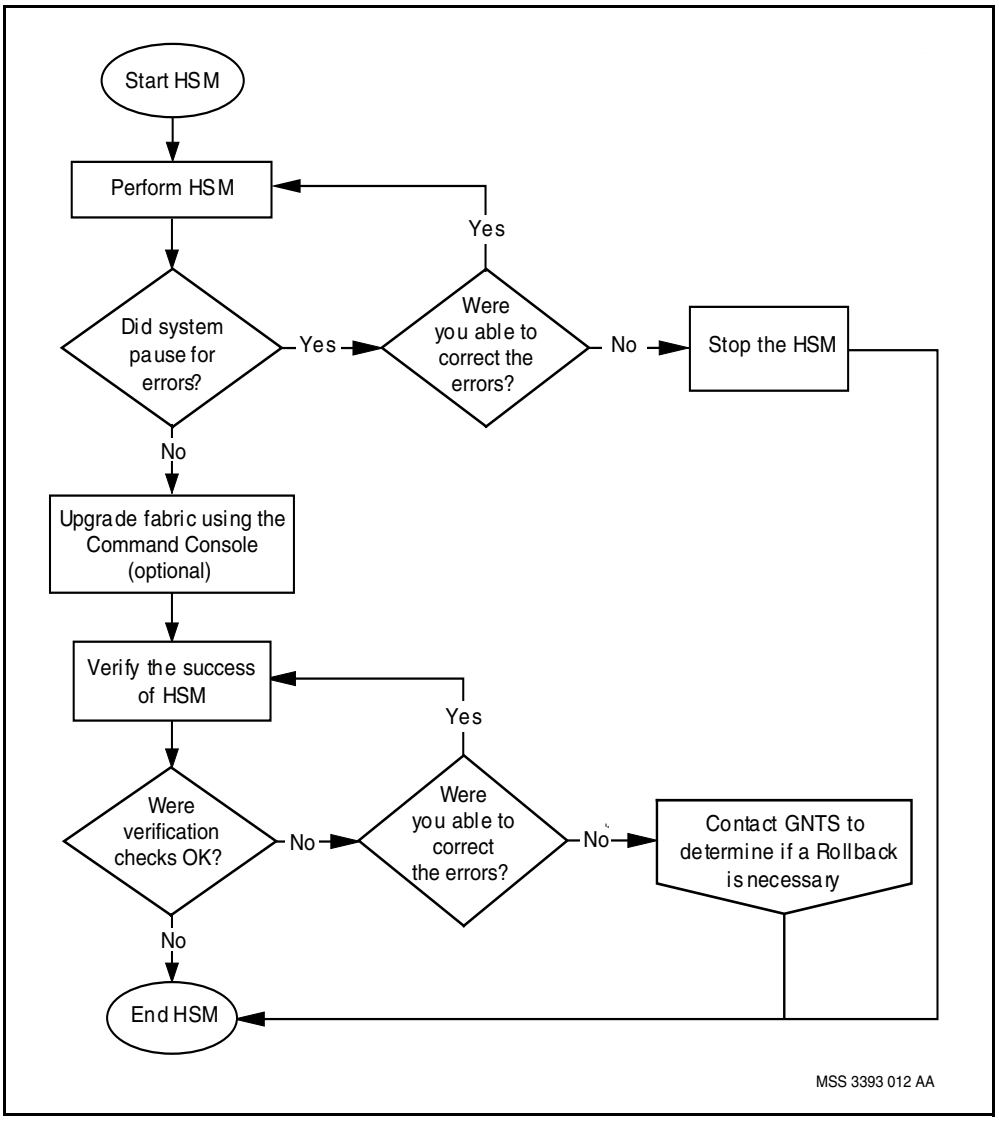
## Prerequisites

- Complete the HSM pre-work. See HSM (Command Console) pre-work on page 1236 for more information.
- Upgrade the Multiservice Switch 15000/Media Gateway 15000 nodes in UA-IP, PT-IP, PT-AAL2, IAC or IAW solution networks one at a time in the order decided on when you performed in x.

## HSM task flow

The task flow shows the sequence of procedures you need to perform the HSM. To link to any procedure, go to the Work flow navigation on page 1262.

### HSM task flow




## Work flow navigation

- Perform HSM using Command Console on page 1263
- Upgrade the fabric on page 1279
- Verify the success of HSM on page 1287
- Stop the HSM using Command Console on page 1294

# Perform HSM using Command Console

Upgrade Multiservice Switch 15000/Media Gateway 15000/20000 nodes in UA-IP, PT-IP, PT-AAL2, IAC or IAW solution networks by setting the application version list, setting the patchlist, if required, and activating the provisioning changes. When the activation completes, the node will be running with the new software.

## Prerequisites to performing the hitless software migration



**CAUTION**
**Calls being setup are dropped**
This strategy removes standby control and function processors from service. As a result, redundancy in the event of failure of the active shelf components is not available and some calls in the process of being set up (known as transient calls) are dropped. Stable calls are unaffected by the migration.

Undertake the procedures required by this strategy during low-traffic periods.

- Perform HSM Pre-work.
- Do not load the software application for the fabric. Refer to Upgrade the fabric on page 1279 for more information about upgrading the fabric firmware.
- Do not modify the “sw avl, pa” lists using the command “load -f (<view name>) prov”. When performing HSM using the Command Console, enter the new “sw avl, pa” lists manually. Use of the “load” command could result in a disruptive software migration.
- Perform this upgrade using the Command Console tool on Nortel Networks Preside Multiservice Data Manager (MDM) server rather than a Telnet session. Using the Command Console, ensures that you remain connected to the node and can monitor the CP switchover. For more information on opening the Command Console, see 241-6001-804 *Preside MDM Workstation Utilities User Guide*.
- The Multiservice Switch 15000/Media Gateway 15000/20000 node in UA-IP, PT-IP, PT-AAL2, IAC or IAW solution networks must contain two control processors (CP). One CP must be active and the other CP must be in standby mode.
- Hitless software migration only applies to FPs in a one-for-one equipment sparing configuration. The active FPs must be

provisioned for one-for-one equipment sparing. During the software migration, equipment protection is unavailable for those cards whose standby card is part of the migration shelf.

- While you perform software migration tasks, the system may interrupt the process to display warnings or notifications. Some of these notifications may require you to confirm your intent before continuing. Respond as required by the online instructions.
- You must have an advanced knowledge of Unix, the Multiservice Switch/Media Gateway software, and Succession portfolio architecture.
- Activate the same software applications in SN07 as are present in the current software release (SN06/SN06.2) to allow hitless software migration. These applications may include: base, networking, atmNetworking, ip, wanDte, ethernet, pvg, and aal1Ces. WanDte is not mandatory for all upgrades. It must only be downloaded and activated in SN07 if it is present in the pre-SN07 release.

  ***Note:*** The ethernet application is required in SN07 to load software on 4pGigE function processors. However since the ethernet application is not present in releases prior to SN07, customers must use a specific pre-SN07 patch to perform a HSM from software releases earlier than SN07. Refer to step 4 of Download software from the Preside MDM server on page 459 or step 6 in this procedure.

- Refer to the software downloads area of the Nortel Networks Web site (*www.nortelnetworks.com*) to determine the software patches that you need to add to the patchlist. If there are no patches listed for this release, it means that there are no patches currently required for this release.

***From the node***

1 Login to the node using the appropriate permissions.

2 Enter provisioning mode so that you can issue the appropriate commands:

**start prov**

The following shows sample output for this command:

```
7> start prov
Prov
The edit view differs from the current view.
Added 2 provisioning component(s) to the edit view.
```

***Note:*** If the system indicates that the edit view and the current view are the same, proceed to step 4.

3 Copy the current view into the edit view to ensure that they are identical:

**copy prov**

***Note:*** If you were referenced to this step as a method to abort the migration before activation, no outage will occur as you have not yet started the hitless software migration.

4 Display the current software application version list:

**display -c Software avList**

The following shows sample output for this command:

```
> display -c software avlist
Sw
   avList = base_CF0129E,          networking_CF0129E,    atmNetworking_CF0129E,
            ip_CF0129E,            wanDte_CF0129E,        ethernet_CF0129E,
            pvg_CF0129E,           aal1Ces_CF0129E
```

***Note:*** If you are upgrading a Media Gateway 15000/20000 from SN06 or SN06.2 to SN07 in an UA-IP, PT-IP, PT-AAL2, IAC, or IAW solution networks, and there are 4pGigE Function Processors (4pGe FP) active on the node, go to step 6. If no 4pGe FPs are active, go to step 5 and skip step 6.

To perform a software upgrade on Media Gateway 7480 elements, or a non-hitless upgrade on Media Gateway 15000/20000 refer to NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software* guide for information.

5 Replace all of the old application versions in the application version list with the new application versions:

**set Software avList ! <new_applications>**

The software applications you need to load are base, networking, atmNetworking, ip, wanDte, ethernet, pvg, and aal1Ces. Do not add any other applications to the application version list. Go to step 7.

***Note:*** Do not set the software applications for the fabric. Refer to Upgrade the fabric on page 1279 for more information about upgrading the fabric firmware.

```
> set software avlist ! base_CF0130E networking_CF0130E
atmNetworking_CF0130E
ip_CF0130E wanDte_CF0130E pvg_CF0130E aal1Ces_CF0130E
```

***Note:*** You may need to set a different list of software application versions.

6 Replace all of the old application versions in the application version list with the new application versions:

**set Software avList ! <new_applications>**

**set Software avList ethernet_CF01D**

***Note:*** For HSM to occur on Media Gateway15000/20000 in UA-IP, PT-IP, PT-AAL2, IAC or IAW solution networks, the new and old applications must be identical (except the load name, e.g. if SN06.2 applications are base, networking, ip, pvg, aal1Ces, atmNetworking, and wanDte then SN07 applications must be the same). However, 4pGe FP in SN07 requires an additional application (ethernet). Normally such an addition would cause a non hitless software migration to occur but patch baseFT397A_CE02S2D in SN06.2 (and its equivalent in SN06) allows the HSM to proceed without problem.

7 Check that the new applications are in the application version list and that the applications are the same as those listed in step 4 (apart from the load name):

**display Software avList**

The following shows sample output for this command:

```
> display software avlist
Sw
   avList = base_CF0130E,  networking_CF0130E,
atmNetworking_CF0130E,
            ip_CF0130E,   wanDte_CF0128H,  ethernet_CF0130E,
            pvg_CF0130E,   aal1Ces_CF0130E
```

***Note 1:*** If you are upgrading a Media Gateway15000/20000 from SN06 or SN06.2 to SN07 in a PT-IP, PT-AAL2, IAC or IAW solution networks, go to step 9.

***Note 2:*** If you upgrading a Multiservice Switch 15000 in UA-IP solution, go to step 8.

**8**



**CAUTION**
**Clear the patch list prior to software migration**
Regardless of whether patches are being applied, execute the following command to clear the patch list prior to software migration: **set software patchlist !**

See the Nortel Networks Multiservice Switch Release Notes for PCR 6.1 to determine the software patches required and apply the patches if needed for SN07 to the patchlist.

***Note:*** This procedure applies only to non-disruptive patches.

**set Software patchlist ! <patches>**

**Attention**: If you are migrating directly from a pre-SN07 release to SN07 FVS with patches, you must apply a patch to your current release before downloading the SN07 FVS software.

Switches must be running baseFT420A_XXXX.

Once this patch is applied, download the SN07FVS software, including patch_CF01xxx. Then migrate to SN07FVS with patches as described in this procedure.

Contact Nortel Networks Global Network Product Support to obtain the appropriate baseFT420A_XXXX migration patch. The patch readme file contains download and activation instructions.

**9** Verify that the patch list is set correctly:

**display -c Software patchlist**

The following shows sample output for this command:

```
PROV 2> d -c Sw patchlist
Sw
 patchlist = atmNetworkingFT032A,
baseFT173A,      baseFT172A,
```

**10**



**CAUTION**
**Potential interruption of calls in progress**
The software upgrade for Multiservice Switch 15000/Media Gateway 15000 nodes is hitless if the new provisioning view contains only the new AVL and optionally, a new patch list. If the system indicates that more than one provisioning change has occurred and one of those two changes was not clearing a patchlist and setting a new one, the node will go through a software migration that is not hitless and all calls on the node are interrupted.

If more than one provisioning change has occurred, repeat step 3 and then perform the procedure Verify the success of HSM on page 1287.

Verify that the *editViewChangedComponents* attribute indicates that you have made only one provisioning change:

The following shows a sample output for the command:

**display -o prov**

```
> display -o prov
Prov
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   provisioningActivity = none
   activityProgress     = n/a
   standbyCpActivity    = none
   standbyCpActivityProgress = n/a
   committedFileName         = UAIP_CF0129E_Complete.full.005
   currentViewFileName       = UAIP_CF0129E_Complete.full.005
   lastUsedFileName          = UAIP_CF0129E_Complete.full.005
   provisioningSession       = Nmis Fmip Session/6
   provisioningUser          = MAINT
   checkRequired             = no
   confirmRequired           = no
   editViewName              = none
   editViewAddedComponents   = 0
   editViewDeletedComponents = 0
   editViewChangedComponents = 1
   currentJournal            = 0
   journalDisabledReason     = not disabled
   restorePossible           = no
```

**11**



**CAUTION**
**Proceeding with a non-hitless software migration**
The nodes will go through a software migration that is not hitless and all calls on the node are interrupted if the system returns the following message:

*All applications will experience service outage.*

If this happens, fix the problem and repeat step 11 or stop the migration if you cannot fix the problem.

Perform a semantic check:

**check prov**

The node can continue with a hitless software migration if the system returns the following message:

Some applications may experience service outage.

The following shows sample output for this command:

```
PROV 2> check prov
Lp/0
   Warning:
      Reason:  Lp 0 (card 0) will be reset when this view is activated.
Lp/8
   Warning:
      Reason:  Lp 8 (card 8) will be reset when this view is activated.
Lp/10
   Warning:
      Reason:  Lp 10 (card 10) will be reset when this view is activated.
Prov
   Warning:
    Activation will disrupt service for the following component(s):
         Lp/0,
         Lp/8,
         Lp/10
   Warning:
    Activation will result in a software migration system reload. Some
   applications may experience service outage.
```

**12** Save the edit view with portable formats:

**save -f(<filename>) -portable prov**

Use a consistent naming convention for all view files and ensure the filename corresponds to the new load.

For example:

UAIP_CF0SXX_UNIQUE_IDENTIFIER

"UAIP" identifies the Succession Solution. “CF01SXX" identifies the Multiservice Switch 15000 software application version. The “UNIQUE_IDENTIFIER" is the part of the naming convention that helps identify the provisioning contained by a view.

13



**CAUTION**
**Unexpected messages about the logical processors**
If the system gives you unexpected messages about the logical processors during the migration, abort the migration. For more information see Stop the HSM using Command Console on page 1294.

Apply the changes:

**activate -pause prov**

***Note:*** The system can pause for one of two reasons: the system has found a fault or an operator issued a pause command. If the system pauses because the operator has used the -pause command, the operator can issue the continue -prov command to continue the HSM.

### Sample output for successful pause

```
PROV> activate -pause prov ... continued ...

The software migration is paused, pause reason:
Details:
ACTIVATE -PAUSE PROV operator command

To resume, type Continue Prov. To stop, type Stop Prov.
```

The following sample shows an example of a failed output for this command.

### Sample output for failed pause

```
PROV> activate -pause prov ... continued ...
The software migration is paused, pause reason:
Details:
On Card 1: some appls(s) may not be ready for SO.
ACTIVATE -PAUSE PROV operator command.

To resume, type Continue Prov.  To stop, type Stop Prov.

PROV> continue prov
Prov
Continue Prov failed due to a pausable event, pause reason:
Details:
On Card 1: some appl(s) may not be ready for SO.
Use -force option to continue the migration.  To abort
migration type Stop Prov.
```

**14**



**CAUTION**
**Unexpected messages about the logical processors**
If the system gives you unexpected messages about the logical processors during the migration, abort the migration. For more information see Stop the HSM using Command Console on page 1294.



**CAUTION**
**Exercise caution when using the continue -force prov command**
Contact Nortel Networks Global Networks Technical Support (GNTS) for advice or assistance before issuing a **continue -force prov** command during a software migration pause.

Always issue a continue prov command:

**continue prov**

The migration is now taking place. The time required to complete the migration depends on the number of calls and components

that have been provisioned on the node. Generally, migrations take between fifteen minutes and three and a half hours.

***Note 1:*** After you enter **activate prov**, after the CP switchover during the hitless software migration, connectivity between the node and Preside MDM server is temporarily lost. The active alarms for the node clear and the node appears grey in the Network Viewer until the connection is re-established. The connection between the node and the server re-establishes itself automatically within a minute. Messages, such as the following, may be observed on the Command Console and the system log display during this time:

(Command Console): `CC_ERROR 1019 Passport Register Command error: APPLICATION_ERROR 1122 FMIP connection locked or down, command terminated`

(System log display): `CO: APPLICATION_ERROR 1112 Fdtr lost connection to DESIGN_2 W MSG 00000001 NMS ft1400-2 (25335) 15-13:37:02CO: APPLICATION_ERROR 1111 Fdtr cannot connect to DESIGN_2 because the connection was lost`

***Note 2:*** If there are any logical processors that cannot participate in the hitless software migration because of provisioning reasons (for example, they are unspared or in a 1 for N configuration) or because of operational reasons (for example, a standby card is unavailable), the system identifies these logical processors.

***Note 3:*** If the list of logical processors changes during the software migration, the system generates a *Migration Visible Alarm*, which pauses the software migration. You have three options at this point, abort (**stop prov**), fix the problem and continue (**continue -force prov**), or ignore the problem and continue (**continue -force prov**).

You can choose to abort the migration at this time. For more information, see Stop the HSM using Command Console on page 1294. You can choose to continue the migration by typing **continue -force prov.**

15 To monitor the progress of the migration, enter the following command:

**display -o prov**

The results of this command are constantly updated in operational mode. Even when the node is reconnecting, you can use this command to monitor the upgrade.

You can continue to issue this command up until you lose connectivity to the node. When the active control processor begins to load the software, connectivity is lost. After you lose connectivity, you will need to log back into the node (see step 16). If you are using Preside MDM Command Console, the connection to the node is automatically re-established, but you will need to get back into provisioning mode. For more information, see step 17.

The following shows sample output for this command:

```
52> display -o prov
Prov
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   provisioningActivity = activation
   activityProgress     = software migration in progress
   standbyCpActivity    = loading new software on CP
   standbyCpActivityProgress = 10%
  committedFileName       = CF01S1A_with_base_Mar22_04.full.006
  currentViewFileName     = CF01S1A_with_base_Mar22_04.full.006
  lastUsedFileName         = CF01S1A_with_base_Mar22_04.full.006
   provisioningSession       =
   provisioningUser          = none
   checkRequired             = no
   confirmRequired           = no
   editViewName              = CF01S1A_base_Mar22_04.full.006
   editViewAddedComponents   = 0
   editViewDeletedComponents = 0
   editViewChangedComponents = 0
   currentJournal            = 0
   journalDisabledReason     = not disabled
   restorePossible           = no
```

These four attributes describe the progress of the migration. They will be updated as the migration proceeds.

**16** If using Telnet, when prompted, login to the node with the appropriate permissions.

**17** Enter provisioning mode: **start prov**

**18** Within 20 minutes of activating the new software and completing the software migration, confirm the changes to avoid a non-hitless rollback to the previously committed configuration:

**confirm prov**

The following shows sample output for this command:

```
PROV 3> confirm prov
Prov
   Activation confirmed. Rollback will not
occur.
```

**19** Check that the edit view is the same as the current view:

**copy prov**

The message should confirm that both views are the same.

The following shows sample output for this command:

```
4> st pr
Prov
The edit view is identical to the current view.
 The current view needs to be semantically checked.
Issue:
    Copy Prov
    Check Prov
to correct. It may also be advisable to re-save
or re-commit.
```

**20** Perform a semantic check on the changes: **check prov**

You may see warnings during the semantic check, but they will not disrupt service.

***Note:*** If the semantic check fails, troubleshoot the problem using “Troubleshooting a software upgrade” in *Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP)*, NN10419-461.

**21** If the semantic check passes, save the view:

**save prov**

**22** If the semantic check passes, commit the final version of the view:

**commit prov**

The following shows sample output for this command:

```
PROV 9> commit prov
Prov
  Saving the current view into CF0151A_base_Mar22_04.full.006
(with commit,portable formats) ...
Prov
  The committed file is CF0151A_base_Mar22_04.full.006.
```

A committed file is required in case of a node reset, at which time the committed view will be reloaded.

**23** Verify that the edit view and the current view are the same:

**display -o prov**

The following shows sample output for this command:

```
20> display -o prov
Prov
adminState = unlocked
operationalState = enabled
usageState       = idle
provisioningActivity = none
activityProgress     = n/a
standbyCpActivity    = none
standbyCpActivityProgress = n/a
committedFileName       = CF0151A_base_Mar22_04.full.006
currentViewFileName     = CF0151A_base_Mar22_04.full.006
lastUsedFileName        = CF0151A_base_Mar22_04.full.006
provisioningSession       =
provisioningUser          = none
checkRequired             = no
confirmRequired           = no
editViewName            = CF0151A_base_Mar22_04.full.006
editViewAddedComponents   = 0
editViewDeletedComponents = 0
editViewChangedComponents = 0
journalUsage              = 0 %
journalDisabledReason     = not disabled
restorePossible           = no
```

24



**CAUTION**
**Do not enable autopatch feature in SN07 for Media Gateway 7480/15000/20000**

Media Gateway 7480/15000/20000 customers should NOT enable the auto patch application feature or perform hitless software FP patching in SN07 as outlined in the NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software* guide. Media Gateway 7480 customers must still perform two upgrades: one from SN06 or SN06.2 to SN07 FCS and the second to apply patches in SN07 FCS. Before applying patches in SN07, Media Gateway 7480 customers must Download the Patch Av from the Multiservice Switch SDS in order to view the patches on the switch and enter provisioning mode so commands can be issued. See NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software* for more details on how to apply patches in SN07.

Exit provisioning mode after the migration is complete:

**end prov**

**Variable values**

| Variable | Value |
|---|---|
| <filename> | The name of the file that contains the committed or portable provisioning data. The variable must be between 1 and 31 characters in length. Use a consistent naming convention. |
| <new_applications> | A space-separated, case-sensitive list of application versions. The release is indicated by the version number after the underscore. |

### Variable values

| Variable | Value |
|---|---|
| | The applications required for Succession UA-IP are base, networking, atmNetworking, ip, wanDte, ethernet, pvg, and aal1Ces. The application version list must not contain any additional applications. *Note*: WanDte is not mandatory for all upgrades. It must only be downloaded and activated in SN07 if it is present in the pre-SN07 release. |
| <patches> | A space-separated, case-sensitive list of patches. The patches you need to add to the patch list are listed at the software downloads area of Nortel Networks website. |

# Upgrade the fabric

You can upgrade the fabric firmware installed on Nortel Networks Multiservice Switch 15000 fabric cards to take advantage of enhancements and new functionality contained in later firmware releases. All software running on Multiservice Switch 15000 nodes is compatible with any firmware running on the fabric cards.



**CAUTION**
**Loss of redundancy in the transport fabric**
This upgrade strategy results in a loss of redundancy in the transport fabric.

Undertake the procedures required by this strategy during low-traffic periods.

Use this procedure to upgrade a Media Gateway 15000/20000 from SN06 or SN06.2 to SN07 in UA-IP, PT-IP, PT-AAL2, IAC, or IAW solution networks.

## Prerequisites

- You do not need to upgrade the fabric card firmware every time you upgrade the control and function processor software. An alarm is raised by the system whenever a newer version of the fabric card firmware is available. To see if you need to upgrade the transport fabric firmware, see *Nortel Networks Multiservice Switch Release Notes PCR6.1*.
- The new fabric card firmware must be downloaded from a Nortel Networks Preside Multiservice Data Manager (MDM) server acting as the software distribution site (SDS). For more information on how to download from the SDS, see NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software*.
- You can install new fabric card firmware at any time during normal node operation. Installing the new fabric firmware during off-peak hours will limit loss of data on the fabric switchover.
- The node must contain two fabric cards. A single fabric card shelf cannot be upgraded.
- The fabric card that is receiving the new firmware version must be locked and must not be running any traffic or tests. The fabric card that is not receiving the new firmware version must be unlocked and enabled.

***From the Command Console***

1 Determine if a fabric upgrade is required for Media Gateway 15000/20000:

**display Shelf Fabric/* banks**

If the output is:

```
"recommendedVersionToInstall = Fabric software
version is up to date".
```

a fabric upgrade is not required.

2 Display the attributes of the fabric card banks:

**display Shelf FabricCard/<n> banks**

The following shows sample output for this command:

```
 1> d sh fa/x banks
 Shelf FabricCard/x
 fixedBankVersion = 8.2
 writableBankVersion = 9.3
 recommendedVersionToInstall = CF01S1A
 activeBank                  = writable
 bankOnShelfRestart          = writable
 downloadProgressPercent     = 100 %
 writableBankStatus          = loaded
 ok             2004-02-23 16:57:25.02
```

3 Verify that the required fabric firmware version has been downloaded to the node:

**list Sw Av/Fabric_<version>**

The following shows sample output for this command:

```
2> l sw AV/fabric_CF01S1A
Sw Av/FABRIC_CF01S1A
 Component has no operational subcomponents of the requested
type.
ok             2004-02-23 23:13:25.85
```

If the correct fabric firmware has not been downloaded to the node, see Download software from the Preside MDM server on page 459.

4 Verify both fabrics are enabled and unlocked:

**display Shelf FabricCard/***

The following shows a sample output for this command:

```
> display Shelf FabricCard/*

Shelf FabricCard/*
   Use -noTabular to see the many hidden attributes.
+==========+=====+====+=====+===========+================+=======+==========
|FabricCard|osiAd|osiO|osiUs|productCode |  serialNumber  |failure|dependency
|          | min |per | age |           |                | Cause | InEffect
+==========+=====+====+=====+===========+================+=======+==========
|x         |unlck|ena |activ|NTHR16BA 03 |NNTM03505HG8    |       |
|y         |unlck|ena |activ|NTHR16BA 03 |NNTM03505J03    |       |
```

**5** Verify that the appropriate card ports on both fabrics are in service:

**display Shelf FabricCard/* CardPort/***

All card ports without a *dependenciesInEffect of CardNotInstalled* must be unlocked and enabled.

The following shows sample output for this command:

```
4> d sh fa/* ca/*
Shelf FabricCard/* CardPort/*
Use -noTabular to see the many hidden attributes.
-------------------------------------------------------------------------
|FabricCard|CardPort|osiAd|osiO|osiUs|failures|dependencies|selfTestEr
|          |        | min |per | age |InEffect|  InEffect  | rorCode
-------------------------------------------------------------------------
|x         |       0|unlck|ena |activ|        |            |         0
|x         |       1|unlck|ena |activ|        |            |         0
|x         |       2|unlck|ena |activ|        |            |         0
|x         |       3|unlck|ena |activ|        |            |         0
|x         |       4|unlck|dis |idle |        |cardNo      |         0
|x         |       5|unlck|dis |idle |        |cardNo      |         0
|x         |       6|unlck|ena |activ|        |            |         0
|x         |       7|unlck|ena |activ|        |            |         0
|x         |       8|unlck|dis |idle |        |cardNo      |         0
|x         |       9|unlck|dis |idle |        |cardNo      |         0
|x         |      10|unlck|dis |idle |        |cardNo      |         0
|x         |      11|unlck|dis |idle |        |cardNo      |         0
|x         |      12|unlck|dis |idle |        |cardNo      |         0
|x         |      13|unlck|dis |idle |        |cardNo      |         0
|x         |      14|unlck|dis |idle |        |cardNo      |         0
|x         |      15|unlck|dis |idle |        |cardNo      |         0
|y         |       0|unlck|ena |activ|        |            |         0
|y         |       1|unlck|ena |activ|        |            |         0
|y         |       2|unlck|ena |activ|        |            |         0
|y         |       3|unlck|ena |activ|        |            |         0
|y         |       4|unlck|dis |idle |        |cardNo      |         0
|y         |       5|unlck|dis |idle |        |cardNo      |         0
|y         |       6|unlck|ena |activ|        |            |         0
|y         |       7|unlck|ena |activ|        |            |         0
|y         |       8|unlck|dis |idle |        |cardNo      |         0
|y         |       9|unlck|dis |idle |        |cardNo      |         0
|y         |      10|unlck|dis |idle |        |cardNo      |         0
|y         |      11|unlck|dis |idle |        |cardNo      |         0
|y         |      12|unlck|dis |idle |        |cardNo      |         0
|y         |      13|unlck|dis |idle |        |cardNo      |         0
|y         |      14|unlck|dis |idle |        |cardNo      |         0
|y         |      15|unlck|dis |idle |        |cardNo      |         0
```

**6** Verify that the fabric ports on the cards are unlocked and enabled:

**display Shelf Card/* fabricPort/* state**

The following shows sample output for this command:

```
5> d sh ca/* fabric/* state
Shelf Card/* FabricPort/*
--------------------------------------------------------------------------------
----
|Card|FabricPort|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|    |          | min |per | age |   l   |       |   l   |   m   |tby | knw
--------------------------------------------------------------------------------
----
|   0|x         |unlck|ena |activ|       |       |       |       |nSet|false
|   0|y         |unlck|ena |activ|       |       |       |       |nSet|false
|   1|x         |unlck|ena |activ|       |       |       |       |nSet|false
|   1|y         |unlck|ena |activ|       |       |       |       |nSet|false
|   2|x         |unlck|ena |activ|       |       |       |       |nSet|false
|   2|y         |unlck|ena |activ|       |       |       |       |nSet|false
|   3|x         |unlck|ena |activ|       |       |       |       |nSet|false
|   3|y         |unlck|ena |activ|       |       |       |       |nSet|false
|   6|x         |unlck|ena |activ|       |       |       |       |nSet|false
```

**7** Lock the fabric card to be upgraded:

**lock Shelf FabricCard/<n>**

The following shows sample output for this command:

```
6> lock sh fa/x
Shelf FabricCard/x; 2002-08-12 16:37:34.50
SET critical operator operationalCondition 00001000
ADMIN: locked        OPER: enabled       USAGE: idle
AVAIL:               PROC:               CNTRL:
ALARM:               STBY: notSet        UNKNW: false
Id: 01000057  Rel:
Com: Fabric Card is locked
Int: 1/0/2/29063; bcsBus.cc; 677; ""
Shelf FabricCard/x
ok             2002-08-12 16:37:34.50

Shelf FabricCard/x; 2002-08-12 16:37:34.50
SET critical equipment processorProblem 00001001
ADMIN: locked        OPER: disabled      USAGE: idle
AVAIL: dependency    PROC:               CNTRL:
ALARM:               STBY: notSet        UNKNW: false
Id: 01000058  Rel:
Com: Fabric Card is disabled
```

**8** Install the new firmware on the locked fabric card.:

**install -file(<version>) Shelf FabricCard/<n>**

Wait a few minutes for the firmware to install and for the system to notify the operator of any errors or success.

The following shows sample output for this command:

```
7> install -file(CF01S1A) shelf fabriccard/x
Shelf FabricCard/x
The command has been issued to the fabric card.

7> install -file(CF01S1A) shelf fabriccard/x ... continued ..
Shelf FabricCard/x
The command completed successfully.
ok              2004-02-24 13:09:57.99
```

**9** Display the attributes of the fabric card banks to verify that the upgrade was a success. If the activeBank is set to *fixed*, the fabric card was not able to use the new firmware load and reverted back to the fixed bank. If this happens, contact GNTS.

**display Shelf FabricCard/<n> banks**

The following shows sample output for this command:

```
  8> d sh fa/x banks
  Shelf FabricCard/x
  fixedBankVersion = 8.2
  writableBankVersion = 9.4
  recommendedVersionToInstall = Fabric software version is up
  date.
  activeBank                  = writable
  bankOnShelfRestart          = writable
  downloadProgressPercent     = 100 %
  writableBankStatus          = loaded
  ok 2004-02-24 13:10:01.43
```

**10** Verify that the fabric card operates correctly by running a manual test with the new firmware before you unlock and send live traffic over the card.

**start Shelf FabricCard/<n> test**

The following shows sample output for this command:

```
9> start shelf fabriccard/x test
Shelf FabricCard/x Test
   Test started.

9> stop shelf fabriccard/x test ... continued ...
Shelf FabricCard/x Test
   Test stopped.
ok              2004-02-24 13:12:19.40
```

The test results show whether the fabric card is operating correctly. You can view the results of a test while the bus test is still in progress or after it has completed.

**display Shelf FabricCard/<n> Test results**

If the entry in the *fabricSelfTestResults* attribute shows OK, the fabric card test has passed.

***Note:*** If there are any problems with the upgraded fabric card, see NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* to interpret the test results.

**11**



**CAUTION**
**Fabric card not returning to service**
If the writable bank is set as the committed bank and it becomes corrupt, the fabric card might not come up. If the writable bank is corrupt, it must be replaced. Contact GNTS.

Unlock the fabric card to return it to service:

**unlock Shelf FabricCard/<n>**

***Note:*** The fabric unlock command may time-out because the response is not returned until the fabric has finished running the diagnostics. This is normal.

**12** Repeat step 4 through step 11 for the other fabric card.

**13** If the test result is not OK, or if the writable bank appears not to be working correctly after being unlocked, lock the fabric and revert back to the fixed bank. To set fabric x from the writable bank to the fixed bank, enter the following commands:

***Note:*** By setting *activeBank* to fixed, *bankOnShelfRestart* is also set to fixed.

**lock Shelf FabricCard/<x>**
**set sh fab/<x> activeBank fixed**
**unlock sh fabric Card/<x>**

Contact Nortel Networks Global Networks Technical Support (GNTS) to inform them about the fabric card upgrade failure.

### Variable values

| Variable | Value |
|---|---|
| <n> | The instance value of the fabric card, X or Y. |
| <version> | The firmware that is referred to by the *recommendedVersionToInstall* in 8. |

# Verify the success of HSM

After completing the upgrade, verify that the HSM executed correctly and that the connections are functioning as they were prior to the upgrade.

Should your checks fail, decide whether or not you should continue with the HSM. If you are uncertain, contact GNTS for help deciding.

If an unexpected service disruption occurs with the HSM for Media Gateway15000/20000 upgrades from SN06 or SN06.2 to SN07 in UA-IP, PT-IP, PT-AAL2, IAC, or IAW solution networks, contact Nortel Emergency Response at 1-800-4NORTEL option 9-1. If you are performing a software upgrade on Media Gateway 7480 elements, refer to the NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software* guide.

## Prerequisites

- If your network has a lot of live connections, displaying the status of the logical processors, SONET ports, and ATM interfaces will result in large amounts of output.
- Verify the status of the node before the upgrade on page 1237
- Perform HSM using Command Console on page 1263

### *From the node*

1. Login to the node using the appropriate permissions.
2. Verify that the disk and file systems are synchronized:

   **display FileSystem syncStatus**
3. Verify the *syncProgress* between the disk and file system is 100%:

   **display FileSystem syncProgress**
4. Ensure that network synchronization on the system is enabled, unlocked, synchronized, and free of alarms:

   **display NetworkSynchronization**
5. Compare the status of the fabrics with the status recorded in step 11 of the procedure Verify the status of the node before the upgrade on page 1237:

   **d shelf fabriccard/* osistate**

6 Compare the status of the logical processors with the status recorded in step 12 of the procedure Verify the status of the node before the upgrade on page 1237:

**display Lp/* osistate**

7 Compare the status of the equipment protection with the status recorded in step 13 of the procedure Verify the status of the node before the upgrade on page 1237:

**display Shelf Card/* SparedServices**

8 Compare the status of the logical processors using the dual L sparing model with the status recorded in step 14 of the procedure Verify the status of the node before the upgrade on page 1237:

**display Dlep/* osistate**

9 Compare the status of the Ethernet ports with the status recorded in step 15 of the procedure Verify the status of the node before the upgrade on page 1237:

**display Lp/* Ethernet/* osistate**

10 Compare the status of the SONET ports with the status recorded in step 16 of the procedure Verify the status of the node before the upgrade.:

**display Lp/* Sonet/* osistate**

11 Compare the status of the *lop, ais, rfi, slm, txAis*, and *txRdi* attributes with the status recorded in step 20 of the procedure Verify the status of the node before the upgrade on page 1237:

**display Laps/* Sts/0**

12 Compare the status of the *Laps* components with the status recorded in step 21 of the procedure Verify the status of the node before the upgrade on page 1237:

**display Laps/* osistate**

13 If configured, compare the status of the *DS3* components with the status recorded in step 22 of the procedure Verify the status of the node before the upgrade on page 1237:

**display lp/* ds3/* osistate**

14 If configured, compare the status of the *DS1* components with the status recorded in step 23 of the procedure Verify the status of the node before the upgrade on page 1237:

**display lp/* ds3/* ds1/* osistate**

15 If configured, compare the status of the *DS3 DS1 Chan* components with the status recorded in step 24 of the procedure Verify the status of the node before the upgrade on page 1237:

**display lp/* ds3/* ds1/* chan/* osistate**

16 If configured, compare the status of the *DS3 IMA* components with the status recorded in step 25 of the procedure Verify the status of the node before the upgrade on page 1237:

**display lp/* ds3/* ima/* osistate**

17 If configured, compare the status of the *DS3 IMA LINK* components with the status recorded in step 26 of the procedure Verify the status of the node before the upgrade on page 1237.

**display lp/* ds3/* ima/* lk/* osistate**

18 Compare the status of the *ATM interfaces* with the status recorded in step 27 of the procedure Verify the status of the node before the upgrade on page 1237:

**display Atmlf/* osistate**

19 Compare the status of the *UNI signalling* components with the status recorded in step 28 of the procedure Verify the status of the node before the upgrade on page 1237:

**display atmif/* uni sig/(operatingMode = normal ) osistate**

20 Compare the status of the *ILMI channel* with the status recorded in step 29 of the procedure Verify the status of the node before the upgrade on page 1237:

**display atmif/* uni ilmi/(operatingMode = addressRegEnabled) osistate**

21 Compare the status of the *PNNI signalling* components with the status recorded in step 30 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Atmlf/* Pnni Sig osistate**

22 Compare the status of the *Atmmpe* components with the status recorded in step 31 of the procedure Verify the status of the node before the upgrade on page 1237:

**display Atmmpe/* osistate**

23 Compare the status of the *Ac* components with the status recorded in step 32 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Atmmpe/* Ac/* osistate**

**24** If the Multiservice Switch 15000 node is connected with GigE to a Multiservice Switch 8600 node, compare the status of the *LanApplications* components with the status recorded in step 33 of the procedure Verify the status of the node before the upgrade on page 1237.

**display La/* osistate**

**25** Compare the status of the *VirtualRouter* components with the status recorded in step 34 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Vr/* osistate**

**26** Compare the status of the *ProtocolPorts* components with the status recorded in step 35 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Vr/* Pp/* osistate**

**27** Compare the status of the *Ip* components with the status recorded in step 36 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Vr/* Ip osistate**

**28** If the Multiservice Switch 15000 node is connected with GigE to a Multiservice Switch 8600 node, compare the status of the *Ospf* components with the status recorded in step 37 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Vr/* Ip Ospf osistate**

**29** If the Multiservice Switch 15000 node is connected with GigE to a Multiservice Switch 8600 node, compare the status of the *Ospf neighbor* components with the status recorded in step 38 of the procedureVerify the status of the node before the upgrade on page 1237.

**display Vr/* Ip Ospf Nbr/* state**

**30** Compare the status of the static routes with the status recorded in step 39 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Vr/* Ip static routeEntry/* operationalState, protectionLevel**

**31** Compare the status of the *nextHop* components under static routes with the status recorded in step 40 of the procedure Verify the status of the node before the upgrade on page 1237. The components must have an operational status of enabled.

**display Vr/VoIP Ip static route/* nexthop/* operationalState**

**32** Compare the status of the *Vsp* components with the status recorded in step 41 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Lp/* Vsp osiState** (for VSP3 - NTHW84xx)
and
**display Dlep/* Vsp osiState** (for VSP3-0 - NTHW77xx)

**33** Compare the status of the *ProcessingModule* components with the status recorded in step 42 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Lp/* Vsp Pm/* osiState** (for VSP3 - NTHW84xx)
and
**display Dlep/* Vsp Pm/* osiState** (for VSP3-0 - NTHW77xx)

**34** Compare the status of the *Nsta* components with the status recorded in step 43 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Nsta/* osiState**

**35** Compare the status of the *TDMAccessGroup* components with the status recorded in step 44 of the procedure Verify the status of the node before the upgrade..

**display Nsta/* vgs tag/* osiState**

**36** Compare the status of the *Aal1Ces* components with the status recorded in step 45 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Aal1Ces/* osiState**

**37** Compare the status of the *IpMConn* components with the status recorded in step 46 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Nsta/* vgs IpMConn osiState**

**38** Compare the status of the *ControlConnection* components with the status recorded in step 47 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Nsta/* vgs Ctrl/* osiState**

**39** Compare the status of the *vt1dot5* components with the status recorded in step 48 of the procedureVerify the status of the node before the upgrade on page 1237.

**display Laps/* sts vt1dot5/* osistate**

**40** Compare the status of the *vt1dot5 DS1* components with the status recorded in step 49 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Laps/* sts vt1dot5/* ds1/* osistate**

**41** Compare the status of the *vt1dot5 DS1 Chan* components with the status recorded in step 50 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Laps/* sts vt1dot5/* ds1/* chan/* osistate**

**42** Compare the status of the *CasDefn* components with the status recorded in step 51 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Nsta/* vgs casdefn/* osistate**

**43** Compare the status of the *IsdnUserAdaption* components with the status recorded in step 52 of the procedure Verify the status of the node before the upgrade..

**display Nsta/* vgs iua/* osistate**

**44** Compare the status of the *Q921* components with the status recorded in step 53 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Nsta/* vgs q921/* osistate**

**45** If the node being migrated relies on OAM Ethernet connectivity, compare the status of the active control processor with the status recorded in step 54 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Lp/0 Oamenet/0 activeStatus**

**46** If the node being migrated relies on OAM Ethernet connectivity, compare the status of the standby control processor with the status recorded in step 55 of the procedure Verify the status of the node before the upgrade on page 1237.

**display Lp/0 Oamenet/0 standbyStatus**

**47** Compare the information about the IP reachability of the first Preside MDM server from the Multiservice Switch 15000/Media Gateway 15000 node with the information recorded in step 56 of the procedure Verify the status of the node before the upgrade on page 1237.

**list ac ipaccess/***

**48** Compare the information about the IP reachability of the first Preside MDM server from the Multiservice Switch 15000/Media Gateway 15000 node with the information recorded in step 57 of the procedure Verify the status of the node before the upgrade on page 1237.

**ping -trace -ip(<MDM1 IP>) Vr/0 Ip Icmp**

**49** Compare the information about the IP reachability of the second Preside MDM server from the Multiservice Switch 15000/Media Gateway 15000 node with the information recorded in step 58 of the procedure Verify the status of the node before the upgrade on page 1237.

**ping -trace -ip(<MDM2 IP>) Vr/0 Ip Icmp**

# Stop the HSM using Command Console

During an upgrade of the nodes, you may encounter problems that require you to abort the upgrade. Generally, you want to abort a hitless software migration if service windows close, failures occur on other nodes, or a MigrationVisibleAlarm is raised, indicating an unknown impact or a known service affecting impact. If a MigrationVisibleAlarm is raised, the system pauses the migration. If you expected the alarm and want to continue with the migration, issue the **continue prov** command.

To abort a hitless software migration, you must issue the **stop prov** command. To do so without causing a service outage, you must issue this command either:

- when the migration is paused due to an **activate - pause prov** command or,
- during the migration switchover phase.

  This phase is a short period of time during which the logical or migrating shelf (which held the former standby control processors and standby function processors, but which are now being loaded with the new software) takes control and becomes the service shelf. By issuing the command during this phase, you can roll back to the view before the software application version list has changed without any system impact.

## Stopping the HSM

### *From the Command Console*

**1**



**CAUTION**
**Service Outage**
Issuing the **stop prov** command after the migration switchover phase will cause a service outage.

Stop the migration:

**stop prov**

The following shows sample output for this command:

```
PROV 56> stop prov
Prov
ok              2001-08-10 15:29:10.78
PROV 57>
    Fs; 2001-08-10 15:29:10.81
SET minor equipment processorProblem 70081019
    ADMIN: unlocked      OPER: enabled       USAGE: active
    AVAIL:               PROC:               CNTRL:
    ALARM:               STBY: notSet        UNKNW: false
    Id: 02BA      Rel: Lp/0
    Com: File system lost disk synchronization.
    Int: 0/0/0/0; sfsFileSys.cc; 1195; ""
PROV 57>
    Fs Disk/1; 2001-08-10 15:29:10.82
CLR cleared processing underlyingResourceUnavail            00000000
    ADMIN: unlocked      OPER: disabled      USAGE: idle
    AVAIL:               PROC:               CNTRL:
    ALARM:               STBY: notSet        UNKNW: false
    Id: 02BB      Rel: Lp/0
    Com: Cleared all alarms against standby DISK
    Int: 0/0/0/0; sfsFileSys.cc; 1238; ""
PROV 57>
--- Response 43 continued ...
   The software upgrade failed due to a failure in upgrading the
standby CP.
   Failure reason: Standby Cp crashed. Software migration aborted.
command failed 2001-08-10 15:29:10.83
PROV 57>
    Prov Migration; 2001-08-10 15:29:10.98
CLR cleared operator operationalCondition                   70000033
    ADMIN: unlocked      OPER: enabled       USAGE: active
    AVAIL:               PROC:               CNTRL:
    ALARM:               STBY: notSet        UNKNW: false
    Id: 02BC      Rel: Lp/0
    Com: Prov Migration component deleted.
    Int: 0/0/2/6973; casAlarm.cc; 1132; S_PCR2.2.1.2
```

2 Exit provisioning mode.

**end prov**

3 To resume a hitless software migration after issuing the **stop prov** command, wait until both control processors' LEDs are green, with one flashing and one solid, and return to step 2 in HSM (Command Console) activation on page 1261.

# Feature activation

**CAUTION**
**No feature activation is required in an SN07 to SN07 UA-IP upgrade.**
In an SN07 to SN07 UA-IP upgrade, no feature activation is required, assuming that the SN07 release was installed from initial commissioning.

The information in this chapter is for reference purposes only and if required, is meant to be used in consultation with GNTS.

The mandatory Nortel Networks Multiservice Switch 15000/Media Gateway 15000 features for a UA-IP solution in this release are:

- Active alarm list
- Debug stream activation
- Enabling the recurring fan alarm

The optional features in this release are:

- Optional Secure FTP activation for a SN07 migration
- Setting the Succession release name identification

The following table lists the SN07 features for a PT-IP, PT-AAL2, IAC, or IAW solution for the Media Gateway 15000/20000 and indicates whether they are mandatory or not.

**Media Gateway features**

| Node | Feature | Mandatory |
|---|---|---|
| Media Gateway 15000/20000 | Active alarm list | Yes |
| Media Gateway 15000/20000 | Recurring fan alarm | Yes |
| Media Gateway 15000/20000 | Secure FTP | No |
| Media Gateway 15000/20000 | Debug stream | Yes |

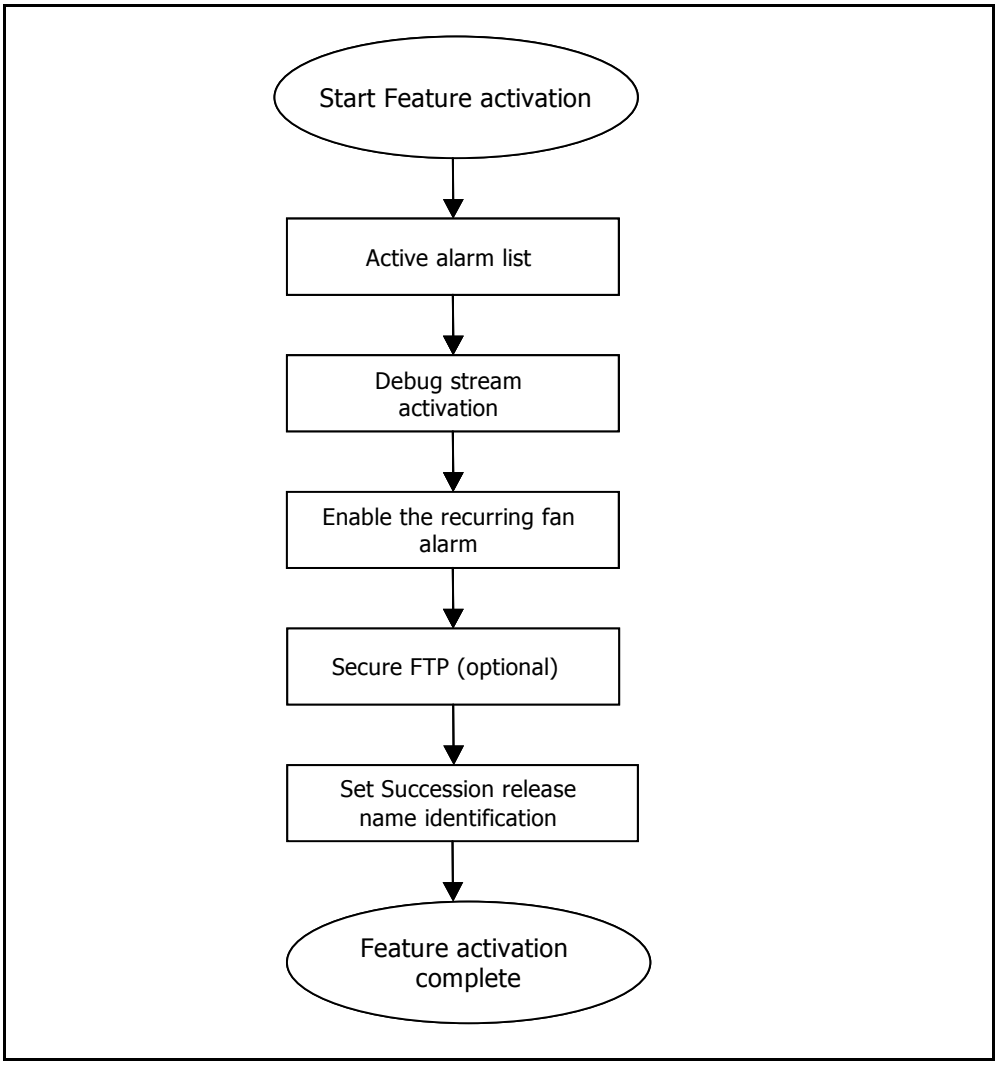
## Prerequisites

- Complete the HSM. See HSM (Command Console) activation on page 1261.

## Feature activation task flow

The task flow shows you the sequence of procedures you need to perform to activate new features in an SN07 to SN07 UA-IP upgrade for a Multiservice Switch 15000/Media Gateway 15000. To link to any procedure, go to the Work flow navigation on page 1298 that follows the flow chart.

**Feature activation work flow**



## Work flow navigation


- Active alarm list on page 1299
- Debug stream activation on page 1301
- Enabling the recurring fan alarm on page 1303
- Secure FTP activation for a SN07 migration on page 1305
- Setting the Succession release name identification on page 1307

# Active alarm list

In a Succession solution, the Nortel Networks Preside Multiservice Data Manager (MDM) server collects alarm data from multiple Nortel Networks Multiservice Switch/Media Gateway nodes. This allows the Preside MDM active alarm list to contain more fault information, and operate more efficiently.

If your network is configured to collect alarm data from multiple Multiservice Switch/Media Gateway nodes you can view the active alarm list through any one of the nodes.

***Note:*** The alarms will display in the local window if the *dataStreams* operational attribute for your log in session has "alarm sending" enabled.

## Prerequisites

- SN07 software must be running on the Multiservice Switch 15000/Media Gateway 15000/20000 node.

***From the node***

1 Login to the node using the appropriate permissions.

2 Enter provisioning mode:

**start prov**

3 Configure the active alarm list feature:

**set sw lpt/cp featurelist activeAlarmList**

4 Perform a semantic check on the changes:

**check prov**

***Note:*** If the semantic check fails, troubleshoot the problem using “Troubleshooting a software upgrade” in *Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP)*, NN10419-461.

5 If the semantic check passes, activate the view:

**activate prov**

6 If the semantic check passes, confirm the final version of the view:

**confirm prov**

7 If the semantic check passes, save the view:

**save prov**

8 If the semantic check passes, commit the final version of the view:

**commit prov**

9 Verify that the you can see active alarms on the node:

**r aas**

# Debug stream activation

In a Succession solution, Multiservice Switch 15000/Media Gateway 15000/20000 nodes can be enabled to collect crash data. To do this, the DCS debug collector agent queue must be configured to spool DCS debug stream data.

## Prerequisites

- SN07 software must be running on the Multiservice Switch 15000/Media Gateway 15000/20000 node.

### *From the node*

1 Login to the node using the appropriate permissions.

2 Enter provisioning mode:

**start prov**

3 Repeat this step for each FP you want to collect debug data for:

**add lp/<n> eng ds/debug**

4 Set the agent queue size override for the DCS debug stream. Repeat this step for each FP you want to collect debug data for:

**set lp/<n> eng ds/debug ov agentQueueSize 50**

5 Turn spooling on for the DCS debug stream:

**set col/debug sp spooling on**

6 Verify that the agent queue size override for the DCS debug stream has been set:

**display lp/<*> eng ds/debug ov agentQueueSize**

7 Verify that spooling has been turned on for the DCS debug stream. Repeat this step for each FP template you want to verify:

**display col/debug sp**

8 Perform a semantic check on the changes:

**check prov**

***Note:*** If the semantic check fails, troubleshoot the problem using “Troubleshooting a software upgrade” in *Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP)*, NN10419-461.

9 If the semantic check passes, activate the view: **activate prov**

10 If the semantic check passes, confirm the final version of the view:

**confirm prov**

11 If the semantic check passes, save the view:

**save prov**

12 If the semantic check passes, commit the final version of the view:

**commit prov**

# Enabling the recurring fan alarm



**CAUTION**
**The recurring fan alarm must not be activated for Media Gateway 7480.**
Do not activate the recurring fan alarm for Media Gateway 7480 in SN07 in a PT-IP, PT-AAL2, IAC, or IAW solution network.

In a Succession solution, it is possible to configure a recurring fan failure alarm on Multiservice Switch 15000/Media Gateway 15000/20000 nodes. The alarm can be repeated periodically (every 8 hours with the same severity, and on the fourth occurrence the fan severity is increased to critical) until the problem is cleared. This raises the operator's attention to the problem and ensures action is taken before an outage occurs.

## Prerequisites

- SN07 software must be running on the node.

***From the node***

1 Login to the node using the appropriate permissions.

2 Enter provisioning mode:

**start prov**

3 Configure the recurring fan alarm feature:

**set shelf repeatFanAlarm ON**

4 Perform a semantic check on the changes:

**check prov**

***Note:*** If the semantic check fails, troubleshoot the problem using "Troubleshooting a software upgrade" in *Upgrading Multiservice Switch 15000 in Succession Networks (UA-IP)*, NN10419-461.

5 If the semantic check passes, activate the view:

**activate prov**

6 If the semantic check passes, confirm the final version of the view:

**confirm prov**

7 If the semantic check passes, save the view:

**save prov**

8 If the semantic check passes, commit the final version of the view:

**commit prov**

# Secure FTP activation for a SN07 migration

The Secure FTP feature is optional and can be activated for Multiservice Switch/Media Gateway 7480/15000/20000.

When you configure secure FTP authentication on a node, encrypted passwords can be used during FTP sessions.

***Note:*** When this feature is activated, the node denies all FTP communication except from a Nortel Networks Preside Multiservice Data Manager (MDM) application configured with secure FTP.

Multiservice Switch nodes initiate FTP sessions with Preside MDM servers for the purposes of downloading software. To ensure that secure FTP authentication is used, configure the FTP daemon and add the security feature to the feature list of the control processor.

## Prerequisites

- Secure FTP authentication must have been enabled on the Preside MDM servers to ensure secure communications. For more information, see NN10185-461 *Upgrading Preside MDM in Succession Networks*.
- SN07 software must be running on the node.

### *From the node*

1. Login to the node using the appropriate permissions.
2. Enter provisioning mode so that you can issue the appropriate commands:

   **start prov**
3. Add the FTP security feature to the feature list of the control processor:

   **set Software Lpt/CP featurelist secureFtpAuth1Only**
4. Perform a semantic check on the changes:

   **check prov**
5. Apply the changes:

   **activate prov**
6. Within 20 minutes of applying the changes, confirm the changes to avoid a non-hitless rollback to the previously committed configuration:

   **confirm prov**

7 Save the view:

**save prov**

8 Commit the final version of the view:

**commit prov**

9 Exit provisioning mode once the migration is complete:

**end prov**

## Setting the Succession release name identification

The commentText field of the Multiservice Switch 15000/Media Gateway 15000/20000 shelf component contains record release and load information that appears in the following order:

- Succession release
- patchlevel of Nortel Networks Preside Multiservice Data Manager (MDM) software used to commission the node
- version of Installation Methods used to commission the node
- version of the Engineering Specification Book used to commission the node

To help identify which Succession release the MDM and Multiservice Switch 15000/Media Gateway 15000/20000 are running and help operators determine if these elements are compatible with other elements in the Succession network, the MDM 15.1 toolset allows you to set the Succession release name on the MDM tool launcher and to modify the commentText field of the shelf component. An alternate way to modify the Succession release name is to use the **Set Shelf Commenttext** command.

Perform either the:

- Setting Succession release name using the Set Shelf CommentText command on page 1307 or
- Setting Succession release name for Multiservice Switch 15000/ Media Gateway 15000 on page 1309

### Prerequisites

- upgrade to SN07.

### Setting Succession release name using the Set Shelf CommentText command

***From the node***

1 Login to the node using the appropriate permissions.

2 Display the comment text field:

**display Shelf CommentText**

The following shows sample output for this command:

```
7> display Shelf CommentText

SN06, MDM 142-09, IM9095 1.01, IM1662 1.35, IM1661 1.04, Spec 2.0
```

3 If the first entry (the release name) is not the release you have running on the node, update this entry by setting the text to contain “SN07” leaving the remainder of the text unchanged. For example:

**set Shelf CommentText "SN07, MDM 142-09, IM9095 1.01, IM1662 1.35, IM1661 1.04, Spec 2.0"**

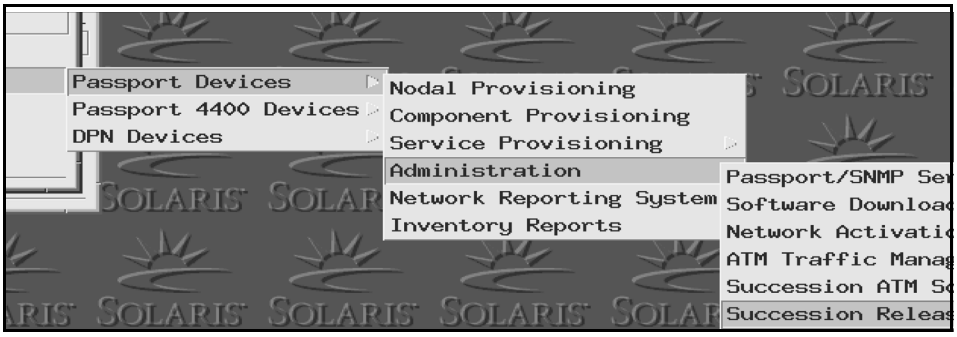
## Setting Succession release name for Multiservice Switch 15000/ Media Gateway 15000

### *From the Preside MDM server*

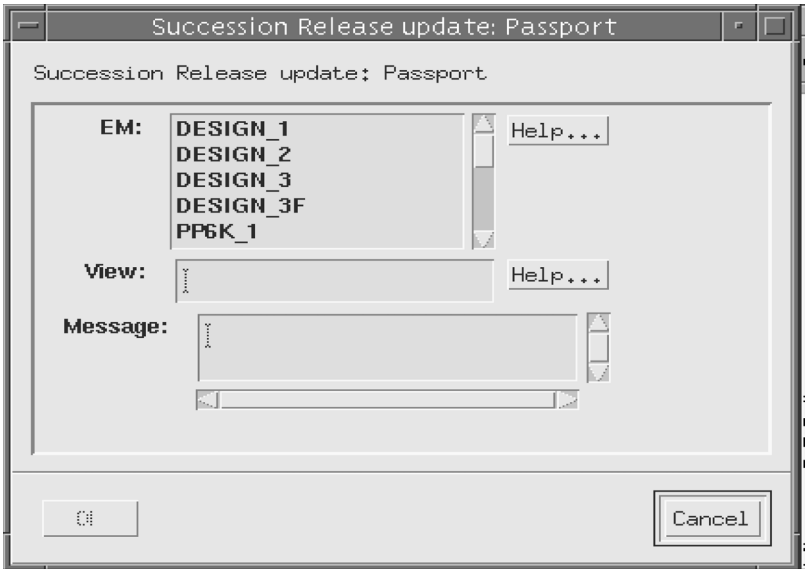
**1** Login — see NN10185-461 *Upgrading Preside MDM in Succession Networks*.

**2** From the Preside MDM window, choose:

Configuration > Passport > Administration > Succession Release Update: Passport.




Initial screen for setting the Multiservice Switch 15000/Media Gateway 15000/20000 shelf display.



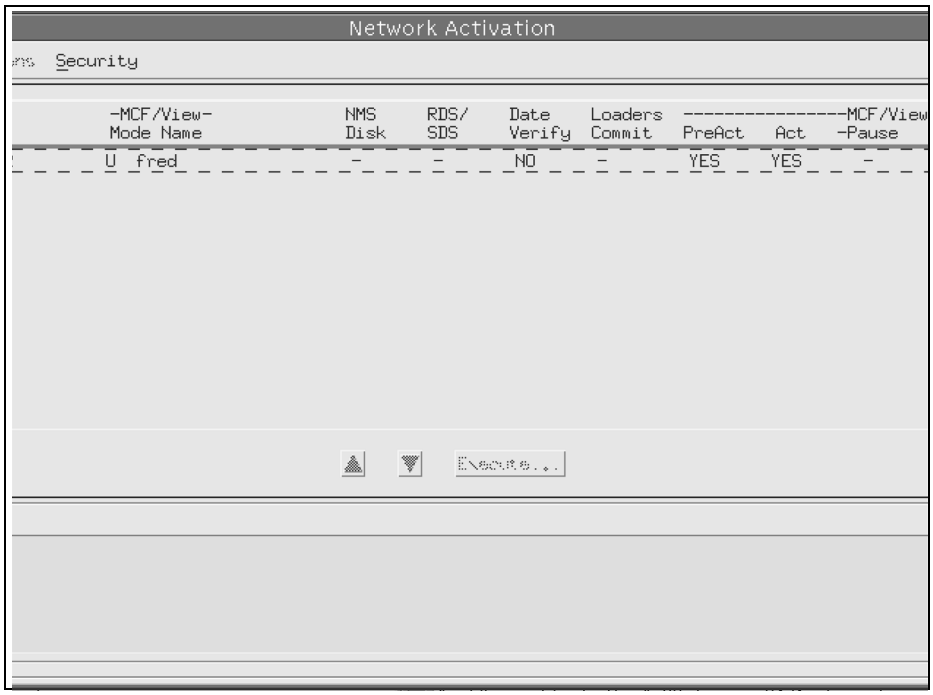

**3** Select the Multiservice Switch 15000/Media Gateway 15000/20000 element name.

**4** Select the View name.

This is the Multiservice Switch 15000/Media Gateway 15000/20000 element name and View name where the provisioning will be saved.

**5** Click **OK**.

The Network Activation tool (NAT) starts.



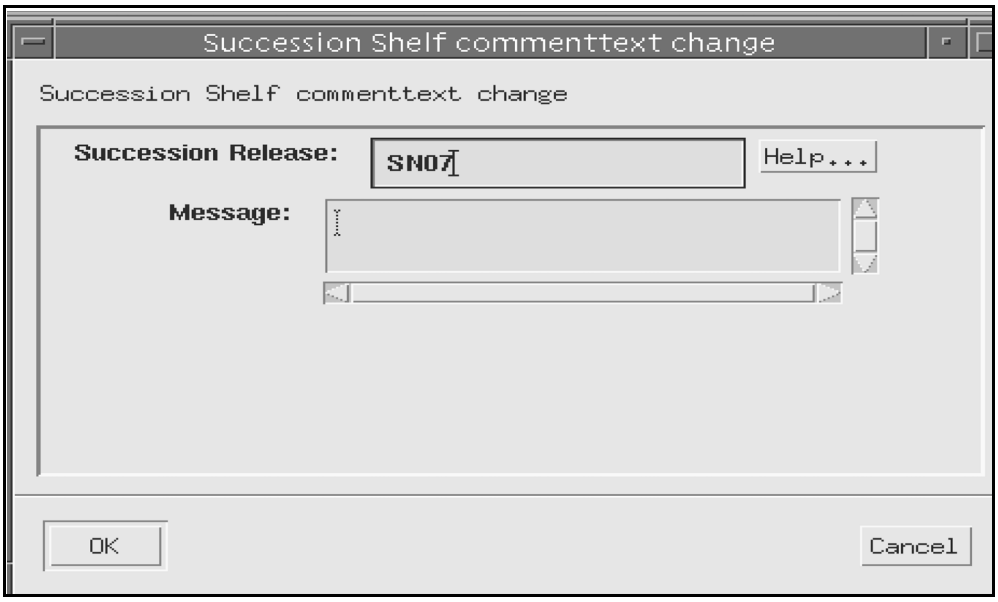

**6** Enter the group name (or select) a Multiservice Switch 15000/Media Gateway 15000/20000 group that has configuration privileges.

**7** Click **Execute**.

After you execute the NAT record, you are prompted for the new Succession release that will appear in the Multiservice Switch 15000/Media Gateway 15000/20000 Shelf CommentText field.

Use the format: SNxx.y (for example, SN06.2 or SN07)

The Succession Shelf comment text change window appears.




**8** Click **OK**.

The Multiservice Switch 15000/Media Gateway 15000/20000 *Shelf CommentText* attribute on the target node is updated with the Succession release name being displayed before the rest of the information in the Shelf CommentText field.

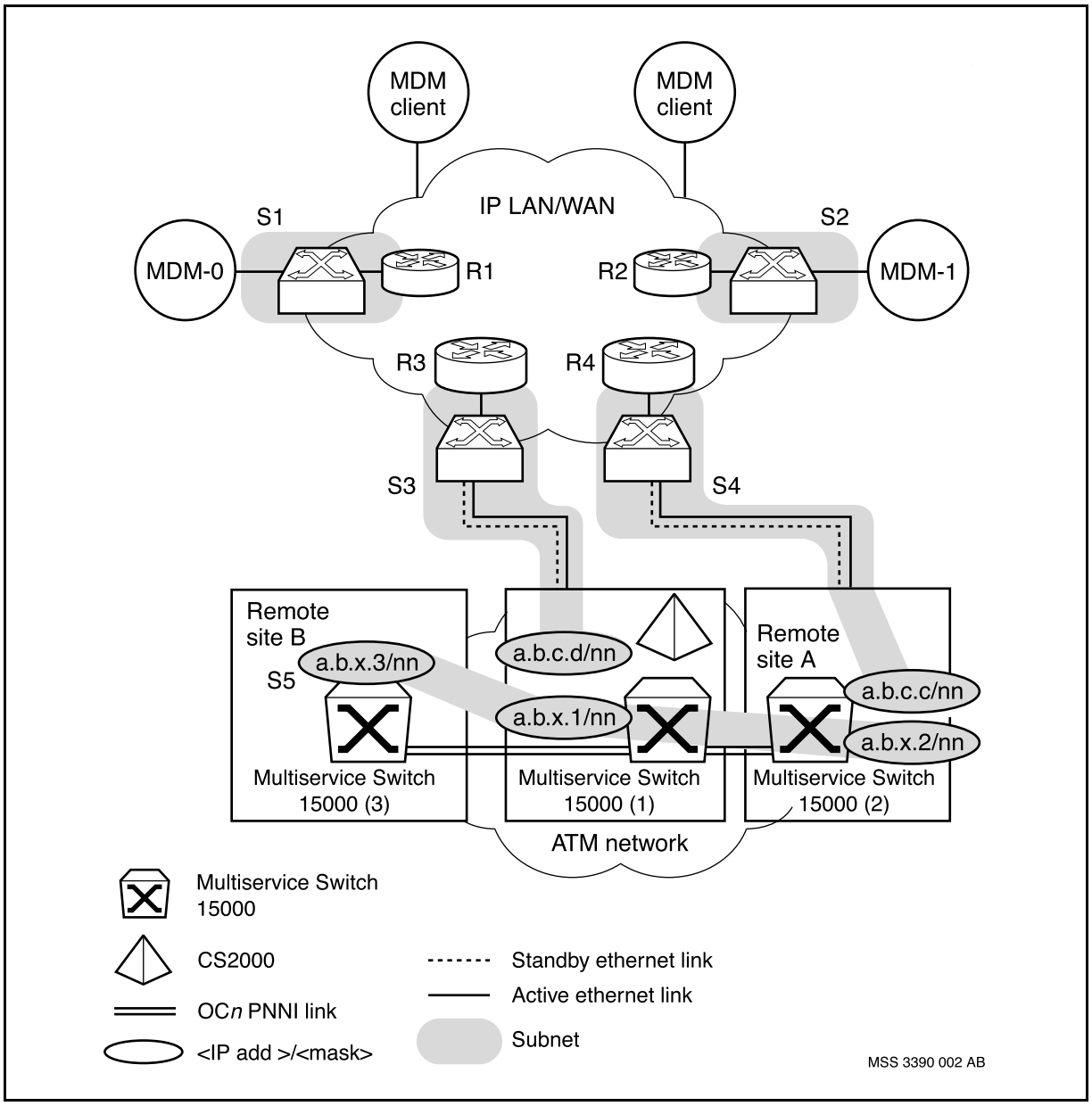
If you click *Cancel*, the process is cancelled and the *Shelf CommentText* attribute remains unchanged.

# In-band OAM quick reference

## Key relationships

The figure, Sample in-band connectivity topology on page 1312 illustrates a typical in-band OAM configuration. A brief description of the items in this diagram and their relationship to each other is provided below.

### Sample in-band connectivity topology



**MDM-0 and MDM-1**

These Nortel Networks Preside Multiservice Data Manager (MDM) servers manage Nortel Networks Multiservice Switch network.

The chosen server is the server that the operator uses as a launching point for Preside MDM applications, such as Command Console.

The alternate server is another Preside MDM server that could be used to perform the same set of tasks, but wasn't chosen.

**Multiservice Switch -1**

This Multiservice Switch 15000 node is in the Succession Office and is a Gateway node using out-of-band connectivity.

From the perspective of Preside MDM-0, S3 represents subnet to the preferred Multiservice Switch 15000 node.

**Multiservice Switch-2**

This Multiservice Switch 15000 node is in a remote office and is a Gateway node using out-of-band connectivity.

From the perspective of Preside MDM-0, S4 represents the subnet to the alternate Multiservice Switch 15000 node.

**Multiservice Switch-2 and Multiservice Switch-3**

S5 represents the in-band OAM subnet. Multiservice Switch-1 has a direct ATMMPE ATM (PVC) connection to every other Multiservice Switch 15000 node.

These Multiservice Switch 15000 nodes are Remote nodes using in-band connectivity with Multiservice Switch-1.

# Upgrading CICM

## General upgrade procedures

This chapter provides the standard procedures for applying MR upgrades to the EM and CICM software. They are performed by Telco administrators.

The standard EM upgrade procedures provided in previous versions of this document do not apply to 7.11 EM upgrades, since there are internal changes to the Operating System used by the 7.11 CICM-EM, which require the nodes to be re-imaged during the upgrade.

The normal mode of access to the CICM EM is via a PC connected to the Administration LAN. The procedures in this document are written based on this mode of access. It is also possible to access the EM locally via a customer-supplied terminal (with keyboard and mouse) directly connected to the EM. In this case, the procedures are the same, except the remote access steps are skipped.

### Verify the software version of a 6.12 EM and CICM

Use this procedure to verify the software version of a 6.12 EM and its 6.12 CICM nodes.

***Note:*** It is required to use administrator userids and passwords to login to the Element Manager.

**Procedure 1 Verify the software version of a 6.12 EM and CICM**

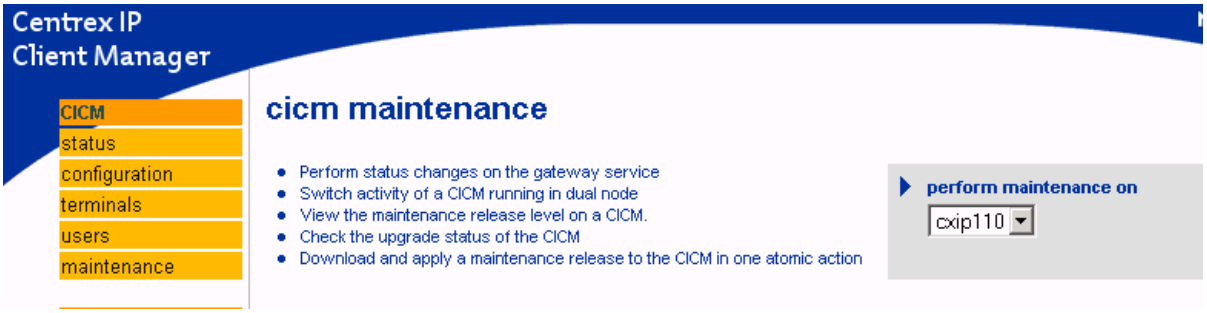
***At the CICM - Element Manager Home page of the Element Manager Web pages***

1 View the Element Manager version on the bottom left corner of any 6.12 Element Manager Web page, as shown in the following figure.



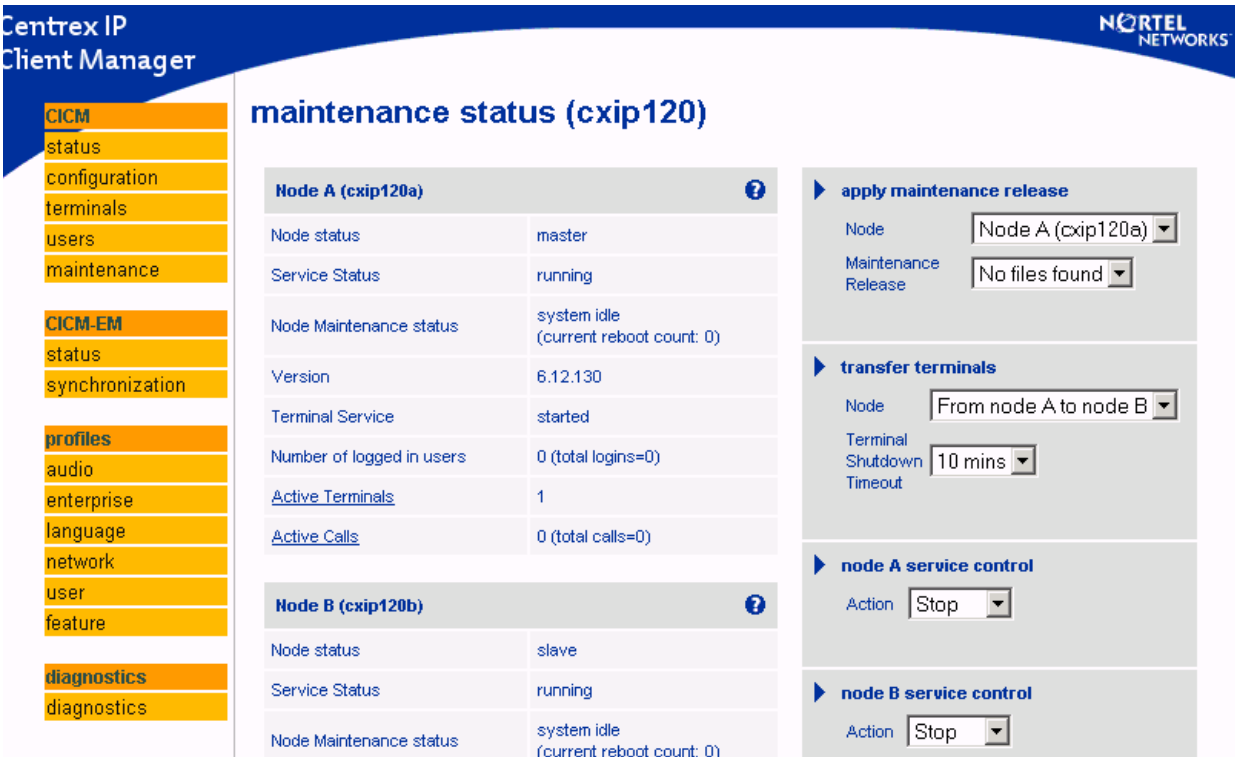

**2** To view the CICM nodes versions, select **maintenance** from the **CICM** section of the left menu.

*Response: The **cicm maintenance** page opens.*




**3** Select the CICM to view from the drop-down menu on the **perform maintenance on** text box on the right.

*Response: The **maintenance status <cicm_name>** page opens.*




4 The software version for each CICM node is shown in the **Version** field of the **Node A/B** status windows. In the figure above, Node A and Node B are both at version 3.12.130.

***Note:*** The EM and CICM nodes software should all be the same version for optimal performance.

5 This procedure is complete.

## Perform an EM 7.11.xxx MR upgrade

Use this procedure to perform a CICM Element Manager 7.11.xxx MR upgrade on an Element Manager already running on a 7.11 software version.

***Note:*** It is recommended to backup the EM prior to upgrading, so that it can be easily restored to its prior software configuration in the event of a failure during upgrade. Use the CXIP Backup/Restore Tool, which is available on the CXIP Backup/Restore Tool CD along with relevant documentation.

## Procedure 2 Perform an EM 7.11.xxx MR upgrade

**ATTENTION**

Verify that the EM and CICM nodes are at the Series 7.11 software version. Refer to the View the software version of a 7.11 EM and CICM procedure above.

If the EM and CICM nodes are not all running software version 7.11.xxx, then do not proceed with this upgrade.

**ATTENTION**

It is required to use Administrator userids and passwords to login to the Element Manager for this upgrade.

### *At a PC on the Administration LAN*

**1** Open a Windows Terminal Services Client or Telnet session and login as an administrator to the Element Manager desktop. It is required to have administrator privileges to perform this procedure.

### *At the Element Manager Windows 2000 desktop*

**2** Obtain the EM upgrade .exe file (\Upgrade files\cicm_em_7.11.xxx.exe) from the CentrexIP Client Manager 7.11 MR CDROM CICEM071_MRx_7_11_xxx.iso and place it in the Element Manager directory of your choice.

**3** Double click on the EM upgrade .exe file to begin installation of the EM product upgrade.

*Response: A DOS text window opens.*

**4** Follow the instructions in the DOS text window to completion. Press the spacebar to scroll through the text. After reading the instruction text, press Enter to begin, and Y to continue. Then press Enter to complete the final step.

This will initiate the following actions:

- The services are stopped
- The files are replaced
- The software is upgraded

- Some directories are added to the path of the current user (Administrator)
- The services are restarted

*Response: The DOS window displays the results of the actions.*

***Note:*** Failures observed at this point are normally due to locked files. If this occurs, run the script one more time. Then if the files are still locked, reboot the EM and execute the EM upgrade again. There are no restrictions on the number of times you can run the EM upgrade .exe file.

***At the Element Manager desktop***

**5** Open a DOS Command Prompt session in the EM.

**6** Run the **swupgrade** command as follows:
At the DOS Command Prompt session, type **swupgrade**, then press Enter.

*Response: The DOS Command Prompt session displays actions that are being taken by the swupgrade command.*

**7** Perform a manual EM reboot by going to the Start menu on the EM desktop and selecting Shutdown, then Restart.

**8** Verify that the Element Manager version as displayed on the Element Manager Web pages in the bottom left corner reflects the 6.12.xxx upgrade as intended. Refer to the Verify the software version of a 6.12 EM and CICM on page 1314.

**9** Repeat this procedure for the other Element Manager, if applicable.

**10** This procedure is complete.

## Perform a CICM 7.11.xxx MR upgrade

Use the following procedure to apply a CICM 7.11.xxx MR upgrade to CICM nodes already running on a 7.11 software version.

***Note 1:*** The Perform an EM 7.11.xxx MR upgrade on page 1317 needs to be performed prior to this procedure. If two Element Managers are in use, both EMs must be upgraded before performing this procedure.

***Note 2:*** It is recommended to backup the CICM nodes prior to upgrading, so they can be easily restored to their prior software configuration in the event of a major failure during upgrade. Use the CXIP Backup/Restore Tool, which is available on the CXIP Backup/Restore Tool CD along with relevant documentation.

***Note 3:*** In the event of a software application failure, the CICM node will resume activity at its current release level.

**Limitations and Restrictions: CICM MR upgrade**

The limitations and restrictions of the CICM 7.11.xxx MR upgrade process are:

- Application of the MR upgrade will result in an outage on that node of approximately 15 minutes. It should therefore be performed only during a scheduled maintenance window.
- Both nodes of the CICM must be in service for the product upgrade to begin.
- The application of the MR upgrade is a manual operation. The activation of the process cannot be scheduled.
- Once the new MR upgrade has been applied, it is impossible to go back to a previous release without a complete re-installation or the recovery of a backed-up image.
- Only one node of the CICM should have the MR upgrade applied at a time.
- Terminals connected to the node being upgraded will suffer an outage while they locate the mate node.
- Active calls using resources on the node being upgraded will be lost.
- The call capacity of the CICM being upgraded is reduced by half.

**Procedure 3 Perform a CICM 7.11.xxx MR upgrade**

**ATTENTION**

It is required to use Administrator userids and passwords to login to the Element Manager for this upgrade.

***At a PC on the Administration LAN***

**1** Use Windows Terminal Services Client to login to the Primary Element Manager desktop.

***At the Element Manager Windows 2000 desktop***

**2** From the CentrexIP Client Manager 7.11 MR CDROM CICEM071_MRx_7_11_xxx.iso, obtain the gateway upgrade .cab file (\Upgrade files\GW_7.11.xxx.cab) for the upgrade

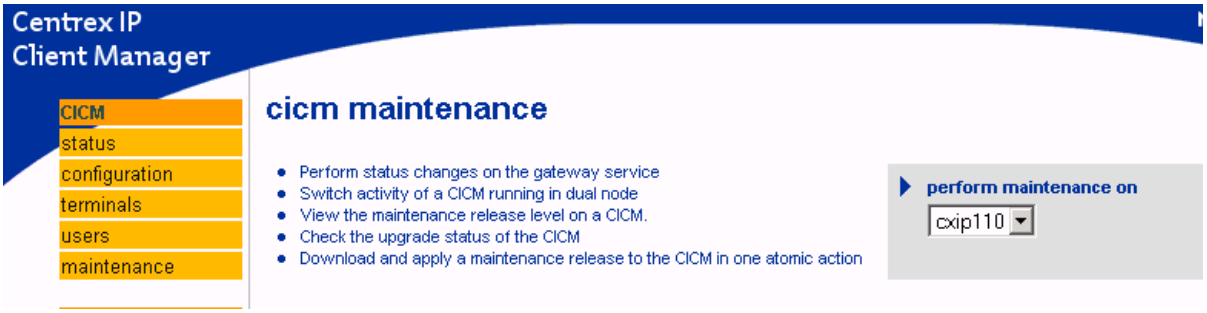
required and place it on the Primary Element Manager in the **C:\CentrexIP\Patching** directory.

***Note:*** If any obsolete gateway .cab files from previous upgrades exist in the **C:\CentrexIP\Patching** directory, you may delete them from this directory.

***At the CICM - Element Manager Home page of the Element Manager Web pages***

**3** Select the **maintenance** link from the **CICM** section of the left navigation bar.

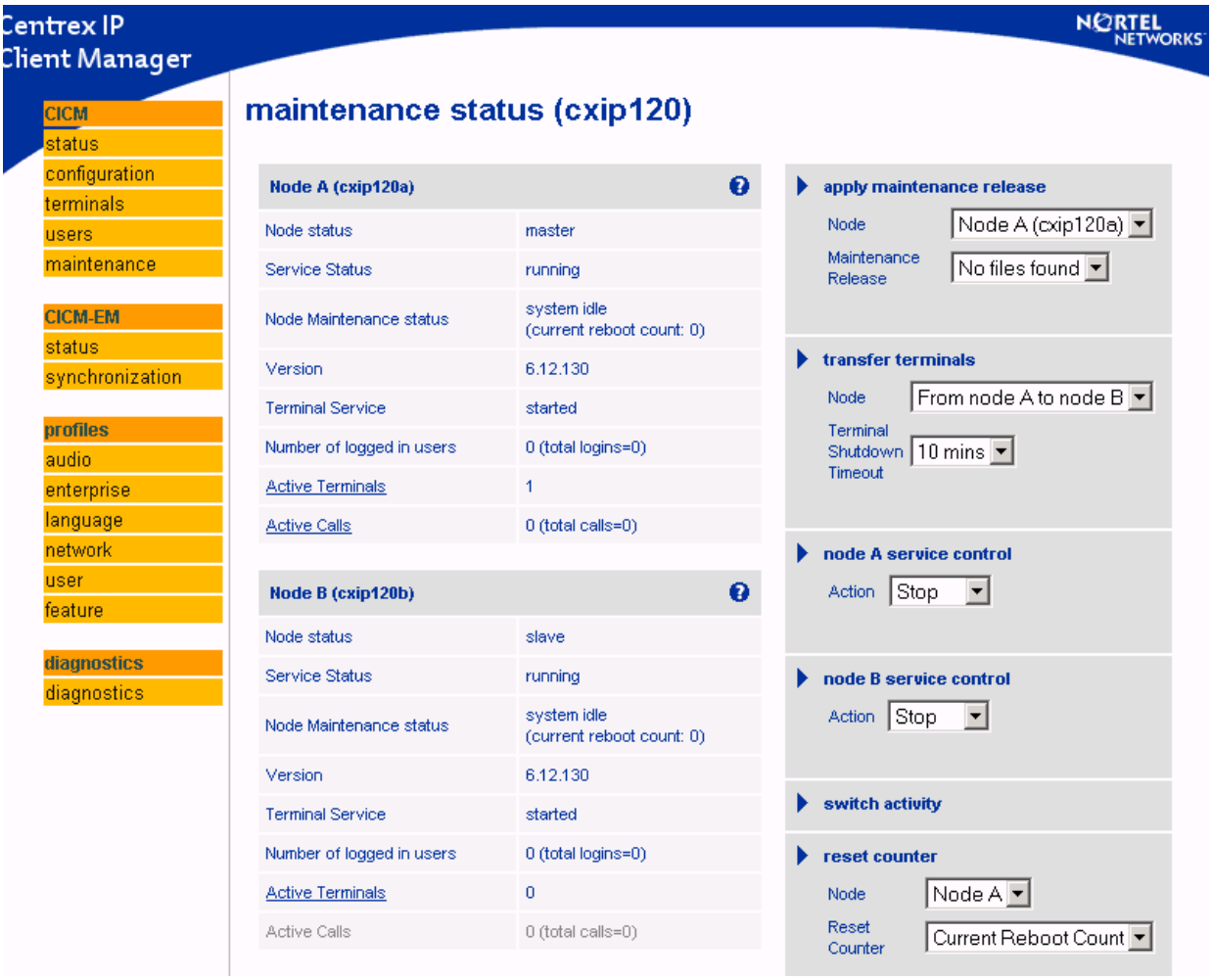
*Response: The **cicm maintenance** page opens.*




**4** Select the CICM to upgrade from the drop-down menu on the **perform maintenance on** menu on the right.

*Response: The **maintenance status <cicm_name>** page opens. The current software version for each node is displayed.*

*The **Node Maintenance status** field details the actions that are being performed on that node (for example, **system idle**, **stopping the cxipboot service**, and **starting the cxipboot service**). When the node is in service, this field displays **system idle** status.*




**5** Transfer the service from the node to be upgraded to the mate node as follows:

On the maintenance status <cicm_name> page, in the transfer terminals menu option on the right:

- From the Node drop-down menu, select the transfer direction:
  - — From node A to node B, or
  - — From node B to node A
- Then select the Terminal Shutdown Timeout in minutes from the drop-down menu.
- Then click on the transfer terminals text.

- When the confirmation screen opens, click on the confirm terminal transfer text.
- Then click on the start auto refresh text on the right menu of the maintenance status <cicm_name> page.

*Response: The terminal transfer will commence immediately upon confirmation, and will terminate when the selected timeout interval has expired.*

***Note:*** The Perform a Terminal Handover procedure in the Security and Administration section of this document provides additional details on Terminal Handover.

**6**

**ATTENTION**
Wait until the terminal transfer has completed before performing this step.

(OPTIONAL)
Busy the VMG units on the CS2K, using standard CS2K procedures.

***Note:*** This step is not essential, because the VMGs will come into service automatically. However, busying the VMG may result in more desirable CS2K performance measurements.

**7** If the **auto refresh** was started in step 5, then go to the **maintenance status <cicm_name>** page and click on the **stop auto refresh** button. This will stabilize the drop-down menus used.

**8** Apply the upgrade. On the maintenance status <cicm_name> page of the EM Web pages, in the **apply maintenance release** box in the right menu bar:

**a** Select the node to upgrade from the Node drop-down menu (this is the node that you have transferred service **from** in step 5 above).

**b** Then select the CICM MR upgrade to apply from the Maintenance Release drop-down menu.

**c** Then click on the **apply maintenance release** text.

**d** Verify the proper node and file have been selected, then click on the confirm maintenance release application text.

*Response: The **maintenance status <cicm_name>** page updates to show the status of the upgrade.*

**9** (OPTIONAL)
To aid in monitoring the progress of the update:
on the maintenance status <cicm_name> page, select the **start auto refresh** option for a periodic automatic refresh of the status pages.

To stop automatic refresh when monitoring is complete, select the stop auto refresh option.

***Note:*** The **auto refresh** option toggles between **start** and **stop**.

**10** To monitor the progress of the update, on the **maintenance status <cicm_name>** page, select the **system status** option on the right menu.

*Response: The **<cicm_name> cicm status** page opens and displays the status details of the CICM.*

**11** Monitor the **<cicm_name> cicm status** page to verify that the **Service** field for the applicable node goes to running status.

***Note:*** A manual restart of the node is not required.

**12** Upon successful completion of the upgrade, check the new CICM node version as displayed in the **Version** field of the **Node A/B** status windows on the **maintenance status <cicm_name>** page.

***Note:*** The CICM node version is displayed on the **maintenance status <cicm_name>** page, whereas the EM version is displayed in the bottom left corner of any EM Web page. Refer to the *View the software version of a 6.12 EM and CICM* procedure above.

**13** (REQUIRED ONLY IF STEP 6 WAS COMPLETED)
If the VMG unit was busied previously in step 6, return the VMG unit to service as soon as the **<cicm_name> cicm status** page shows the service is **running** on the upgraded node. Use standard CS2K procedures.

**14** After the VMG(s) are In Service, perform test calls on the upgraded node to verify that the upgraded node is working.

**15** Repeat this procedure (starting at step 3) for the mate CICM node.

**16** This procedure is complete.

## Add card(s) Procedure

This section provides the procedure for adding cards to the chassis.

### Procedure 4 Add card(s)

**ATTENTION**

To minimize the impact to service, it is recommended to add all the new cards to a CICM node at one time, for a one-time node reboot.

***At the CICM home Web page***

**1** Select **maintenance** from the **CICM** section of the left menu.

*Response: The **maintenance home** page opens.*

**2** Select the CICM from the drop-down menu in the **perform maintenance on** option in the right menu.

*Response: The **maintenance status <cicm_name>** page opens.*

**3** Transfer the service from the node to be upgraded to the mate node as follows:
On the maintenance status <cicm_name> page, in the transfer terminals box on the right:

- From the Node drop-down menu, select the transfer direction:
  - — From node A to node B, or
  - — From node B to node A
- Then select the Terminal Shutdown Timeout in minutes from the drop-down menu.
- Then click on the transfer terminals text.
- When the confirmation screen opens, click on the confirm terminal transfer text.
- Then click on the start auto refresh text on the right menu of the maintenance status <cicm_name> page.

*Response: The terminal transfer will commence immediately upon confirmation, and will terminate when the selected timeout interval has expired.*

***Note:*** The Perform a Terminal Handover procedure in the Security and Administration section of this document provides additional details on Terminal Handover.

### *At the CS2K interface*

**4**

**ATTENTION**

Wait until the terminal transfer has completed before performing this step.

(OPTIONAL)

***Note:*** This step is not essential, because the VMGs will come into service automatically. However, it may result in more desirable CS2K performance measurements.

Busy the VMG units on the CS2K, using standard CS2K procedures.

***Note:*** This step is not essential, because the VMGs will come into service automatically. However, busying the VMG may result in more desirable CS2K performance measurements.

### *At the CICM EM Web pages*

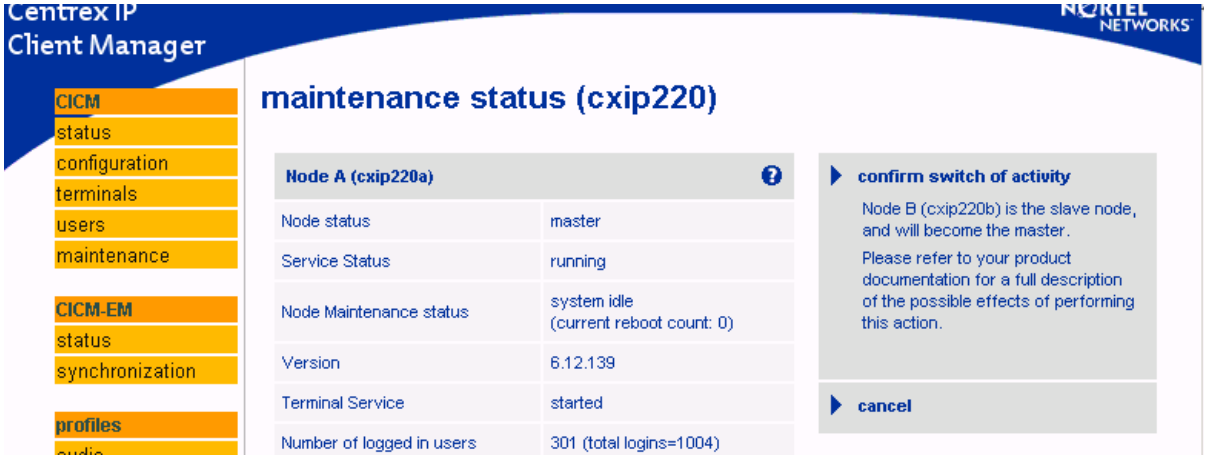
**5**

| If | Do |
|---|---|
| The card(s) is to be added to the Slave node | Do **not** do a switch of activity: skip step 6 and proceed to step 7. |
| The card(s) is to be added to the Master node | Proceed with step 6 to perform a switch of activity. |

6 Perform a switch of activity:

- From the maintenance status <cicm_name> page, select **switch activity** from the right menu.

  *Response: The maintenance status <cicm_name> page* updates to request a confirmation of the switch of activity.

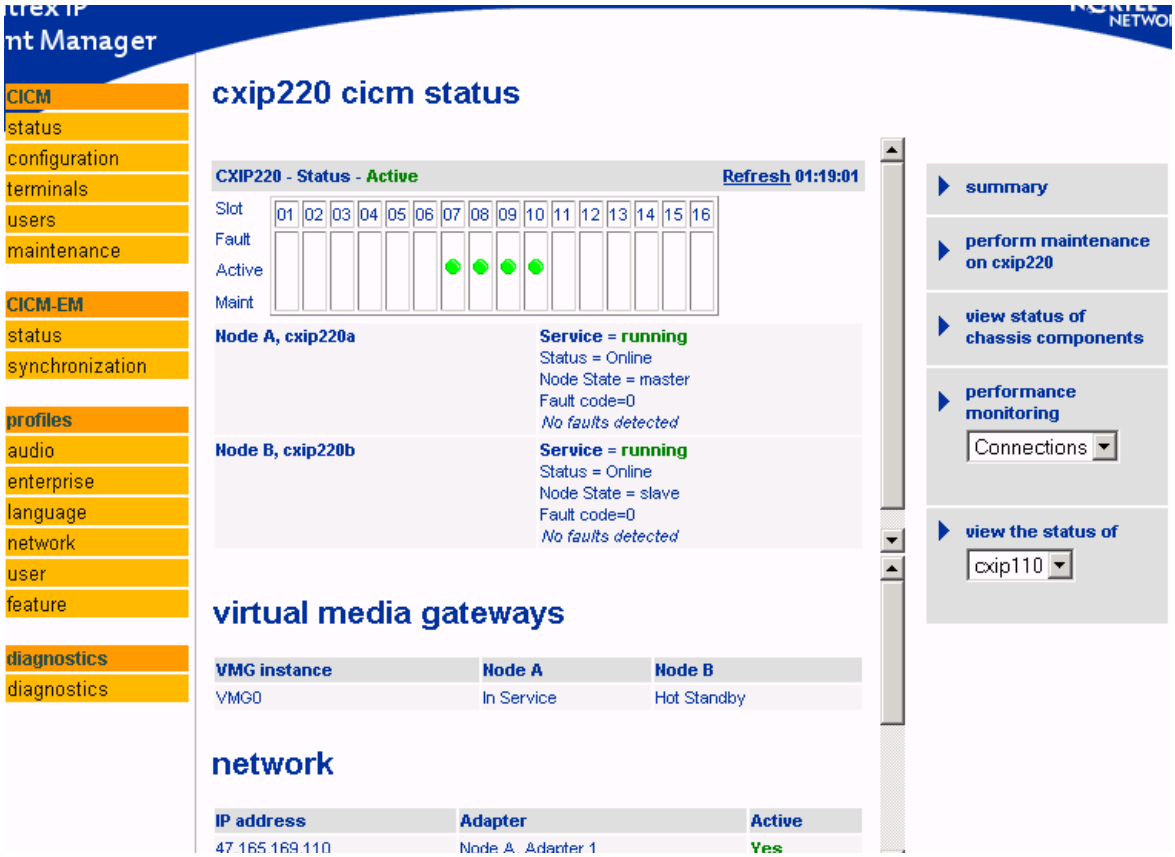



7 Stop the CICM service on the node to be powered down (i.e. the node where the card will be added).

**a** Click on the status option from the **CICM** section of the left menu bar to open the **cicm home** page.

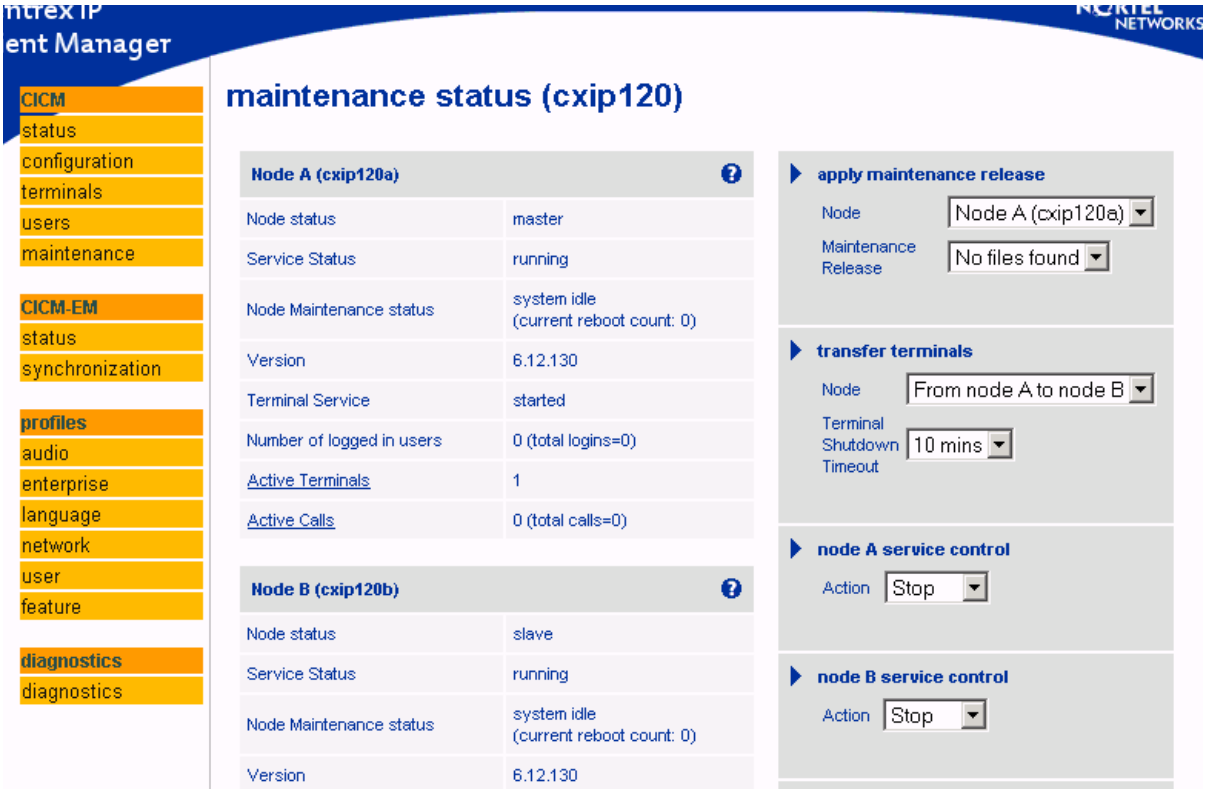
**b** In the **view the status of the following CICM** menu option on the right, select the CICM to view from the drop-down menu.

*Response: the **<cicm_name> cicm status** page opens.*




**c** Select **perform maintenance on <cicm_name>** option in the right menu bar.

*Response: The **maintenance status <cicm_name>** page opens.*

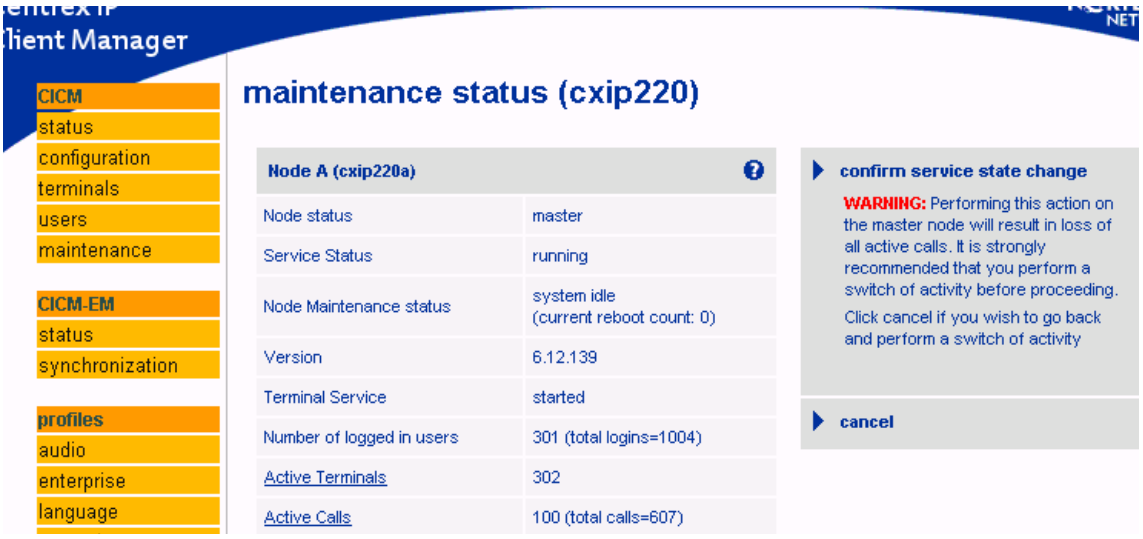



**d** In the **node A service control** or **node B service control** option on the right menu:

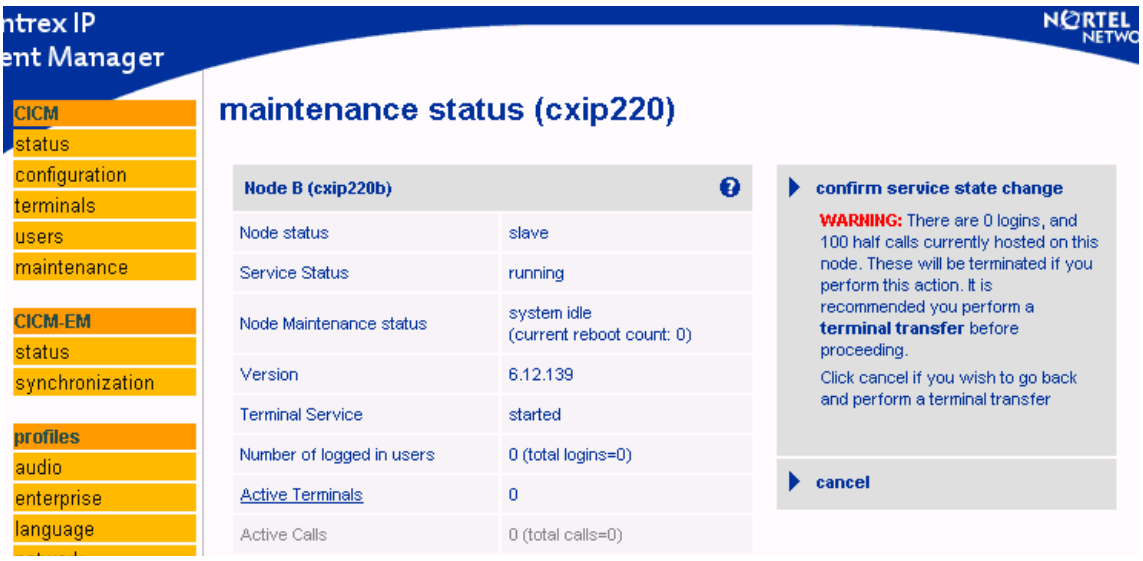
**i** Select **Stop** from the drop-down menu for the node to add the card(s) to,

**ii** Then click on the **node A service control** or **node B service control** option (corresponding to the node to add the card to).

*Response: The **maintenance status <cicm_name>** page displays the **confirm service status change** panel on the right.*
*If the node is the Master node, the **Warning** note will remind you to perform a Switch of Activity first, as in the illustration below. This switch of activity was done in step 6.*




*If the node is the Slave node, the **Warning** note will remind you to perform a terminal transfer before proceeding, as illustrated in the following illustration. This terminal transfer was done in step 3.*




**e** If a terminal transfer (step 3) or switch of activity (step 6) was not performed as required, then click on the **cancel** text and return to the **maintenance status <cicm_name>** page to complete these step(s).

**f** After verifying that the terminal transfer and switch of activity was performed as required:
on the **maintenance status <cicm_name>** page,

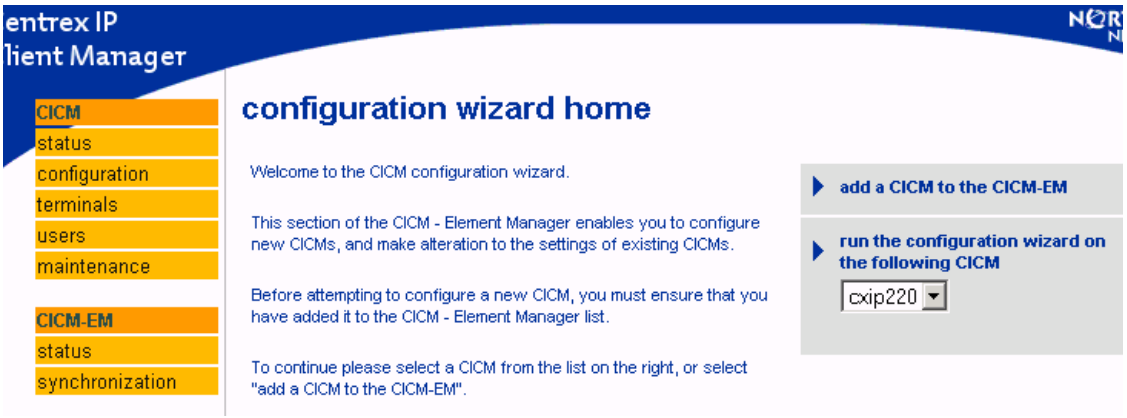
click on the **confirm service state change** text above the warning to stop the node service.

*Response: The CICM service is stopped on the selected node, and the node **Service Status** field changes to **stopped**.*

**8** Change the hardware configuration in the EM configuration wizard, as follows:

**a** On the Element Manager Web pages, select configuration from the **CICM** section of the left navigation bar.

*Response: The configuration wizard home page opens.*




**b** Select the CICM to run the configuration wizard on from the drop-down menu on the right, then click on the run the configuration wizard on the following CICM text.

*Response: The configuration wizard home on <cicm_name> page opens.*



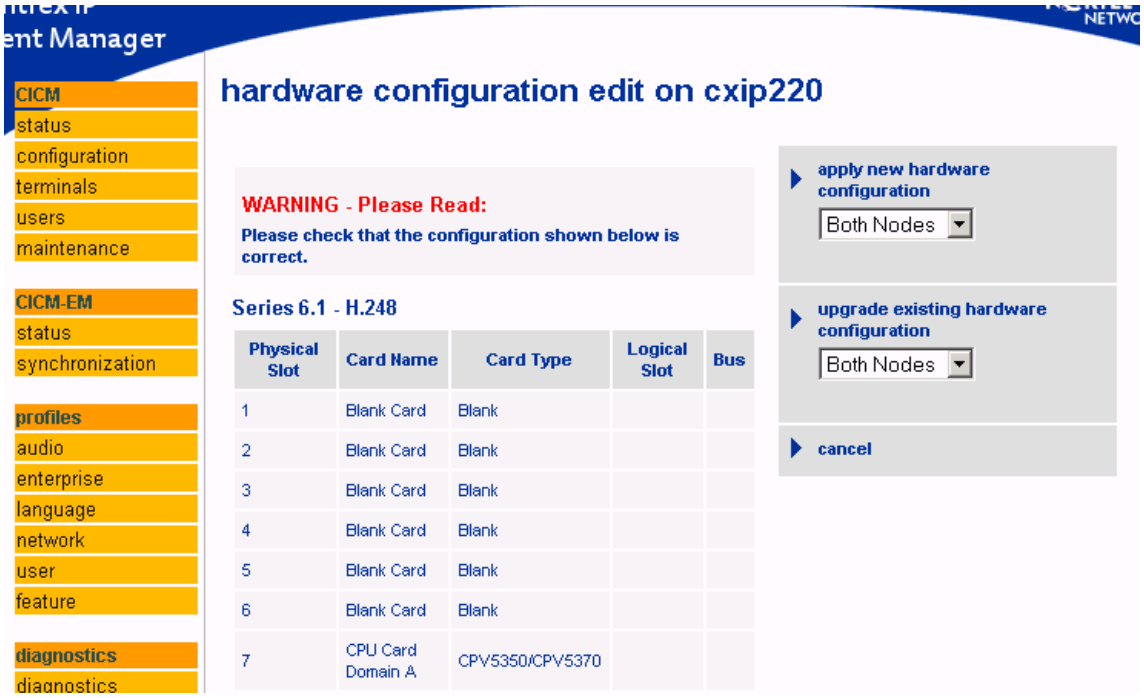
**c** Click on Hardware Configuration option from the Configuration Wizard window panel in the center.

*Response: The hardware configuration modification on <cicm_name> page opens.*




**d** From the choose new hardware configuration drop-down menu on the right, choose the configuration you desire to have (after you will add the new card(s) in the steps below), then click on the choose new hardware configuration text.

*Response: A **hardware configuration edit on cicm_name** confirmation page opens. A warning is displayed.*




**e** From the **upgrade existing hardware configuration** drop-down menu on the right, select:

- Both nodes
  If a symmetrical hardware upgrade is being made, with the same number of new cards being added to both nodes.
- Node A Only
  If the hardware upgrade is being made only to node A.
- Node B Only
  If the hardware upgrade is being made only to node B.

Then click on the **upgrade existing hardware configuration** text.

*Response: The configuration is upgraded and a confirmation window is displayed.*

**9** Complete the CICM configuration. All items on the Configuration wizard home on <cicm_name> page (i.e. Global Settings, Hardware Configuration, Virtual Media Gateways) must be in configured status before proceeding to the next step, as shown in the following figure.

***Note:*** After the hardware configuration has been upgraded in the previous step, the status of the CICM configuration items

changes to unconfigured, as indicated on the Configuration wizard home on <cicm_name> page. If any item is in unconfigured status, the CICM node will not be able to be put into service.




Assure that the CICM configuration is complete (all items in configured status) as follows:

**a** Verify that Global Settings is shown as **configured**.

**b** Verify that Hardware Configuration is shown as **configured**. This configuration is automatically datafilled upon selecting a hardware configuration.

**c** Verify that the Virtual media Gateways item is shown as configured.

**10** Shut down the node where the card(s) will be added, as follows:

**a** Open a Telnet session to the CICM node where the card(s) will be added, and type the following on the command line:

C:\>**shutdown /l /t:0**

Then press **Enter**

*Response: A request for confirmation is displayed.*

**b** To confirm the shutdown of the node, type

y

then press **Enter**

*Response: There is no confirmation from the Telnet session since the node is shut down. The shutdown status of the node can be checked by viewing the <cicm_name> CICM status Web page.*

**11** Power down the node where the card(s) will be added, as follows:

***Note:*** To minimize the level of impact on customer service, it is recommended to power down only the node of the CICM where the card(s) will be added. The mate node of the CICM will take over the workload in order to maintain services to all customers hosted on the CICM.

**a** Open a Telnet session to the CICM mate node (i.e. the node that is mate to the node where the card(s) will be added), and type the following on the command line:

C:\>**powerdown**

Then press **Enter**

*Response (example when the mate node is A):*

```
This CPU is in domain A
Continuing will power off domain B processor
resulting in the loss of all CentrexIP
service on that node.

Press ENTER to continue, Ctrl-C to abort.
```

**b** To continue to powerdown the node, press **Enter**

*Response:*

```
Powering down domain B processor
Powerdown complete.
```

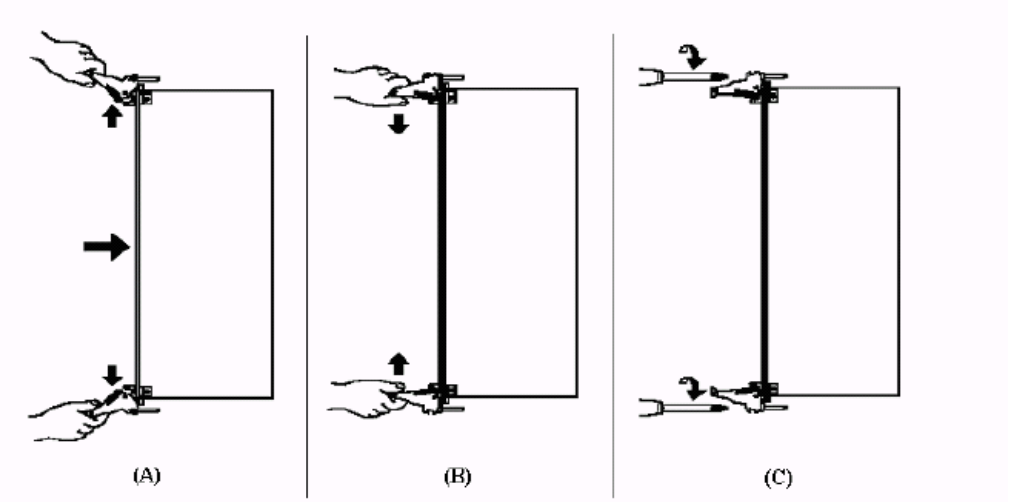
**12** Verify that the node is powered down by checking the following on the LED indicator panel (on the physical device) (In our example, the LED panel for node B):

**a** All LEDs on the CPU card (labeled CPV5370) are off, including the PWR LED.

**b** The PWR LED located on the CPU transition module located at the back panel of the CICM is off.

**13** Locate the slot number where the card(s) will be added, and remove the blanking plates from the slot positions that the card(s) will be placed into.

**14** Insert the new card into the CICM chassis, as illustrated in the following figure.




**a** Holding the ejector levers outwards, carefully insert the new card into the designated slot of the CICM.

**b** After the card is inserted, push the ejector lever towards each other. The card will be seated onto the back plane connectors by performing this action.

**c** Tighten the screws to secure the card to the designated slot.

**d** Repeat this step for all cards that need to be added. For each CPU card, add the associated Transition Module into the back of the chassis as well.

**15** Locate and connect the proper cable for each port on the new cards.

**16** Power up the node as follows:

**a** Establish a Telnet session to the CICM mate node.

**b** On the command line of the mate node, type the following:

C:\>**powerup**

Then press **Enter**

*Response (example for mate node A):*

```
Powerup: Power up the other domain processor.

This CPU is in domain A
Powering up on domain B processor
Powerup completed.
```

***Note:*** The service of the node will be recovered in 15-20 minutes.

**17** *(REQUIRED ONLY IF STEP 4 WAS COMPLETED)*

If the VMG unit was busied in step 4, return the VMG unit to service as soon as the <cicm_name> cicm status page shows the service is **running** on the upgraded node. Use standard CS2K procedures.

**18** Verify that the service has started correctly.
On the **<cicm_name> CICM status** page of the Element Manager Web pages, scroll down the **node modification on <cicm_name>** section to the **Service State** field, and verify that it is in the **running** state.

**19** Check that the configuration is correct, and update the configuration if required.

**20** Repeat this procedure for the opposite node.
If all the configuration steps for both nodes have been done when configuring the first node, then those configuration steps can be skipped for the second node.

**21** This procedure is complete.

# Upgrading non-MG 15000 gateways and gateway managers

Refer to your media gateway and gateway manager upgrade documentation.

# Upgrading the MCS Management Server

**ATTENTION**
Make sure you install the latest software loads. Check with your support team for the correct latest load.

## Requirements

The 2.0 software is currently installed on the system.

Nortel Networks strongly recommends the use of high-speed data network connectivity for optimum remote service capability. Without broadband connectivity, remote service options are limited. We recommend our Contivity Remote Access Solutions for this function.

Nortel Networks also recommends following standard data center conventions for having a Universal Power Supply (UPS) as the power backup for the servers.

For power over Ethernet in the closet switches, Nortel Networks recommends use of our Baystack 460 Power Over LAN layer 2 Ethernet switches.

Note also that

- For the Oracle* upgrade, this document assumes the default directory (/IMS/ora_cds) was used to install the Oracle data files. If this is not the case, then substitute the correct directory for all uses of the /IMS/ora_cds directory in the Oracle upgrade steps.
- If the 2.0 system being upgraded has an RTP Media Portal configured, please refer to the *RTP Media Portal Basics* document.

There are a total of 9 CDs available for the upgrade, including

- 6 CDs for Oracle 9.2.0.4 (Oracle CDs 1-6; these are the same as for a fresh installation in Windows*)
- 1 CD for the Solaris upgrade
- 1 CD for the System Management Console (This is the same as for a fresh installation)
- 1 CD for the 3.0 application software (This is the same as for a fresh installation)

The upgrade may fail for one of the following reasons:

- Solaris patch missing: Supplementary instructions will appear on the screen. Follow those directions and then attempt the upgrade process again.
- Solaris patch level is not correct (found using the **uname –v** command). If the patch level is less than or equal to 18 or MR27, the system cannot be upgraded. Contact your next level of support.
- Hardware is non-standard; the system cannot be upgraded. Contact your next level of support.

## Upgrade strategy

**ATTENTION**
For this entire process, it is best to connect to the console port either directly or by going through the terminal server. Do not connect to the server.

**ATTENTION**
The complete upgrade must be performed at one time. It cannot be split up. It is recommended that you install Oracle 9.2.0.4 to disk ahead of time to make sure there are no problems with reading in the data from the CDs. Total time required for upgrade is a minimum of 5 hours, depending on the size of the database.

This document covers the upgrade information for the basic 4-server system. For additional components, please see the appropriate component documentation.

Use the following procedures to perform your system upgrade:

- Upgrade Solaris* on every box.
- Remove and install the new Oracle on the database box.
- Upgrade the software to 3.0.

The upgrade consists of the following procedures:

- Copy Oracle CDs to the database.
- Install the new pool onto the Management Server.
- Perform backup of database.
- Stop all running components (including SysMgr processes) *except* the RTP Media Portal(s). The RTP Media Portals *must* remain in

service in order to provide continuous service environment during this upgrade procedure.

- Perform Solaris upgrade on all Sun boxes.
- Do the 3.0 imssipdb (Install Files Only) step.
- Update Database - remove and reinstall Oracle, import data, deploy imssipdb as a single database.
- Undeploy and redeploy Management Module.
- Install the 3.0 System Management Console.
- Upgrade all of the applications. Once the System Manager and Database are upgraded and brought back into service, each of the RTP Media Portals can be upgraded in turn.

***Note:*** Management Module and database have already been done.

## Estimated time of upgrade

The following table lists the estimated time for each of the steps to upgrade the system.

**Table 1 Estimated times for upgrade steps (Sheet 1 of 2)**

| Step | Time (in minutes) |
|---|---|
| 1. Install Oracle to disk. | 60 |
| 2. Install the 3.0 pool onto the MgmtSvr. | 15 |
| 3. Back up the database. | 15 |
| 4. Only stop the System Manager and Database. The RTP Media Portal *must* remain in service. | 10 |
| 5. Stop the SysMgr processes. | 5 |
| 6. Execute the Solaris upgrade CD. | 180 |
| 7. Update the database. | 120 |
| 8. Undeploy the Mgmtsvr and redeploy it with the new load. | 10 |
| 9. Begin using the 3.0 System Management Console. | |

**Table 1 Estimated times for upgrade steps (Sheet 2 of 2)**

| Step | Time (in minutes) |
|---|---|
| 10. Enter the 3.0 license key. | 5 |
| 11. Upgrade and start each RTP Media Portal in turn. | 30 minutes for each RTP Media Portal. |
| **Total estimated time** | **7.25 hours** |

## Key stroke symbols

The following key stroke symbols are used in this document:

| When you are asked to | You must... |
|---|---|
| Press **Esc+2** | Press Escape then press 2 |
| Navigate | Use the arrow keys to move up or down |
| Select | Use the spacebar to select an item |
| <Value in brackets> | Enter value indicated in brackets. |
| [Enter] | Press key indicated in brackets |

## Text conventions used in this document

This document uses the following text conventions:

- Bolded type is used to signify commands or buttons that you must press to perform an action, for example, **Apply.**
- Courier type is used to signify what appears on screen, for example, `Enter your password.`
- Italic type is used for emphasis, for special words, or for reference information; for example, "Log in as *root.*"

## Loading disks

Base Platform System Software disks are loaded on the following servers as indicated in Table 2, Mapping of Kit NTVW01BE disks to servers (with times)

**Table 2 Mapping of Kit NTVW01BE disks to servers (with times)**

| Base Platform System Software: Order code NTVW01BE | Approximate time to install | Database server | Management server | Management PC |
|---|---|---|---|---|
| Oracle CDs 1-6 | 60 minutes | X | | |
| Solaris upgrade (4 copies) | 180 minutes | X | X | |
| Upgrade software | 120 minutes | | X | |
| System Management Console software (Windows) | 30 minutes | | | X |

## CS 2000 documentation

In addition to the following documentation, be sure to refer to the customer-specific information (CSI) datasheet for your specific system requirements.

# Installing Oracle 9.2.0.4 to the database server

**ATTENTION**
Make sure you install the latest software loads. Check with your support team for the correct latest load.

## Upgrade preparation

You can copy the disks any time before you actually upgrade the Oracle database. There is no destructive behavior associated with this process, which takes about 1 hour. This procedure can be performed in advance on the database servers to ensure there are no problems reading data from the CDs.

For the Oracle upgrade, this document assumes the default directory (/IMS/ora_cds) was used to install the Oracle data files. If this is not the case, then substitute the correct directory for all uses of the /IMS/ora_cds directory in the Oracle upgrade steps.

If you enter a directory to install to, the directory must either be empty or non-existent to allow for easy removal of these files once the upgrade is completed.

**ATTENTION**
Perform this procedure on the database server only.

### Installing Oracle 9.2.0.4 to disk

***At the database server,***

1. Using the database console port on the in-Reach terminal server, log in as *root* to the database server, then
2. **cd /IMS** [Enter]
3. **du .** => returns the number of free blocks (The minimum required space is 4.6 GB. If enough space is not available, contact support.)
4. Press **Enter** to continue.
5. Insert CD 1 (repeat these steps for all CDs).

   ***Note:*** Use CD8 to CD13 with order code RMPP0070.
6. **cd /cdrom/cdrom0/** [Enter]

7 **cp Install_CD_to_Disk / [Enter]**

***Note:*** Make sure all the files were copied.

8 **cd / [Enter]**

9 **./Install_CD_to_Disk [Enter]**

10 Take the default directory, unless the required disk space is not available (3.5 GB) on the /IMS partition. (If you do enter a directory, that directory must either be empty or non-existent, which allows the easy removal of these files later.) Press **Y**, then **Enter**.

**ATTENTION**

After CD6 is installed, a Checksum is performed on each Oracle disk. Enter **Cntrl + C** to abort the script at any time.

Identify all Layer-2 switch ports that are connected to the Solaris hosts. This is required for the OS upgrade process in Executing the Solaris upgrade on page 1349.

Once the installation begins you will see the following various messages appear for each of the CDs:

```
Waiting for CD mount ….

Copying files from CDROM to /IMS/ora_cds/Disk1…

Waiting for CD mount ….

Copying files from CDROM to /IMS/ora_cds/Disk2 [or whichever disk is in the CD-ROM] ….

Performing check sum on /IMS/ora_cds/Disk1…
```

# Making a backup of the database

**Making a backup of the database**

**ATTENTION**

Before upgrading Solaris and Oracle,

- Make a backup of the database.

- FTP the backup file to another server or pc for safekeeping.

**ATTENTION**

The backup file is stored in /backup/orabackup. Move this file temporarily to another directory (/IMS/imssipdb); otherwise, it is deleted when you remove the old version of Oracle.

***At the database server,***

1 At whatever point you stop operations on the old database, make a backup of this database.

Log in as `oracle [Enter]`

2 Change to backup directory:

**cd /IMS/imssipdb/data/db_schema/backup** `[Enter]`

3

**ATTENTION**

When you back up the database, you create a <name_of_backup> file, for example, ims_3.0_build350.

The <name_of_backup> file contains the backup of the database that has an extension of .dmp.

Export to a backup directory: **./export_imsdb1.sh PRIMARY <name_of_backup> DISK** `[Enter]`

4 Log in as `sysadmin.`

5 `su root [Enter]`

6 **cd /backup/orabackup**

7 **cp <name_of_backup>.dmp /IMS/imssipdb** where <name_of_backup (for example ims_3.0_build350) is the name of the file that will be created and that contains the backup of the database with a .dmp extension. The backup file is stored in the /backup/orabackup/ directory.

***Note:*** This file must be temporarily moved to another directory; otherwise, it will be deleted in the step that removes the old version of Oracle. FTP this backup file to another server or pc for safekeeping.

# Installing the upgrade software on the Management servers

## Installing the 3.0 upgrade software to the Management servers

Use the CD that contains the MCP 3.0 software loads. This step takes about 15 minutes.

**ATTENTION**
For this procedure, use the disk labeled MCP_3.x.x_BXXX_CD6 upgrade disk (order code RMPC0070.4).

### Installing the upgrade software on the Management servers

***At the management pc,***

1 Using PuTTY SSH, log in as `root` to the Management server. `[Enter]`

2 **cd /cdrom/cdrom0**

3 **./install**

The CD will eject when this part of the installation is complete.

# Stopping processes

These procedures take about 15 minutes.

### Stopping all running components

***At the System Management Console,***

1 To stop a “running” component, right click on the component. Select **Stop** from the shortcut menu that appears.

2 Only stop the System Manager and Database Module. The RTP Media Portals *must* be left in service to provide continuous service during the upgrade.

### Stopping the SysMgr processes

***At the Management server,***

1 Log in as `nortel` to the Management server.

2 **cd /IMS/mgmtsvr/bin/mgmtsvr**

3 **./MgmtSvrShutdown.pl**

### Verifying all applications are stopped

***At the System Management Console,***

1 Check the display window of the Configuration tree.

***Note:*** Only stop the System Manager and Database. The RTP Media Portals *must* be left in service to provide continuous service during the upgrade.

2 Verify that all applications are stopped.

## Executing the Solaris upgrade

The upgrade script performs the following functions:

- upgrades kernel patch release
- installs the new version of NTme
- upgrades the DSM scripts

Use the Solaris Upgrade CD on all the servers, starting with the Management server. You can also start with the database, since you are already upgrading Oracle on that server. Perform these steps on all Unix machines in parallel if multiple upgrade CDs are available. Total time required is 3 hours.

**ATTENTION**
For this procedure, use the disk labeled MCP2.0-3.0 Upgrade disk (order code RMPC0070.4).

### Executing Upgrade script

***At the management pc,***

**1** Identify the Layer 2 switch ports that are connected to this Solaris host. At the layer 2 switch, enable auto-negotiation at the port speed configuration settings. The ports speed will not synchronize to full duplex until the end of the OS hardening process. This will be verified later in the procedure. This step takes five minutes.

**2**

**ATTENTION**
This procedure will cause a system reboot so it will be service interrupting. However, it is not destructive. This step takes about 10 minutes.

Log in to the appropriate server as `root`.

**3** Search for SUNWj3 packages:

**pkginfo -i | grep SNWj3**

If any SUNWj3xxx packages are installed, they will be listed.

4 Remove all listed packages:

**pkgrm <package name>**

Answer **Y** to all questions.

5 Perform this operation on the T1400 server that is acting as a combination System Manager and Database. This step takes about 2-1/2 hours. When this operation is complete, you will see a message saying: `Upgrade Complete.`

Use the console port or the terminal server login to execute this step. If you are telneted into a given server, the Solaris upgrade will not finish until the server is rebooted. The telnet break sequence is <cr>~^B (carriage return, tilde, control+b). This sequence has to be completed in 5 seconds in order to send the break sequence.

**a** Log in as `root` to the appropriate server.

**b** **cd /cdrom/cdrom0**

**c** **./upgrade**

**d** Answer "**Y**" to the Reboot prompt. The upgrade script then copies the required files to the /tmp/patch directory.

The script will apply the remaining patches and reboot the machine.

Next the script will prompt to see if you are ready to continue with OS hardening.

During OS Hardening of the server, password aging is enabled. In other words, after the server reboots and the user logs in as *root*, the system prompts the user to change the password. The user can reset the root password using its original value.

**e** Verify that the Solaris has been performed correctly by executing the command: **uname -v**
This should return the following: `Generic_108528-23`

If the patch level is not 29, then check the /usr/localbin/upgradelog file for errors.

6 At the Solaris host, invoke the command: **nicstat**.

7 Verify the following settings for all ports:

Autospeed: On

Status: Up

Speed: 100Mb

Mode: Full Duplex

8 Once the OS Hardening has completed, you will no longer be able to telnet into the machine. You must use an SSH connection to log into the machine.

In addition, you cannot SSH directly into the machine as the *root* user. You must first log in as *sysadmin* and then *su* to *root*. However, you will still be able to log in as *nortel* and *oracle*.

# Updating the database

## Prerequisites

Ensure the following:

- The System Manager and the Database are still "stopped" after the Solaris upgrade has been performed. All RTP Media Portals remain in service.
- Oracle is upgraded on database server.
- Solaris Upgrade is completed on the database server.

## Updating the database

This step takes about 2 hours.

### Installing the imssipdb load to the database

***at the pc***

1 Log in as `nortel` to the management server. `[Enter]`

2 Execute the dbdeploy.pl script. [`Enter`]

3 Select the appropriate imssipdb load (it should have 3.0 in the name somewhere). You will see the following statements or questions:

4 `"Is this a Replicated Database?"` Enter "**N**"

5 Select the Type of Deployment as "Install Files Only".

6 When prompted, enter the machine logical IP addresses of the database (DB), Mgmt Svr, and SysMgr (Mgmt Svr again).

7 `Is the above data correct?` Enter "**Y**".

### Upgrading the database to Oracle 9.2.0.4

***at the System Management Console***

1 Ensure there are no oracle logins to the database machine before the installation starts.

**a** Log in as `root` to the database (If the machine has been hardened, you will need to log in as `sysadmin` and `su` to `root`.).

**b** Type **who –u** `[Enter]`

**c** Look for logins as the 'oracle' user. If any exist, contact them and have them log off.

2 Remove current version of Oracle as follows:

**a cd /IMS/ora_cds/Disk1/install**

**b ./rmoracle** [Enter]

***Note:*** If there are logins as **oracle**, this script will not run. The following message will be displayed: `The oracle user has not been deleted, because someone is currently logged in as oracle. This is not a problem if you are going to install another version of oracle. Note, however, before you start the oracle installation, you must have every oracle user log out first. If this machine will not be used as a db machine any more, you must manually delete the oracle user.`

3

**ATTENTION**
Never **su** to oracle. Always log in as **oracle**.

Press to continue

4 Install Oracle 9.2.0.4 as follows:

**a cd /IMS/ora_cds/Disk1**

**b ./Oracle_Install | tee /tmp/oracleinstall.log**

5 When you receive prompts from the Oracle_Install script, use *oracle* as the new password. There is a delay before other prompts appear after you enter the password.

6 The Oracle_Install script prompts you for the following information:

**a** The database configuration. Select the one suitable for your product ("Enterprise").

**b** Replication information for this database. (Choose "**N**" when prompted with "`If replicated`.")

7 Confirm that your input was correct. (It takes about 45 minutes after this step is completed until the next prompt appears.)

***Note:*** After the input is confirmed, you will see the following message for each of the six disks:

```
Performing check sum of Oracle Disk1
Untar….
```

8 Take the default value when prompted for the local bin directory.

9 If prompted to overwrite files, enter "**Y**". (It takes about 5 minutes before the next prompt appears.)

10 "`Remove Disk 1….6 from /IMS/ora_cds`". Answer "**Y**".

11 Enter **Cntrl + C** after you receive the message "`Oracle_Install complete`".

### Importing data (from backup) to database

#### *at the System Management Console*

1 Log in as `oracle` to database machine. (Must log in again after the new version of database is installed.)

2 **cd /backup/orabackup**

3 **cp /IMS/imssipdb/<name_of_backup>.dmp .**

4 **cd /IMS/imssipdb/data/db_schema/backup**

5 **./import_imsdb1.sh PRIMARY <name_of_backup> DISK**

6 You will see the message "`Database setup complete`" when the process has finished. The time needed for completion depends on the size of the database.

### Deploying the new imssipdb bundle to the database (deploy it as a single database)

#### *at the System Management Console*

1 The following process takes 10 minutes.

Log in as `nortel` to the Management server using the new password.

2 Execute the dbdeploy.pl script.

3 Select the appropriate imssipdb load (it should have 3.0 in the name).

4 "`Is this a Replicated Database?`" Enter "**N**"

5 Select the Type of Deployment as "Upgrade of Database" (option 2).

6 When prompted, enter the machine logical IP addresses of the database, Management server, and SysMgr and the service logical IP address of the SysMgr.

7 Confirm that your data is correct.

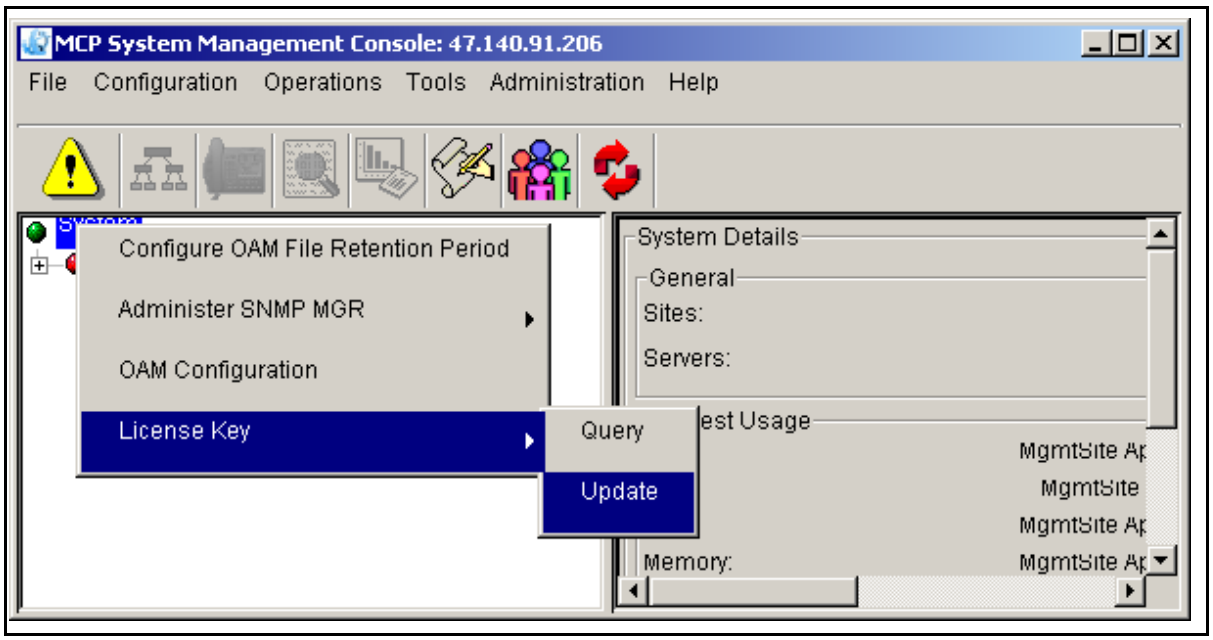
# Updating the License Key

### Updating the license key

***At the System Management Console,***

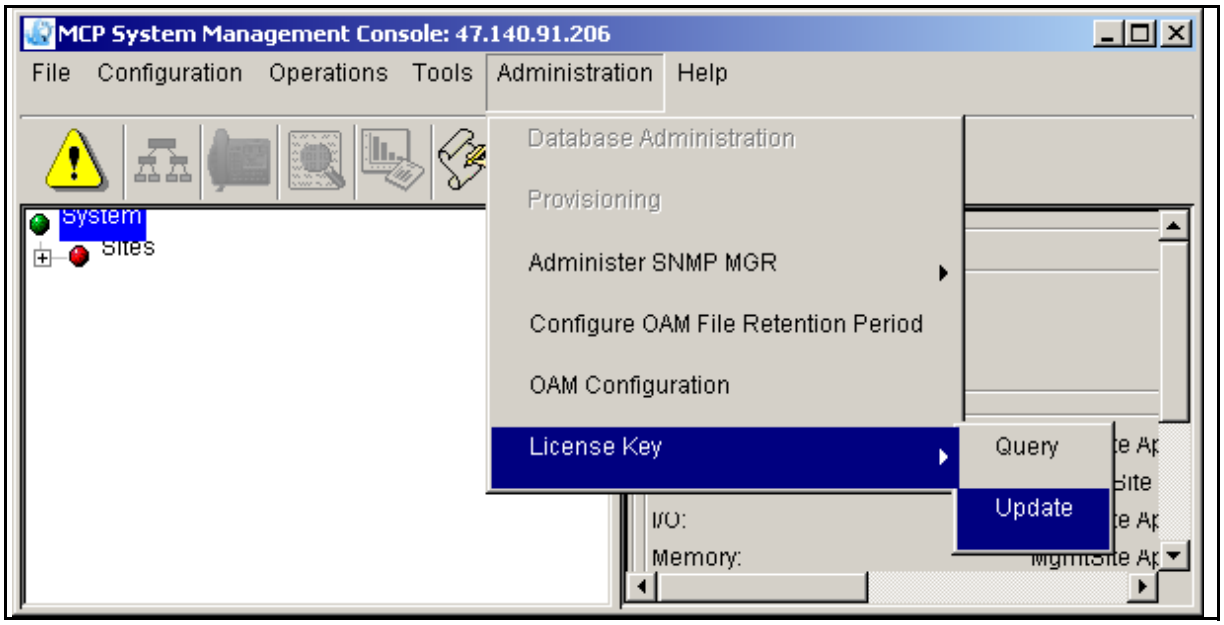
1 To update the license key from the System Management Console, you can select the menu option as shown in the following figure.

**Management Console Update License Key Right-Click Option**




You can also select the update option from the Administration menu, as shown:

## Management Console Update License Key Menu Option




2 Once you have selected the update menu item, you will see a dialog box. Select the appropriate license key and press the **Apply** button.

# Undeploying and redeploying the Management server

## Undeploying and redeploying the Management server with the new load

***at the pc***

**1** The following procedure takes about 10 minutes.

Log in as `nortel` to the Management server using your new password.

**2** Telnet into the management server: `<machine logical IP address of the MgmtSvr> [Enter]`

Example: 120.120.12.22

**3** Run the mgmtdeploy.pl script and answer the questions from the script.

**4** Select the appropriate mgmtsvr load (the one with small and 3.0 in the name for Enterprise.)

**a** "`Is this a Replicated Database?`" Answer "**N**"

**b** When prompted, enter the machine logical IP addresses of the database and Management servers.

**c** "`Will there be a SIP PriGwy or SIP Audio Svr Deployed?`" Answer "**N**" if you are not using a component running on a Motorola chassis.

**d** Verify that the above data is correct.

**e** `Do you want to undeploy` ..... Answer "**Y**"

**f** `Start up the SysMgr and TSS processes?` Answer "**Y**".

**g** Prints "`..... was successful .....`" when complete.

# Installing and launching the new System Management Console

## Installing the System Management Console

**ATTENTION**
Make sure that the version of the System Management Console you are installing matches the version of MCP software you are using.

**ATTENTION**
For this procedure, use the disk labeled MC_MCPX.X.X_BXXX.

### Installing the System Management Console on the customer-provided pc

***At the management pc,***

1 The following procedure takes about 5 minutes.

Put the CD (MCS Management Console PC software) into the pc's CD-ROM.

2 Navigate to the CD-ROM drive and double click on the executable immsc_setup.exe.

3 To install the System Management Console, click **Next**.

***Note:*** The file that contains all the previously entered IP addresses from the old version is saved and accessed by the new version of the System Management Console.

4 To select default program folder, click **Next**.

5 Keep default destination folder. Click **Next**.

6 Review settings before copying files. Make sure there is enough disk space before starting the installation of files.

7 Click **Next** to begin installation. You should see a popup window that reads "Installation successfully completed."

8 Click **OK**.

9 To launch the System Management Console, select **Start ->Programs ->MCP->System Management Console**.

**10** Fill in your login and password.

**ATTENTION**

Powering the Sun servers off and on from the System Management Console requires a modification to the management server computer. Each server you want to have the power feature on must have an entry in /etc/hosts.

Each entry in /etc/hosts requires an IP address and a hostname. The IP address must match the IP address in the IP address field found when querying the server from the System Management Console (for information on how to query the server, see the *System Management Console User Guide*. The hostname can be found by logging into the IP address as *nortel*, and typing *hostname*.

# Upgrading the RTP Media Portal

## Upgrading the RTP Media Portal

### *at the System Management Console*

**1** The following procedure takes about 2 hours.

From the System Management Console, upgrade the RTP Media Portal to a new load by right clicking on it in the tree and selecting Update from the shortcut menu.

**2** Use the following order to update the components:

**a** RTP Media Portal

**b** OracleMonitor

***Note:*** The Management Module and database have already been deployed.

## Updating the component tabs

At this point you can also upgrade the associated pc clients used in your system.

### Updating the components

***At the System Management Console,***

1. Log in to the System Management Console.
2. Expand by clicking **Sites->MgmtSite->Servers->Components ->><component you are updating>**

   In the case of UFTP, expand by clicking **Sites->MgmtSite->Servers->IPCMProvWCM ->BaseSoftware ->uftp**
3. Right click on the component you are updating.
4. Select **Update** from the shortcut menu that appears. A loadlist pop-up box appears.
5. Click on the latest component (Small) build.
6. Click **Apply**. The tabs will appear. Make any specific changes to the tabs and their fields that you need to make.

Check the configuration for each component. Press **Apply** when you are satisfied with the data entered in each of the components' fields. The following list shows only the changes that occurred with the MCS 3.0 upgrade.

## Changing the component configurations

When you update a component, the system maintains all the configuration values entered during the previous deployment. The following changes occurred in the components for this release.

### Accounting Module tabs

The Accounting Module does not require any new datafill. Press the **Apply** button to update this component.

### SIP Application Module tabs

The following tabs were deleted from the SIP Application Module:

- **Application Server**
- **SipFwdAdaptor**
- **Data Synchronization**
- **Registration**

The following tabs are new in release 3.0:

- **Registrar Service**

  One field: *Maximum Registration Duration* (default: 86400)
- **Server Subscription**

  One field: *provServerURL* (default: 0.0.0.0:5095:80:http)
- **Subscription Processing**

  One field: *maximumExpires* (default 86400)

The following changes occurred in the remainder of the tabs:

- **In Memory Database** tab

  The following fields were deleted:

  — *Number of call logs*

  — *IM CallLog DB write interval*

  — *Subscriber cache interval*

  The following field changed:

  — *Number of users (*default changed to 100000 from 131073)
- **Local Accounting Manager** tab

  The *Enable Billing For Instant Message* field was deleted.
- **Media Portal** tab

  The *ignoreMediaPortalInsertionRules* field was deleted.
- **Web Client Manager** tab:

  The *Allow Auto Login* field was added.

Press the **Apply** button to update this component.

**Provisioning Module (Web Bundle)**

The **Meet Me Conf Manager** tab was deleted.

There are two new fields in the **Web Client Manager** tab: *Allow Auto Login* and *Download JRE Version*.

**SIP Personal Agent tab**

The following fields were deleted:

- *SMTP Server*
- *Admin Email Address*

- *Send Email on User Signup*
- *Use Direct DB Connection*

Press the **Apply** button to update this component.

**IP Client Manager tabs**

The **Domains** tab has been deleted.

**IP Client Manager** tab fields are new, deleted, or changed as follows:

- *Max Number Devices* (new, default is 2000)
- *Max Login Duration* (new, default is 2678400)
- *Overflow Server* (new, default is 0.0.0.0)
- *Phase 1 Firmware ID* (new, default is B60)
- *Phase 2 Firmware ID* (new, default is A10)
- *Server Recovery Time Min* (new, default is 1)
- *Server Recovery Time Max* (new, default is 5)
- *F/W Download FileID* (deleted)

The **In Memory Database** tab is new.

**Web Client Manager tabs**

There are two new fields in the **Web Client Manager** tab: *Allow Auto Login* and *Download JRE Version*.

**Oracle Monitor tabs**

There were no changes for this release.

**iPlanet Monitor tabs**

The **iPlanet Monitor** tab name has changed to **Web Monitor**.

**H.323 Gatekeeper tabs**

The **H323GatekeeperBase** tab has changed. The *GatewayUser-Agent Header* field has been removed.

# Full release upgrades

## Operations, administration, and management

The Communication Server 2000 may try to contact the RTP Media Portal while the update is in progress, potentially generating error logs. To minimize impact to service, the RTP Media Portal should first be SHUTDOWN so that it does not accept new service requests. While shutting down, the RTP Media Portal will continue to process established media sessions. These pre-existing media sessions are cleared as the associated calls end. The RTP Media Portal automatically transitions into the LOCKED state when there are no active media sessions present. When this occurs, it is safe to proceed with the upgrade without affecting service.



**CAUTION**

It is possible to update and reboot one RTP Media Portal in a chassis, while the RTP Media Portal in the other half of the chassis continues to run the previous software. Once one RTP Media Portal is updated, the other RTP Media Portal in the chassis can be shutdown, locked, updated, and rebooted. This rolling upgrade will only impact available capacity and will not cause a service outage.

Upgrading all RTP Media Portals concurrently will cause a service outage.

If an upgrade fails during the initial stages, a rollback to the previous load is performed. A notification of the failure appears within the System Management Console.

If a component upgrade fails after the initial stages of the upgrade, it does not rollback automatically. A dialog box appears in the Management Console stating that the upgrade failed and prompts the administrator to determine whether a rollback should be performed.

The length of time required to complete the RTP Media Portal upgrade is approximately 30 minutes. While there is no impact to call-processing services, perform updates during low traffic periods to minimize reduced capacity.

## Upgrade tasks

This section provides instruction for a full release RTP Media Portal upgrade.

***From the System Management Console and terminal window***

1. Shutdown the targeted RTP Media Portal component. For details, please refer to Shutdown the target RTP Media Portal component on page 1365.
2. Perform the upgrade. For details, refer to Upgrade the RTP Media Portal component on page 1366.
3. Deploy the upgraded RTP Media Portal. For details, refer to Deploy the RTP Media Portal component on page 1367.

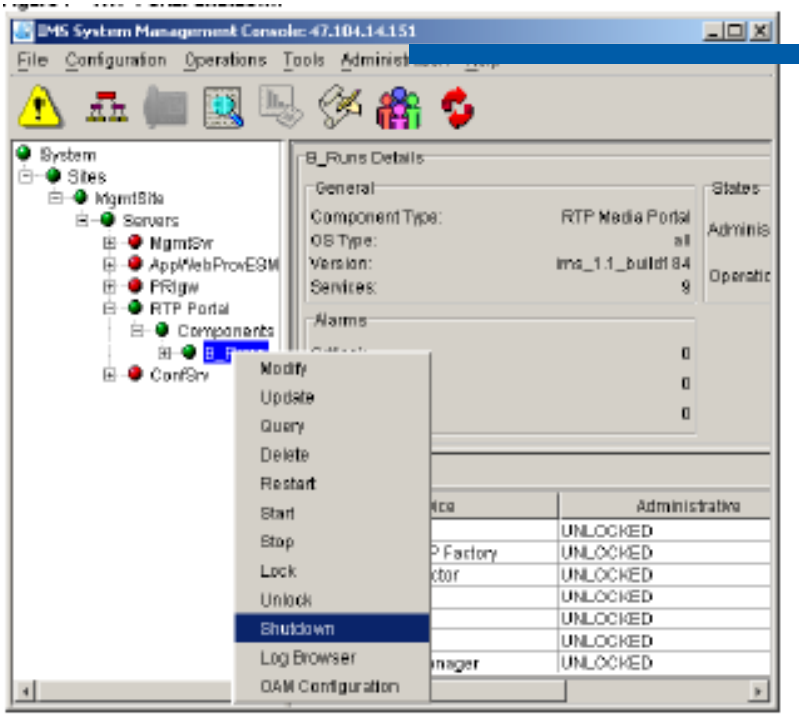
### Shutdown the target RTP Media Portal component

The following procedure describes how to shutdown the target RTP Media Portal component.

***From the System Management Console***

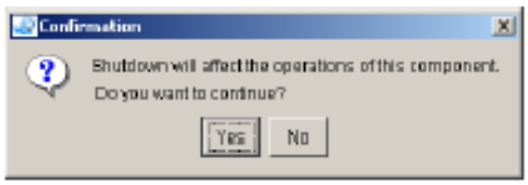
1. In the System tree, right-click on the target RTP Media Portal component.
2. From the pop-up menu, select the **Shutdown** command. Users may also choose the shutdown command from the pull-down **Operations** menu.

**Figure 1 RTP Portal Shutdown**




3 A confirmation window appears. Click on the **Yes** button to continue.

**Figure 2 RTP Portal Shutdown confirmation**




4 The RTP Media Portal component shuts down gracefully and eventually goes into a LOCKED state when the last active media session ends (as seen in the General Information Area of the System Management Console).

## Upgrade the RTP Media Portal component

The following procedure describes how to upgrade the RTP Media Portal load. Use Terminal Server access, or the main console with keyboard and monitor attached.

### *From a terminal window*

1 Log in as **root** on the target RTP Media Portal.

2 Insert the upgrade CD into the associated CD-ROM.

3 Mount the CD.

mount /dev/cdrom <Enter>
mnt/cdrom <Enter>

4 Change directory to the top-level directory on the CD.

**cd /mnt/cdrom** <Enter>

5 Run the install script.

**./install** <Enter>

6 Change directory.

**cd** <Enter>

7 Dismount the CD.

umount /mnt/cdrom <Enter>

8 Eject the upgrade CD from the CD-ROM.

**eject** <Enter>

9 Remove the upgrade CD from the CD-ROM.

10 Repeat step 2 through step 9 for each upgrade CD.

11 Reboot the RTP Media Portal.

**reboot** <Enter>

## Deploy the RTP Media Portal component

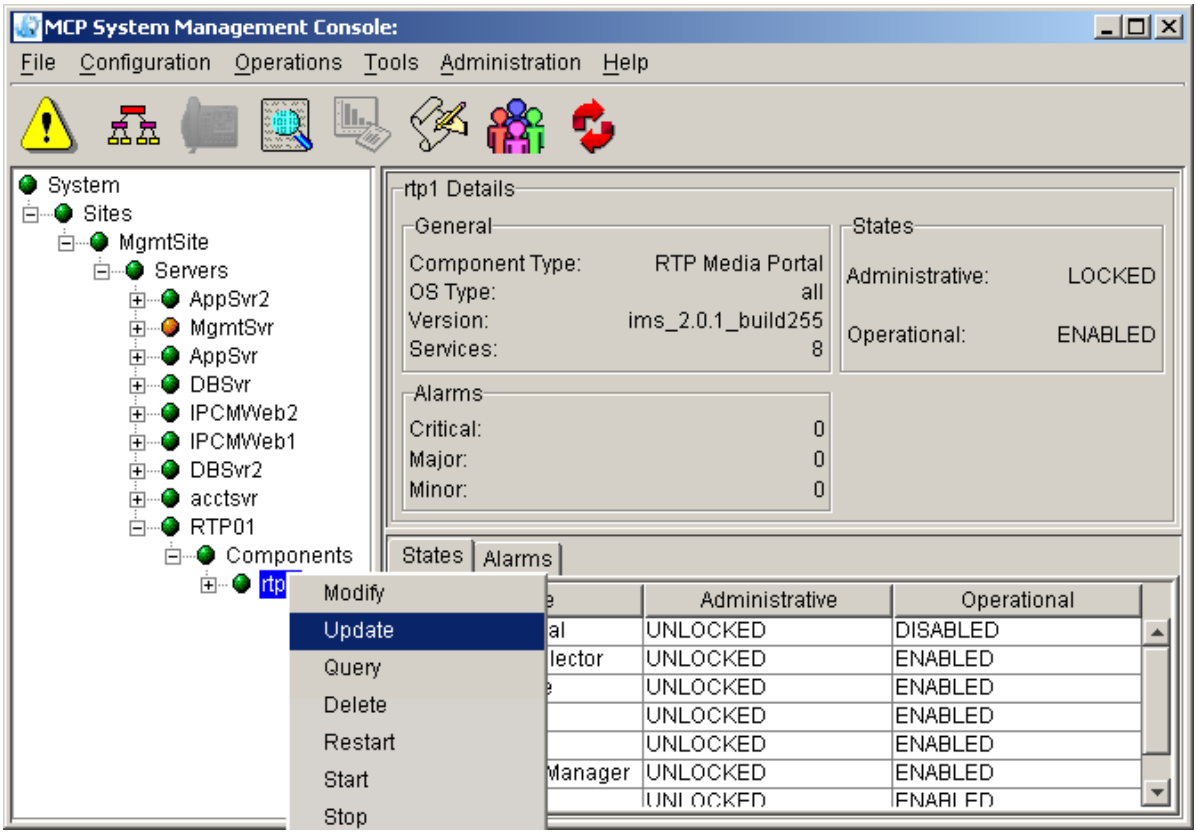
This section provides instruction to deploy the upgraded RTP Media Portal component.

### *From the System Management Console*

1 In the System tree, right-click **Components** under the appropriate RTP Media Portal server.

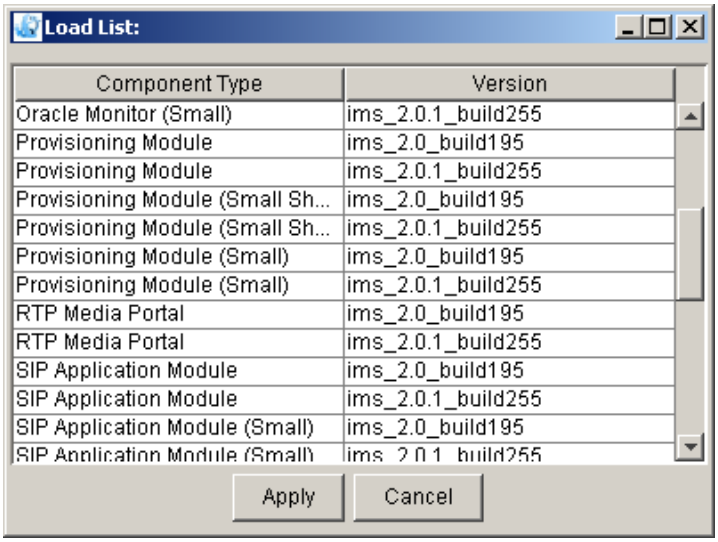
2 From the pop-up menu, select the **Update** command. This command may require substantial time to complete execution.

**Figure 3 Update from the pop-up menu**




**3** The Load List window appears with all available component loads (except for those components already deployed to the server).

**Figure 4 Load list**




**4** Select the desired software load version for the RTP Media Portal. Click on the **Apply** button.

**5** No reprovisioning is required as previous configuration information is applied.

**6** When deployment completes, and information dialog message appears to indicate that the action was successful.



Copyright © 2005, Nortel Networks


# Post upgrade tasks, patching, and additional procedures

## In this section

This section consists of the following information:

- Post upgrade procedures
- Succession Patching
- Additional Procedures

# Post-upgrade procedures

Complete the following optional post-upgrade procedures as needed after upgrading your network to (I)SN07.

**Table 1 Post-upgrade procedures**

| Requirement | Applicable Solutions | Documentation |
|---|---|---|
| **Re-enable the Network Patch Manager patch autoapply function** | All solutions | Re-enable the patch autoapply function after the completion of the office upgrade. This activity entails enabling the execution of the SYSTEMPLAN, which includes the AUTOAPPLY task.<br>Refer to Modifying a plan using the NPM on page 1759 |
| **Remove or update DCE** | IP solutions only:<br>PT-IP<br>PT-AAL2<br>IAW | Distributed Computing Environment (DCE) on page 1372<br>*CS 2000 Core Manager Administration and Security*, NN10170-611 |
| **Cutover USP messaging from core bounce to direct messaging** | IP solutions only | USP core bounce to direct messaging cutover on page 1374 |
| **Complete any required post-upgrade tasks for each component** | All solutions | Refer to the Completing the upgrade sections, later in this document. |
| Clean up old data in the NPM database | All solutions | Refer to Cleaning up old data in the NPM database on page 1902 |

# Distributed Computing Environment (DCE)

The Distributed Computing Environment (DCE) was decoupled from Succession in (I)SN05.

If you plan to remove DCE, upgrade the CS 2000 Management Tools server before removing DCE from the CS 2000 Core Manager. For information about removing DCE, refer to *CS 2000 Core Manager Administration and Security*, NN10170-611.

Some customers may choose to use DCE as part of an evolution plan for their OSSs, but this should be implemented in coordination with ASG Technologies/Passwerks or another security solution provider.

In (I)SN05 and later releases DCE is only an option for XA-Core and SDM access (ETA, ATA, and Secure EADAS). All other OAM&P interfaces, including the default/standard solution for XA-Core and SDM, will be using UNIX, DCE, PAM and Passwerks or another security solution provider for security.

Upgrades to (I)SN07 are not affected by DCE.

## Restrictions

(I)SN07 SAM21 Manager clients cannot be rolled back to (I)SN05 if DCE server is no longer present because communication between the CS 2000 Core Manager and CS 2000 Management Tools requires DCE. Rollbacks from (I)SN07 to (I)SN06 or (I)SN06.2 are not affected by removal of DCE since SAM21 is on SSPFS for both those releases.

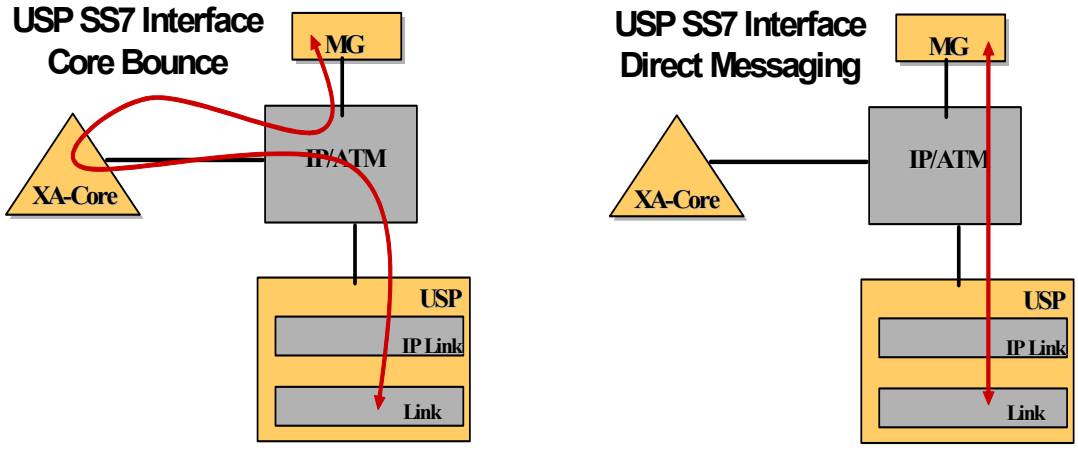
# USP core bounce to direct messaging cutover

**ATTENTION**
This section applies only to IP solutions using the Universal Signalling Point (USP) platform.

Core bounce messaging is messaging between nodes that must first pass or "bounce" through the XA-Core. The USP messaging path to the GWCs is set to core bounce by default. Direct messaging moves directly between nodes. Use this documentation to configure direct messaging between the GWC and USP. For additional information, refer to the Succession engineering guidelines for your solution.

You can perform an abort of the cutover at any time during the cutover procedure until final office cleanup step is completed.

The following figure illustrates the SS7 ISUP message path for Core Bounce compared with Direct Messaging.




This USP core bounce to direct messaging cutover documentation is divided into the following sections:

## GWC IPS7 provisioning

Use GWC IPS7 provisioning to provision the GWC IPS7 data on the USP. All GWCs setup to handle ISUP traffic must have two IP paths

provisioned. GWCs not set up to handle ISUP traffic do not require IP paths.

## GWC cutover from core bounce to direct messaging

Use GWC cutover from core bounce to direct messaging on page 1383 to perform the actual cutover to direct messaging of individual GWCs. All GWCs must be cutover to direct messaging independently, regardless of whether they handle ISUP traffic.

## Prerequisites

Obtain the following from your installation materials before starting this procedure:

- GWC number
- AS Name
- ASP Name (GWC)
- GWC IP address
- USP IPS7 card slot number
- Path ID



**CAUTION**

The core bounce procedures should be used with great care in an office that has working CCS7. Failure to do so can cause degradation to service on existing CCS7 links.

## Standard precautions

Observe all of the following standard precautions prior to and during this procedure.

- Observe all local general safety precautions against personal injury and equipment damage.
- Follow all Electro-Static Discharge prevention practices when handling any hardware. Refer to Method 03-9051, “Event 01 - Planning - DMS Physical Handbook.”
- Follow standard troubleshooting procedures, contacting the next level of support for assistance when required.
- At any point during the USP cutover procedure, you may be required to cut back to a previous point in the cutover procedure, or back out of the cutover completely.

- When re-booting the XA-Core with a previously backed-up image, it must be compatible with the image running on the USP.
- Always ensure that the USP and XA-Core datafill are aligned before images are taken on both of these components and only back up to versions taken within context of each other.
- If datafill misalignment is suspected, please contact the next level of support.

**Preparations**

The following preparations are essential preliminary work to do prior to completing this procedure.

- Nortel Networks strongly recommends that this USP core bounce to direct messaging documentation to be read in its entirety before starting these procedures.
- Prior to starting operations covered by this method, the tools and equipment should be arranged at the work location to minimize fatigue, inconvenience, and maximize productivity.
- The USP must be physically installed and commissioned prior to performing the cutover.
- To ensure proper balance of traffic within your network, Nortel Networks strongly recommends that you enable 8-bit SLS on the CORE.
- Ensure that an office image is taken of the XA-Core and the USP prior to performing this method.
- Determine which Gateway Controllers are setup to handle ISUP traffic. These GWC will require IP paths on the USP. All GWC must be cutover to Direct Messaging but may not require IP paths.

**Determine the current SLS state**

Also as part of the preparations for this procedure, determine the current SLS state as follows.

***On the XA-Core***

1 To enter the SLS8BIT level, enter the following:

**SLS8BIT**

If the SLS8BIT feature is available, the following output displays:

SLS8BIT

If the SLS8BIT feature is unavailable, the following output displays:

```
TEL00009 must be soc_on to activate/deactivate
8 bit SLS.
```

Contact your Nortel Networks Account Team to purchase the feature.

2 To display the current status of 8-bit SLS, enter the following:

DISPL

If 8-bit SLS is deactivated, the message "`8 bit SLS is deactivated`" displays.

If 8-bit SLS is active, the message "`8-bit SLS is activated`" displays.

3 After successfully entering the SLSBIT level, enter "**ENABLE**"

4 To exit the SLS8BIT level, enter the following:

**QUIT**

# GWC IPS7 provisioning

Use this procedure to provision Gateway Controllers (GWC) that handle ISUP traffic as an Application Server (AS) using the USP GUI. Once the GWC has been provisioned as an AS, two IP paths must be set up from the USP to the GWC. Each IP path is set up to a different IPS7 card on the USP. All IP paths between the USP and the GWC are set up to the active GWC. If 4 IPS7 cards are provisioned on the USP, engineering rules determine how the IP paths should be set up to the ISP7 cards based on call capacity.

## Provision GWC IPS7

***At the USP GUI***

1 From the main **USP** menu, click **Network Management**.

2 From the **Network Management** window, click **IPS7**.

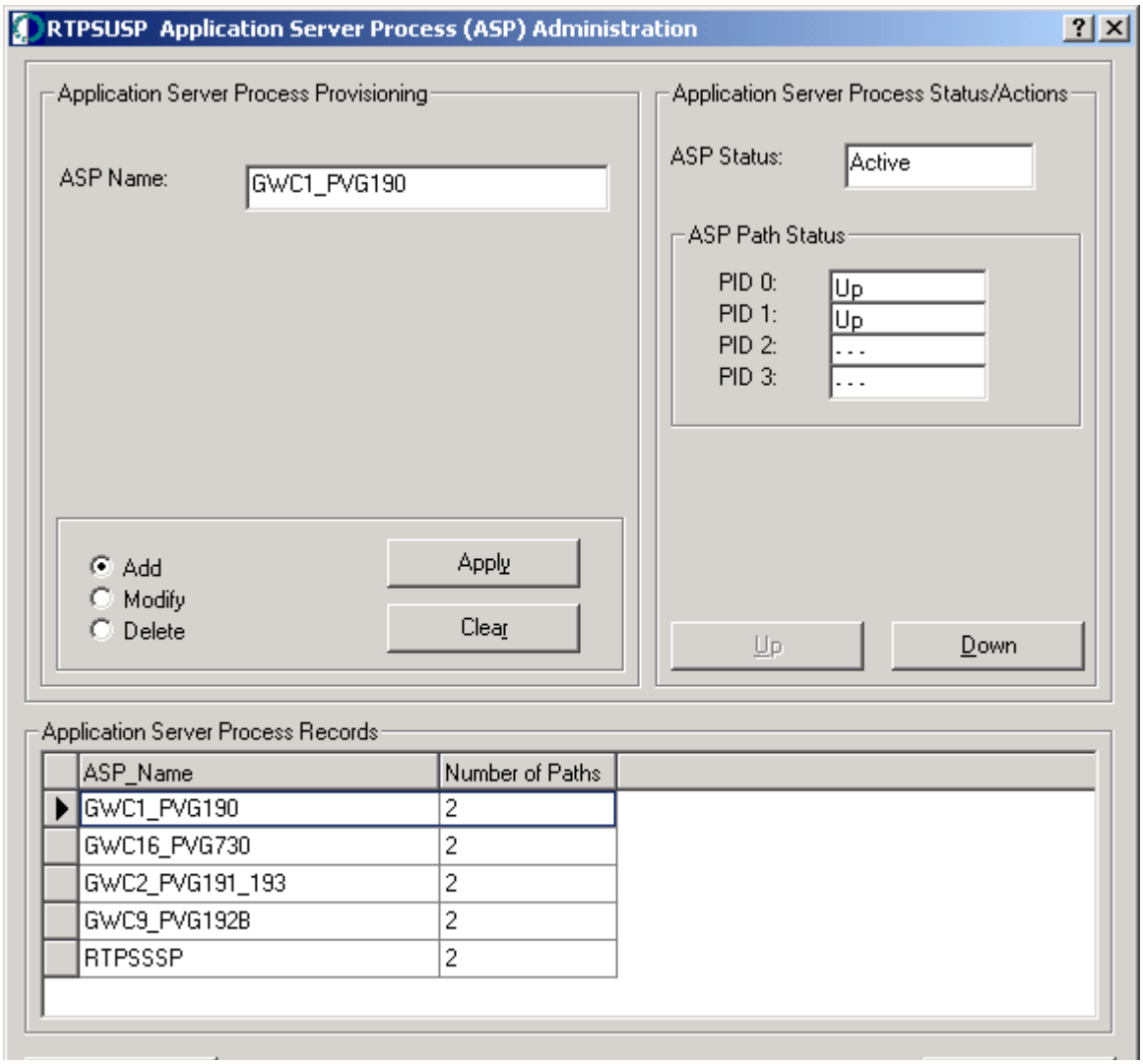
3 In the **IPS7** window, click **ASP**.

4 Enter the **ASP Name (GWC)** and click **Apply** and click **OK** to confirm the addition of the ASP and close the **ASP** window.

*The new ASP is listed in the Application Server Process Records window.*

*ASP status reads inactive.*

*No IP paths will be assigned at this stage.*



5 Click **AS** in the **IPS7** window and do the following:

**a** enter the name of the AS in the **Application Server Provisioning** window and

**b** select the corresponding **ASP Name** as the **Prim ary Process** and click **Apply** and close the **AS** window.

6 In the **IPS7** window, click **ASP Paths** and do the following:

**a** Select the **ASP Name**, **Path ID** (enter "0"), **Shelf Name** (USP shelf name) and **System Node Name** (IPS7 card) for the first IP path in the **Application Server Process Path Provisioning** window.

**b** Select **M3UAv2/SCTPv5_Client** as the Transport Protocol. The **SCTP Parm Index** = 0.

**c** Enter the IP Address of the **Application Server (GWC)** and its associated Remote Port for the IP path. The remote port is (**2905**).

***Note:*** Enter the active ip address of the Application Server (GWC).

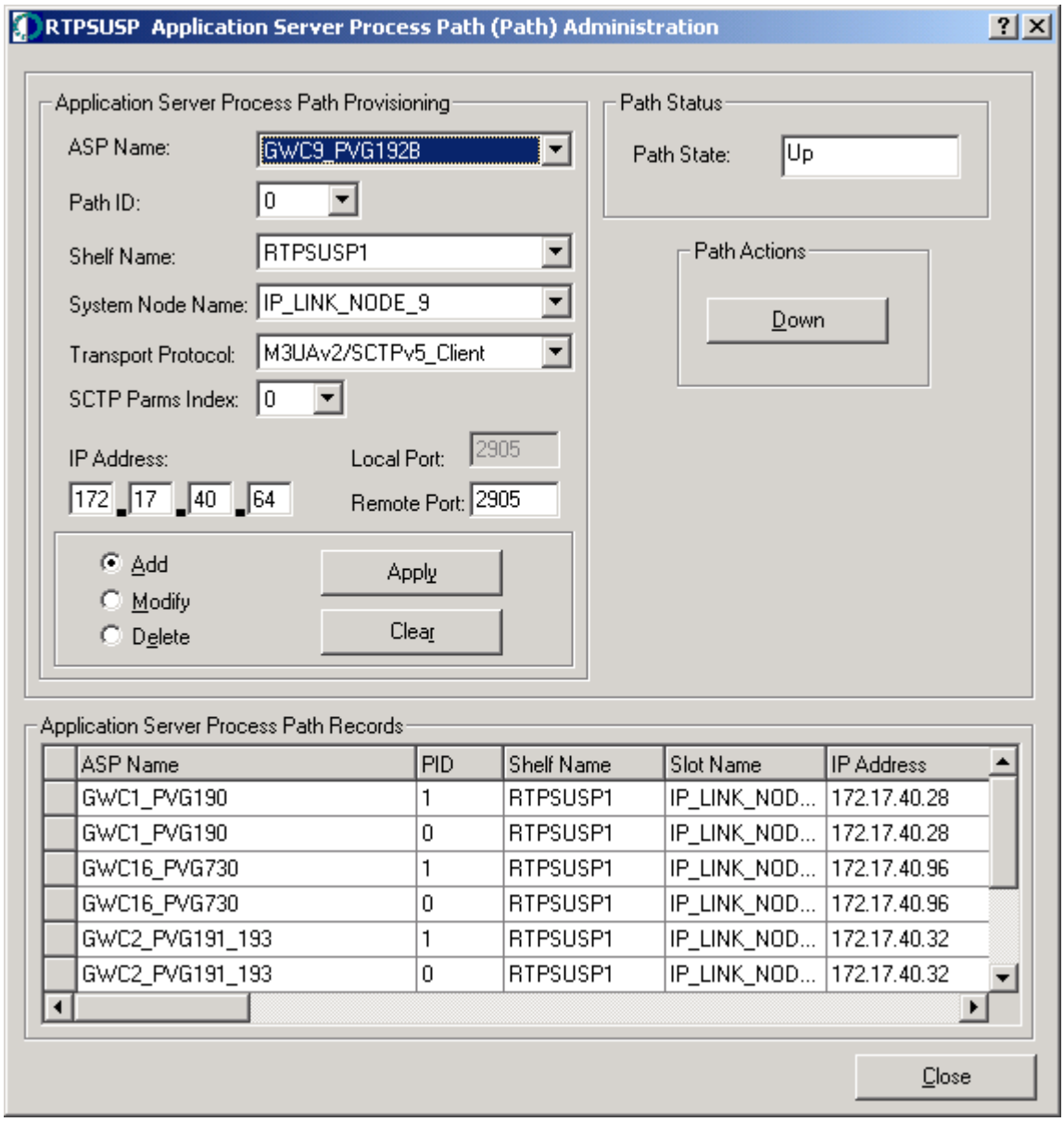
**d** Click **Apply** to add the IP Path.

7 In the **Application Server Process Path Records** window, do the following:

**a** Highlight the path and under **Path Actions** click **Up** to activate the IP path.

**b** Repeat step 6, adding an entry for the second path. Increment the path id to '1'.

*The following is an example of the **Application Server Process Path Records**.*



8 Close the windows as follows:

a Click **Close** to apply the changes and close the **ASP Paths** window.

b Close the **IPS7 Paths** window.

c Close the **Network Management** window.

9 Repeat this procedure for each GWC. Each GWC handling ISUP traffic must be set up as an AS and have two IP paths assigned.

# GWC cutover from core bounce to direct messaging

In CS 2000-based solutions, the Universal Signaling Point (USP) messaging path to the CS 2000 GWCs must switch from bouncing through the XA-Core to a direct messaging path.

***Note 1:*** It is essential that this procedure is completed to support future upgrades.

***Note 2:*** If at any time you need to stop or abort the USP direct messaging cutover procedure, refer to Aborting the USP direct messaging cutover procedure.

## Cutover the USP from core bounce to direct messaging

Use this procedure to perform the core bounce-to-direct-messaging cutover for the USP.



**CAUTION**

You must cutover all GWCs to direct messaging.

Table SERVRINV lists all GWCs. Use the **list all** command to display all GWCs.

To cutover each GWC to direct messaging, repeat step 9 through step 12.

***On the USP GUI***

1 From the main **USP** menu, click **Network Management**.

2 From the **Network Management** window, click IPS7.

3 From the **IPS7** window, click **ASP Paths**.

4 Verify that all IP Paths are up for each GWC and **Close** the **IPS7 Paths** window and **Network Management** window.

5 Check the USP and XA-Core for any service affecting conditions.

***On the XA-Core***

**6** Enter the **USPCUTOVR** level of the **MAP** as follows:

> **USPCUTOVR**

The following warning and cutover output displays:

```
WARNING: USPCUTOVR already active. Please
coordinate activities.

USPCUTOVR: USP cutover utility.
```

**7** Start USP cutover to direct messaging as follows:

**STARTCUTAS**

The following output displays:

```
STARTCUTAS must meet the following criteria
before continuing:
 1) AS Cutover is not already started
 2) LPP cutover to USP has been completed
STARTCUTAS command will perform the following:
 1) Update AS Cutover active state
Are you sure you want to continue?
Please confirm ("YES", "Y", "NO", or "N"):
```

**8** To confirm the USP cutover to direct messaging enter the following command:

> **Y**

**9** Perform this step for all GWCs.

**a** Switch the Application Server to perform direct messaging for the first GWC you want to cutover.

**> CUTOVAS GWC <gwc_number>**

The following output displays:

```
CUTOVAS must meet the following criteria
before continuing:
 1) Application Server must not be cutover
 2) STARTCUTAS must have been initiated
CUTOVAS command will perform the following:
 1) Notifies the specified Application Server
(AS) of cutover
```

```
 2) ISUP MHD data will be re-sent to USP with
the IP address of the Application Server to
allow for direct messaging.

ATTENTION:

Please ensure all Application Servers are
properly provisioned on the Universal
Signaling Point (USP) and all IP messaging
paths are inservice (UP).

Are you sure you want to continue?

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

**b** To confirm the switch to direct messaging, enter the following command:

**> Y**

**10** Display the SS7 message path for the previously cutover GWC, by entering

> **STATAS GWC <gwc_number>**

The following output displays:

```
Application Server Messaging Status: Direct
```

### *At the USP GUI*

**11** Verify that all IP paths to the GWC previously cutover are still up.

### *At the GWC*

**12** Verify that ISUP calls are completing as normal.

***Note:*** All GWCs, including those that do not handle ISUP traffic, must be cutover before the **CLEANUPAS** command can be performed.

## Aborting the USP direct messaging cutover procedure

### *At the USP*

1 Abort the cutover and switch the SS7 messaging path from direct messaging back to core bounce by entering

**> ABORTAS GWC <gwc number>**

The following output displays:

```
Starting ISUP MHD data transfer...
   100 tuples transferred.
   200 tuples transferred.
   .
Application Server cutover completed.
```

2 Repeat step 1 for all GWCs previously cutover.

3 Display the SS7 message path for the previously cutover GWC, by entering

> **STATAS GWC <gwc_number>**

The following output displays:

```
Application Server Messaging Status: Bounce
```

4 Stop the USP Application Server cutover process by entering

> **STOPCUTAS**

The following output displays:

```
Are you sure you want to continue?
Please confirm ("YES", "Y", "NO", or "N"):
```

5 Enter **Y** to complete the **STOPCUTAS** command. The following output displays:

```
Stop AS cutover started...
Stop AS cutover completed successfully
```

## Setting USP direct messaging as the office default



**CAUTION**

Once the cleanup phase has been completed you cannot return to core bounce messaging.

Therefore, you must take an office image of XA-Core and a snapshot of the USP before you do the next procedure (Setting USP direct messaging as the office default).

***At the USP***

1 Issue the CLEANUPAS command as follows to set USP direct messaging as the office default:

**> CLEANUPAS**

The following output displays:

```
CLEANUPAS must meet the following criteria
before continuing:

 1) All Application Servers are cutover 2) USP
direct messaging cutover is NOT already complete

CLEANUP command will perform the following:

 1) Set USP Direct Messaging state

Are you sure you want to continue?

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

2 Enter "**Y**" to confirm the cutover to direct messaging.

**> Y**

The following output displays:

```
*****************************

* WARNING * WARNING * WARNING *

*****************************

Confirmation of this command will permanently
set USP direct messaging. There are no
procedures to abort this command!

*****************************
```

```
Please enter CLEANUPAS to continue, or NO to
cancel.

Are you sure you want to continue?
```

3 Confirm USP direct messaging is set as the office default.

**> CLEANUPAS**

The following output displays:

```
Cleanupas started...

USP Direct messaging is now the office default.

Cleanupas completed successfully.
```

4 Exit the **USPCUTOVR** utility.

# Completing the Preside MDM upgrade

## Post-migration checks

After completing the software upgrade for Nortel Networks Preside Multiservice Data Manager (MDM) servers, you must verify that the servers are functioning correctly.

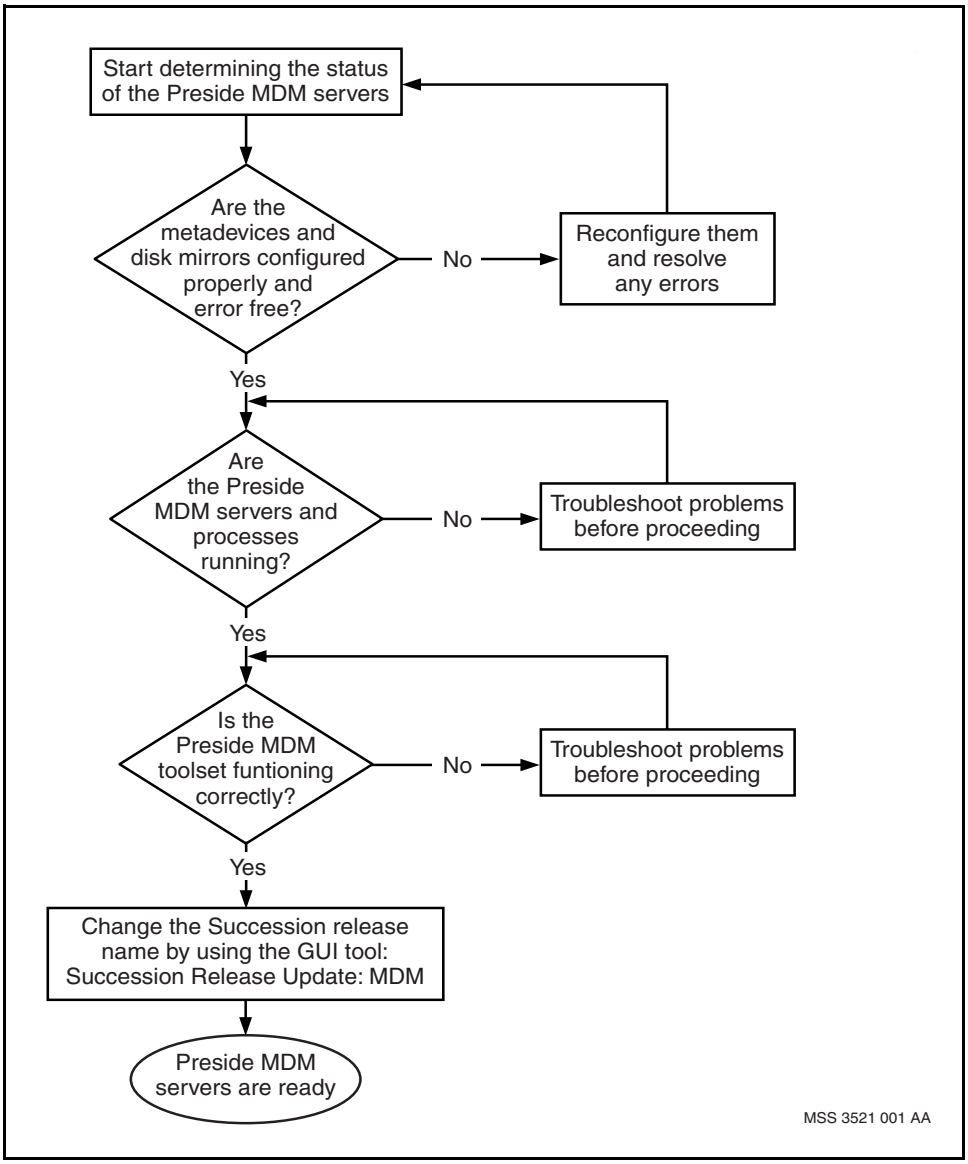
## Prerequisites

You must have:

- access to a text editor on the terminal connected to the servers so that you can open various files. We recommend using the UNIX VI text editor.
- an advanced knowledge of UNIX and Preside MDM tools and software.

The figure Preside MDM post-migration check task flow on page 1390 shows you the sequence of procedures you must perform to determine the status of the servers after a migration.

**Figure 0-1 Preside MDM post-migration check task flow**




## Post-Migration checks

After you have successfully completed the upgrade, perform the following procedures:

- Verifying the status of the metadevices and disk mirroring on page 165
- Verifying that Preside MDM servers and processes are running on page 166
- Verifying that Preside MDM servers and processes are running post-migration on page 1391

## Verifying that Preside MDM servers and processes are running post-migration

***From the Preside MDMserver***

1 Login — see Logging into Preside MDM servers on page 522.

2 Open a Preside MDM window — see Opening the Preside MDM window on page 522.

3 From the window, choose Administration > Server Administration.

4 Scan the server list and verify that all of the servers are in a *Running* state.

***Note:*** See the 241-6001-310 *Preside MDM Server Reference Guide* for information on starting a server.

5 To view more detailed information about the server, click on the name of the server whose information you wish to view.

6 From the Edit menu, select *View*.

The server name in the Server Administration dialog indicates the descriptive name assigned to the server.

7 Click *OK* when you have finished with the dialog.

8 Close the Server Administration tool.

9 From the Preside MDM window choose System -> Administration -> GMDR Administration.

***Note:*** For more information, see Using the GMDR Administration tool in the 241-6001-303 *Preside MDM Administrator Guide*.

10 Ensure that there are two FMDR servers for every distinct Succession office, and two IMDR servers (total) listed. Ensure that each server is associated with a different workstation, and that all are in a connected state.

11 Close the GMDR Administration window.

12 If you have migrated from release MDM 14.3 and the MDP servers were installed, use the Server Administration tool to ensure the servers are running.

The servers must be started in the following sequence:

- MDP Disk Manager (mdpdiskmgr)
- MDP File Mover Manager (mdpfmmgr)
- MDP Data Model Manager (mdpdmm)

- MDP Passport File Manager (mdppmgr)
- MDP File Prober Manager (mdpfpmgr)

***Note:*** Start the Server Administration tool using the "mdpadmin" userid used to start the MDP servers.

If the installation was successful, follow these steps.

***From the Preside MDM server***

1 If the software was downloaded successfully, remove the software download directory:

**rm -r /MDM151**

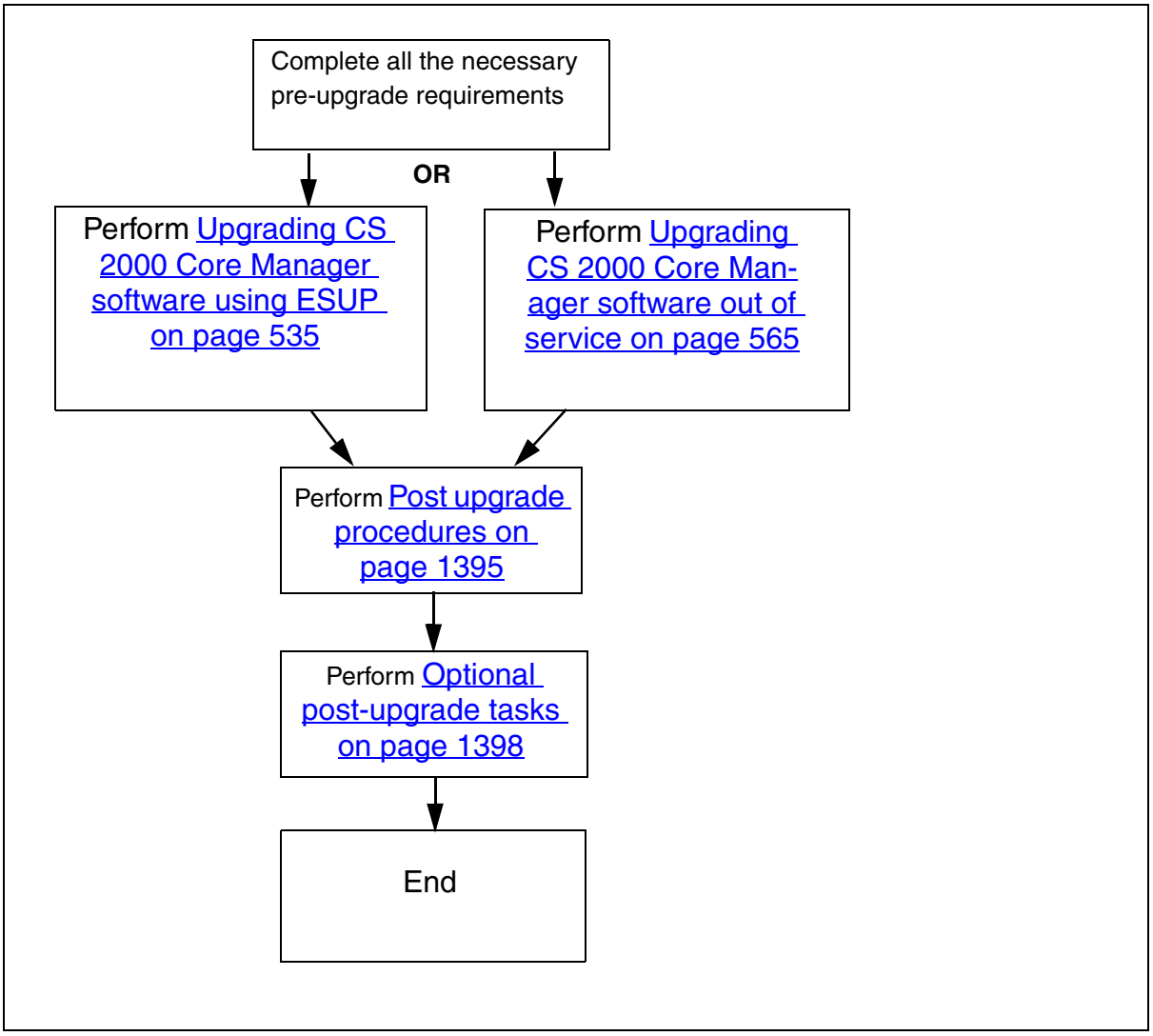
2 Remove the software patch directory:

**rm -r /patch151**

# Completing the CS 2000 Core Manager upgrade

Use the following task flow to complete the software upgrade.

**Task flow for completing the CS 2000 Core Manager upgrade**



## Purpose

After completing specific software upgrade tasks, you must perform the following post-upgrade procedures:

- verify the application state, to ensure that all applications are in-service. Use the procedure Verifying the application state on page 1395.
- verify the current software load, to confirm that the upgrade was successful. Use the procedure Verifying the current software load on page 1397.
- perform a backup of your new system image. Use the procedure "Creating system image backup tapes (S-tapes)" in *CS 2000 Core Manager Administration and Security*, NN10170-611.

If the upgrade software was delivered using Electronic Software Delivery (ESD), you will have an ESD logical volume on your system, which must be removed to free up disk space. Follow the instructions in the procedure Removing an ESD logical volume on page 1399.

If you upgraded from tape, eject the CS2E0070 NCL 7.x (1 of 1) from the tape drive and store it in a safe place.

Depending on the configuration of your network, you may also be required to:

- remove any DDMS filesets and logical volumes which you no longer require. See the procedure Removing DDMS filesets on page 1455. Succession PT-AAL1 offices MUST perform this procedure.
- upgrade and configure client-side application software on the required workstations in your network. See the procedure Upgrading and configuring client-side application software on page 1398.
- apply additional software patches. Contact your Operations management office to determine if and when any patches need to be applied to your system. If you need to apply a patch, use the procedure Upgrading the CS 2000 Core Manager with software patches on page 590. For more information, contact your next level of support.

# Post upgrade procedures

## Verifying the application state

### *At the VT100 console*

1 Access the application level of the CS 2000 Core Manager maintenance interface:

```
# sdmmtc appl
```

2 Determine whether all applications are in-service (indicated by a dot under the “state” heading next to each application that is in-service).

***Note:*** The Passport Log Streamer application will be in an offline state and unconfigured if you had the Succession log delivery application installed and configured with parameter “Passport 15000 present in the network” set to “No” prior to this upgrade. Refer to “Installing and configuring the log delivery application” in the Configuration Management document to configure it and return it to service. When complete, return to this procedure and continue where you left off.

| If | Do |
|---|---|
| all applications are in-service | step 7 |
| not all applications are in service | step 3 |

3 Manually busy (ManB) each application that is not in service:

```
> bsy <x>
```

*where*

**<x>**
is the number next to one of the applications that is not in service

Response

```
Application Busied - Command complete.
```

4 Repeat step 3 for each application that is not in service.

5 Return each application to service (RTS):

```
> rts <x>
```

*where*

**<x>**
is the number next to each application you busied in the previous step.

Response

```
Application RTS - Command complete.
```

6 Repeat step 5 to return each application to service.

7 You have completed this procedure. To confirm that the upgrade was successful, perform the procedure Verifying the current software load on page 1397.

## Verifying the current software load

### *At the CS 2000 Core Manager console*

1 Exit the maintenance interface:

```
> quit all
```

2 Verify that the product code, located at the top left-hand corner of the screen, is CS2E0070:

```
# querysdm loads
```

| If the product code | Do |
|---|---|
| is CS2E0070 | step 3 |
| is *not* CS2E0070 | contact your next level of support |

***Note:*** Dashes (----) displayed next to the platform maintenance are part of a normal output.

3 You have completed this procedure. Proceed to Optional post-upgrade tasks on page 1398.

# Optional post-upgrade tasks

**ATTENTION**

If your system is configured with the Distributed Computing Environment (DCE) service, and you plan to remove it, make sure that you do not decommission the DCE until the CS 2000 Management Tools server is upgraded. Otherwise, communication outages between the CS 2000 Core Manager and the CS 2000 Management Tools server will occur.

DO NOT decommission DCE if your system is configured with any DCE-dependent application, such as ETA, ATA, SFT, or GR740 Pass Through.

## Upgrading and configuring client-side application software

1 Upgrade and configure client-side application software on the required workstations in your network. Refer to the specific application procedures in the CS 2000 Core Manager information suite. For the CS 2000 SAM21 manager client application, refer to the Upgrading the CS 2000 SAM21 manager GUI client application procedure.

***Note:*** You may need to contact your system administrator, as client-side upgrades require root access to the workstations.

2 After your CS 2000 Core Manager is upgraded from the CS2E0004 to the CS2E0070 load, but the CS 2000 Management Tools server is not upgraded yet, a communication outage between the server and the core may occur. To re-establish the communication, complete the following substeps.

**a** Stop and start the DDMS proxy on the CS 2000 Management Tools server. Refer to the Stopping and starting the DDMS proxy procedure in the Upgrades section.

**b** Stop and start the Tomcat Servlet Container component on the CS 2000 Management Tools server. Refer to the Stopping and starting the Apache Web Server and Tomcat Servlet Container procedure in the Upgrades section.

**c** Configure the SESM server application. Refer to the procedure “Configuring the SESM server application” in *Upgrading the CS 2000 Core Manager*, NN10060-461.

3 You have completed this procedure.

## Removing an ESD logical volume

**ATTENTION**
If you choose to remove the ESD logical volume from the CS 2000 Core Manager, the removal is permanent.

### *At the CS 2000 Core Manager*

1 Access the storage level:

```
# sdmmtc storage
```

2 Remove the ESD logical volume and its contents:

```
> esddel
```

3 When prompted, confirm the Delete command:

```
> y
```

4 Exit the maintenance interface:

```
> quit all
```

5 If you upgraded from the CS2E0004 or CS2E0005 load, and you have SAM21 EM on your system, the SAM21 EM application on the SDM is temporary. Please see section “Upgrading the CS 2000 Management Tools” in this document for migrating SAM21 EM from SDM to SSPFS platform. Once the migration is completed successfully, remove the SAM21 EM fileset from the SDM using procedure “Removing CS 2000 Core Manager application filesets” in the Upgrade section of this document.

6 You have completed this procedure.

## Performing a system image backup

1 Perform a backup of your new system image using the procedure “Creating system image backup tapes (S-tape) manually” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

***Note:*** If you choose not to perform a backup of your new system image, the CS 2000 Core Manager will be in-service trouble (ISTb) and the status of the Backup Status alarm will be *Required* (if the alarm is enabled). You can force-clear the alarm using the procedure “Clearing a system image backup Required or Failed alarm” in the Fault Management document. If the backup Required alarm is disabled, the alarm will not be raised.

Return to Task flow for upgrading the CS 2000 Core Manager on page 524.

# Adding I/O controller modules

## Purpose

Use this procedure to add one of the following hardware modules to the CS 2000 Core Manager:

- NTRX50FU - I/O controller module with two 2-Gbyte disk drives and Ethernet
- NTRX50GP - I/O controller module with two 4-Gbyte disk drives and Ethernet
- NTRX50NL - I/O controller module with two 36-Gbyte disk drives and Ethernet
- NTRX50NY - X.25 controller module

I/O controller modules do not require LAN personality modules (NTRX50FS) installed at the back of the CS 2000 Core Manager except for the mandatory NTRX50GN I/O controller modules located in slots 2 and 3, and slots 13 and 14.

I/O controller modules can be added to slots 4 and 5, and 15 and 16, of the CS 2000 Core Manager main chassis, and to unoccupied slots in the I/O expansion chassis. All available slots can be used in the I/O expansion chassis to install two I/O controller modules as a logical pair; however, the left slot position of the left I/O controller module must be 8 slot positions apart from the left slot position of the right I/O controller module of the pair. For example, if the left I/O controller module of the pair occupies slots 1 and 2, the right I/O controller module must occupy slots 9 and 10. Both modules in a logical pair must have the same PEC.

The rear LAN personality module I/O controller module must occupy the lower number of the two rear slots that are associated with the front module. For example, if the new I/O controller module occupies front slots 4 and 5, its associated LAN personality module must be installed in rear slot 4. The unused rear slots remain covered by filler plates.

## Prerequisites

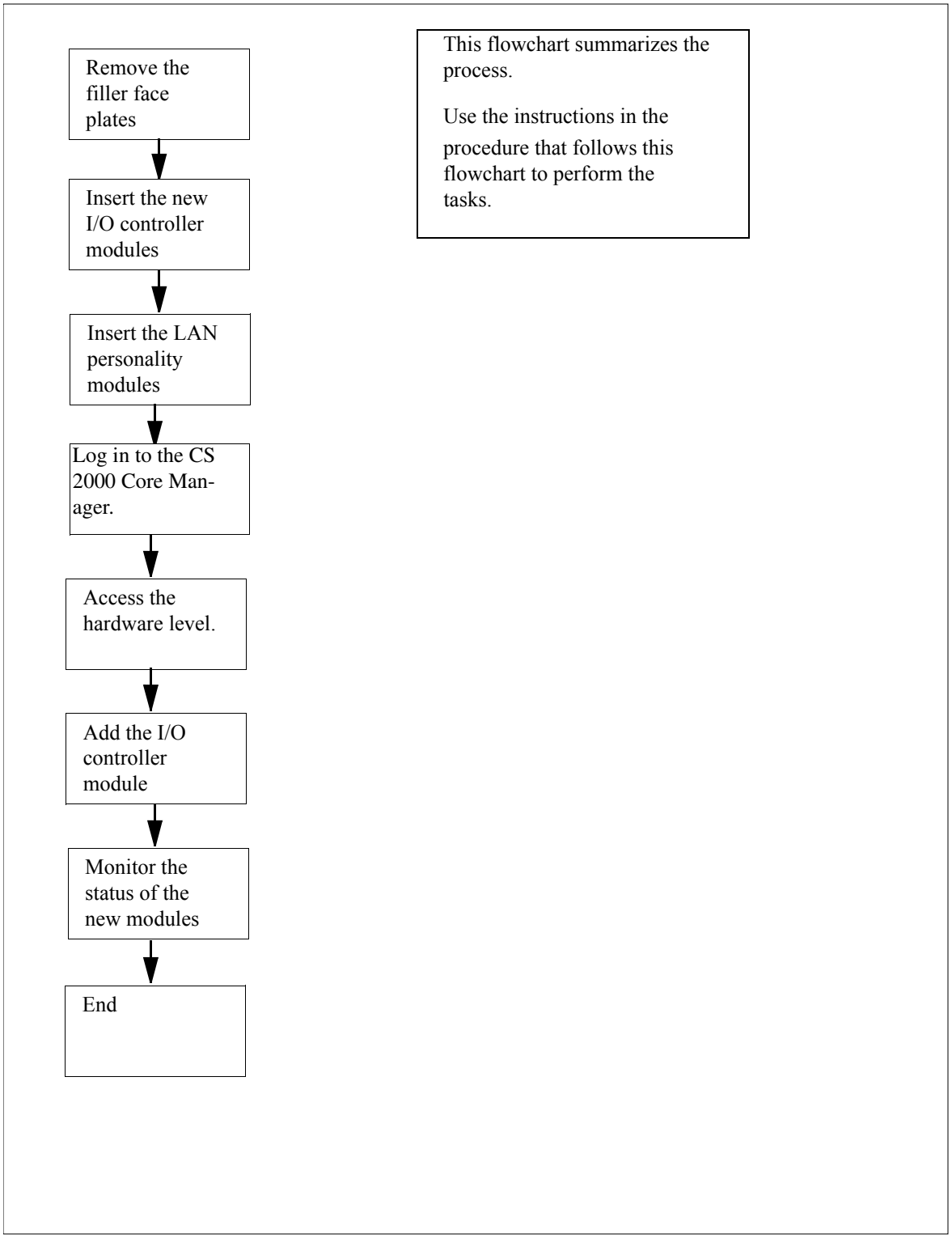
To perform this procedure, you must have the following information:

- the chassis type (SDMM for a main chassis; SDME for an I/O expansion chassis)
- the I/O controller module's slot number (from 1 to 16)
- the I/O controller module's product engineering code (PEC)

## Task flow diagram

The following flowchart provides an overview of the process. Use the instructions in the procedure that follows the flowchart to perform the task.

## Task flow for Adding I/O controller modules



# Procedure

## Adding I/O controller modules

### *At the front of the CS 2000 Core Manager*

**1**



**WARNING**

**Static electricity damage**

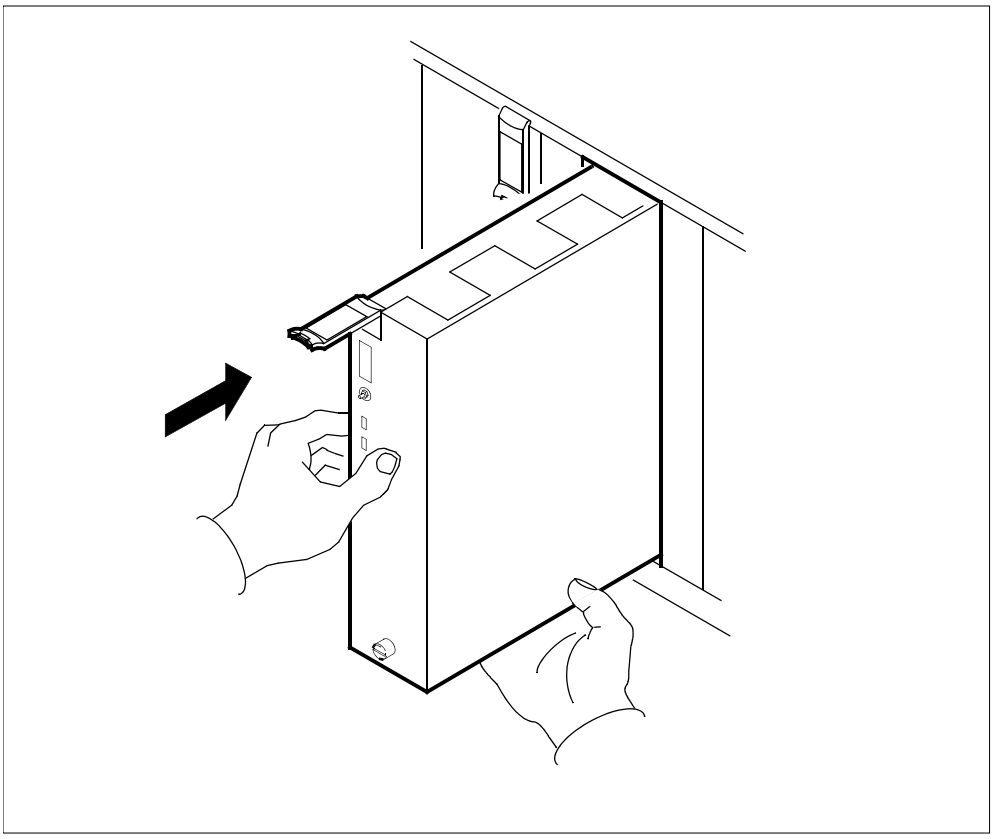
Wear an ESD grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on the ESD grounding wrist strap.

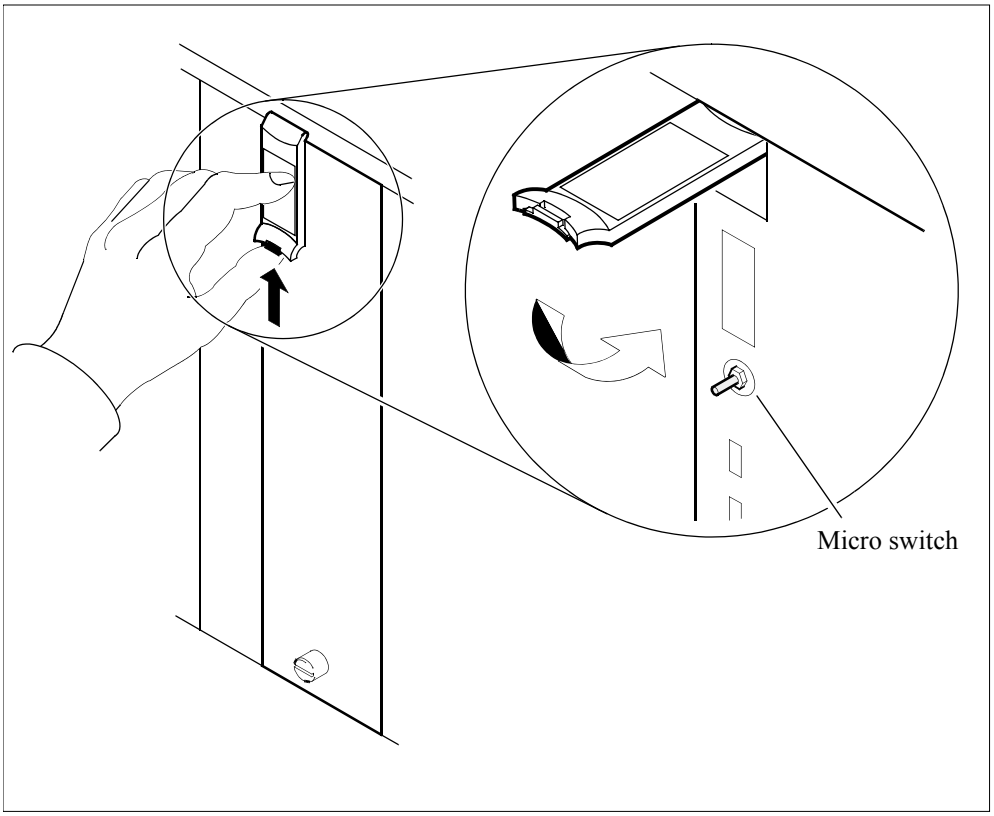
**2** Remove the filler plates covering the slots in which you will install the new modules.

**3** Insert the replacement module into the CS 2000 Core Manager shelf.

**4** Gently slide the module into the shelf until it is fully inserted.



**5** Close the locking lever to secure the module. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.




**6** Tighten the thumbscrews on the module.

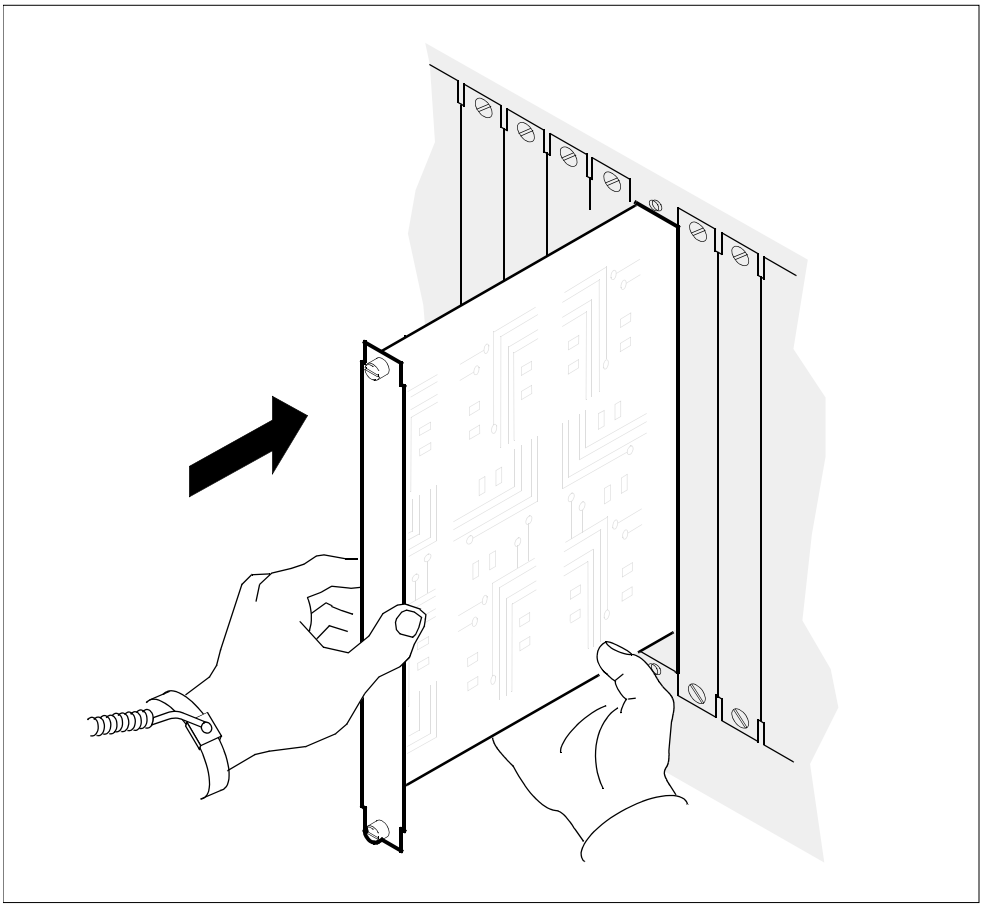
**7** Use the following table to determine your next step.

| If you | Do |
|---|---|
| need to install a LAN personality module | step 8 |
| do not need to install a LAN personality module | step 11 |

### *At the back of the CS 2000 Core Manager*

**8** Insert the new LAN personality module into the CS 2000 Core Manager shelf.

**9** Gently slide the LAN personality module into the shelf until it is fully inserted.



**10** Tighten the thumbscrews at the top and the bottom of the LAN personality module.

### *At the local or remote VT100 console*

**11** Log in to the CS 2000 Core Manager as the root user.

**12** Access the maintenance interface:

```
# sdmmtc
```

**13** Access the hardware (Hw) level:

```
> hw
```

**14** Add the logical pair of I/O controller modules:

**`> add <chassis> <slot> <pec>`**

*where*

***chassis***
is the chassis where the module will be located (“SDMM” for a main chassis or “SDME” for an I/O expansion chassis)

***slot***
is the lower of the two physical slot numbers the module occupies

***pec***
is the product engineering code (PEC) of the I/O controller module you want to add

***Note:*** This command adds both modules in the logical pair simultaneously. The command ‘>add <chassis> simplex <slot> <pec>’ adds one I/O controller module to domain 0.

**15** The ADD command may take several minutes to complete. When the command is finished, the following message is displayed:

*Response:*

```
Hardware Add Module - Command complete.
```

**16** Monitor the status of the new hardware at the hardware (Hw) level. The screen does not initially show the new hardware that has been added.

*Example response*:

```
          I F C E D 5 D X
          C A P T S 1 A 2
          M N U H K 2 T 5

Domain 0  . . . . . . . .
Domain 1  . . . . . . . .
```

The system takes a few seconds to display the appropriate new hardware elements (DSKn for hard disks). Previously installed disks on the system are automatically renumbered, as required, to reflect the new hardware configuration. The status of the new hardware elements may initially appear as “F” (failed).

*Example response*:

```
          I F C E D D D D 5
          C A P T S S S A 1
          M N U H K K K T 2
```

```
                  1 2 3
Domain 0 . . . . . F F . .
Domain 1 . . . . . F F . .
```

After a few seconds, the modules are automatically put in service, at which time their status changes to in-service (indicated by a dot).

*Example response*:

```
          I F C E D D D D 5
          C A P T S S S A 1
          M N U H K K K T 2
                  1 2 3
Domain 0 . . . . . . . . .
Domain 1 . . . . . . . . .
```

***Note:*** Devices have been renumbered. Use the Locate command to verify slot numbers.

**17** You have completed this procedure.

# Removing an I/O expansion chassis (NTRX50EC)

## Purpose

**ATTENTION**
Do not perform this procedure if there are any hardware faults on the CS 2000 Core Manager.

Use this procedure to remove an I/O expansion chassis (NTRX50EC) from an existing system.

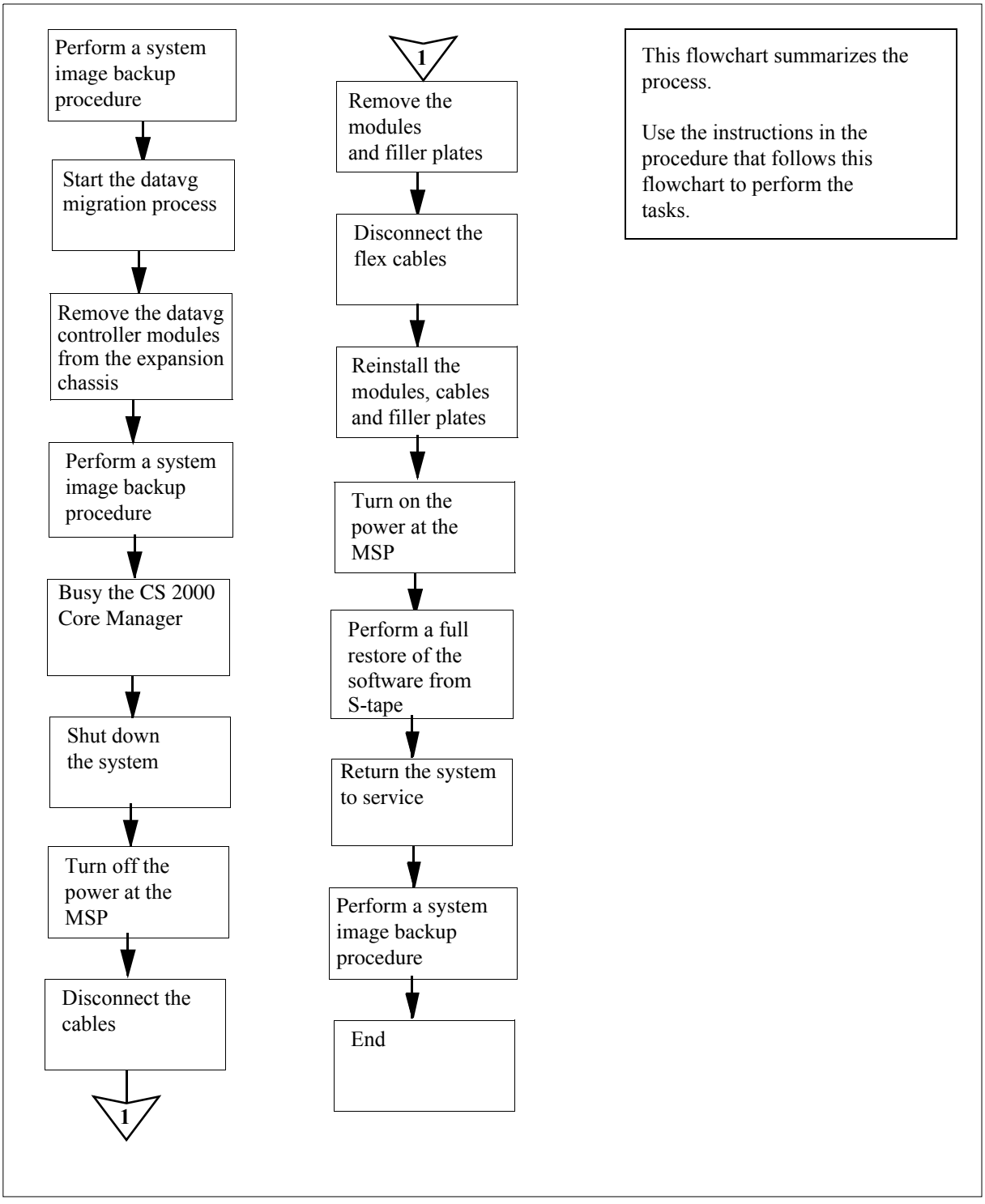
## Prerequisites

Make sure that your main chassis has been upgraded to the 36-Gbyte + 36-Gbyte Ultra-Multifunction Input/Output (UMFIO), before you start this procedure. Use the procedure Upgrading a datavg MFIO to MFIO or UMFIO on page 1497, if required.

## Task flow diagram

The following flowchart provides an overview of the process. Use the instructions in the procedure that follows the flowchart to perform the task.

## Task flow for removing an I/O expansion chassis (NTR50EC)



## Procedure

### Removing an I/O expansion chassis (NTRX50EC)

***At the local or remote VT100 console***

1 Perform a system image backup. Use the procedure “Creating system image backup tapes (S-tapes)” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

2 Exit the maintenance interface and return to the AIX command line:

```
> quit all
```

3 Check that no faults exist on the CS 2000 Core Manager:

```
# querysdm flt
```

| If | Do |
|---|---|
| faults are present | correct the faults using the procedures in the Fault Management document, and return to this procedure |
| no faults are present | step 4 |

4 Start the process of migrating datavg from the expansion chassis to the main chassis:

```
# ftmigratepv
```

The system performs several checks, listing them on the screen. If the system displays an error message, use the following table to determine your next step. If no error is displayed, continue with step 5.

| If the error message is: | Do |
|---|---|
| `You don't have physical volumes for datavg in expansion chassis` | go to step 18 |
| `There is insufficient free disk space on main chassis for migration` | contact your next level of support |

5 When prompted, confirm that you want to continue the data migration:

```
y
```

**6** Confirm again that you want to continue the data migration:

**y**

**7** The system continues the data migration process, listing all completed sub-processes, and then it prompts you to remove the datavg modules on the expansion chassis. The migration process takes approximately 30 minutes.

*Example response*

```
Please take out the datavg module in slot 1 on
the expansion chassis from the SDM. Please take
out the datavg module in slot 9 on the expansion
chassis from the SDM.
```

***At the front of the CS 2000 Core Manager***

**8** Remove the datavg controller modules from the expansion chassis slots indicated by the system.

**9**



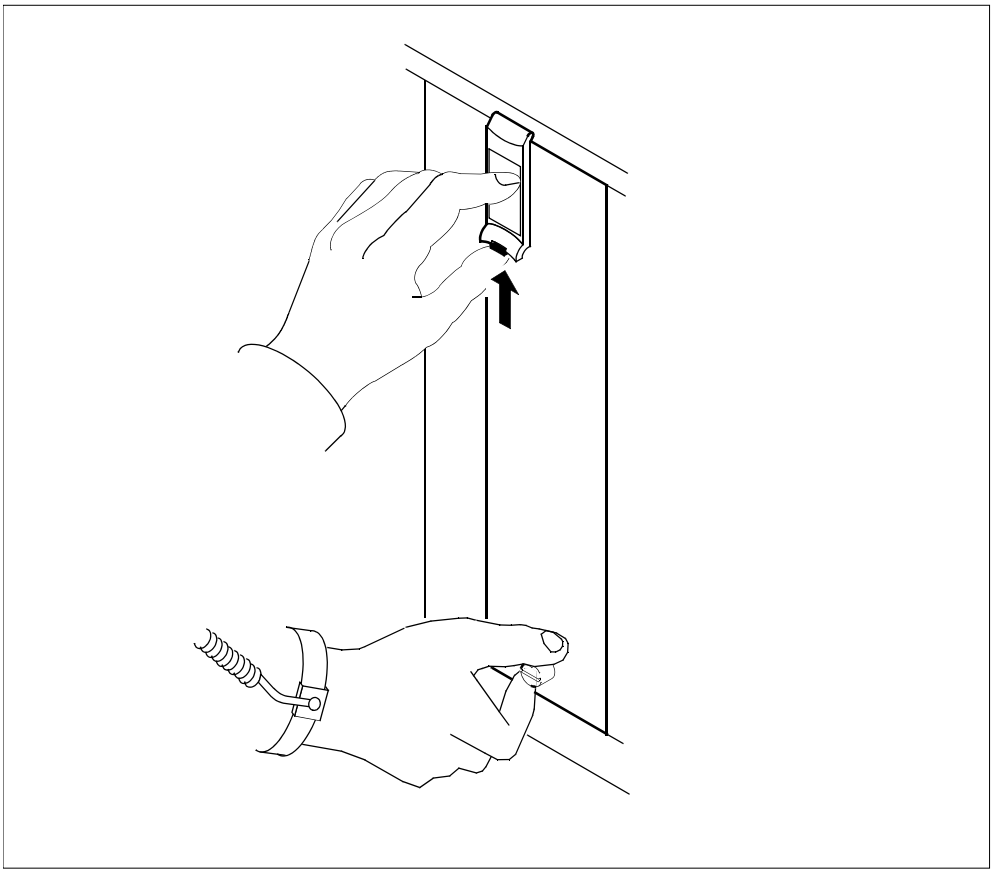
**WARNING**
**Static electricity damage**
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge grounding wrist strap.

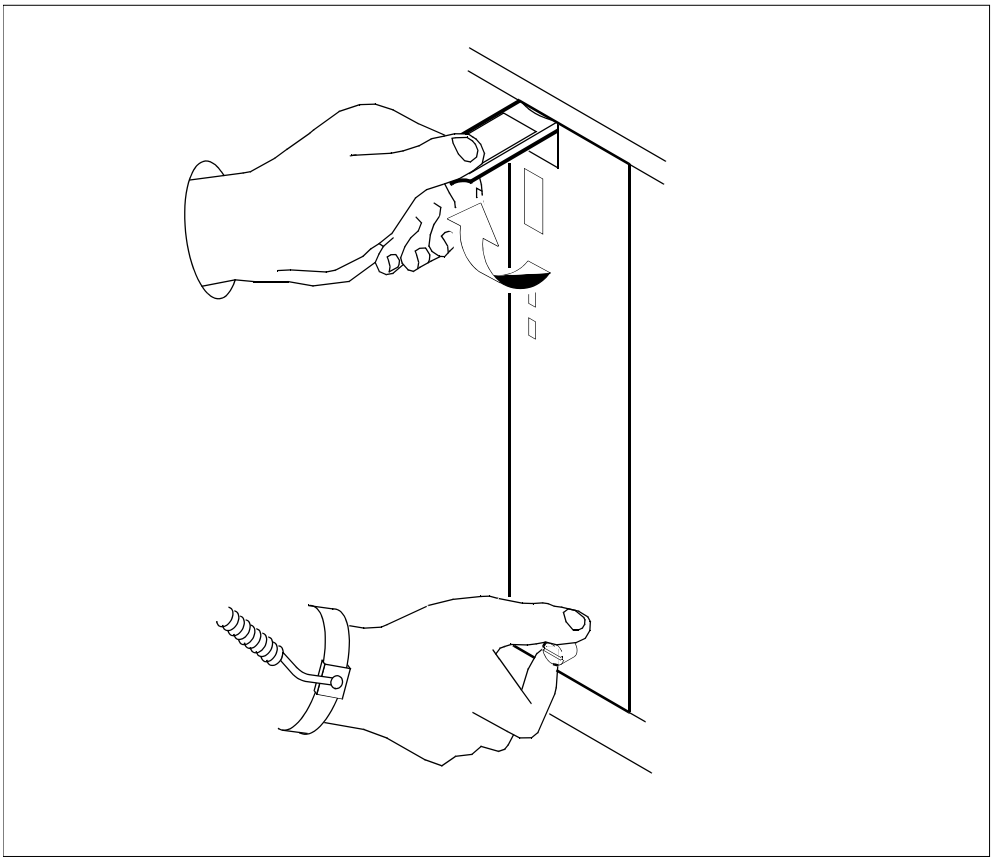
**10** Undo the thumbscrews located on the top and the bottom of the datavg controller module in domain 0.

***Note:*** The thumbscrews are the captive type, and cannot be removed from the module.

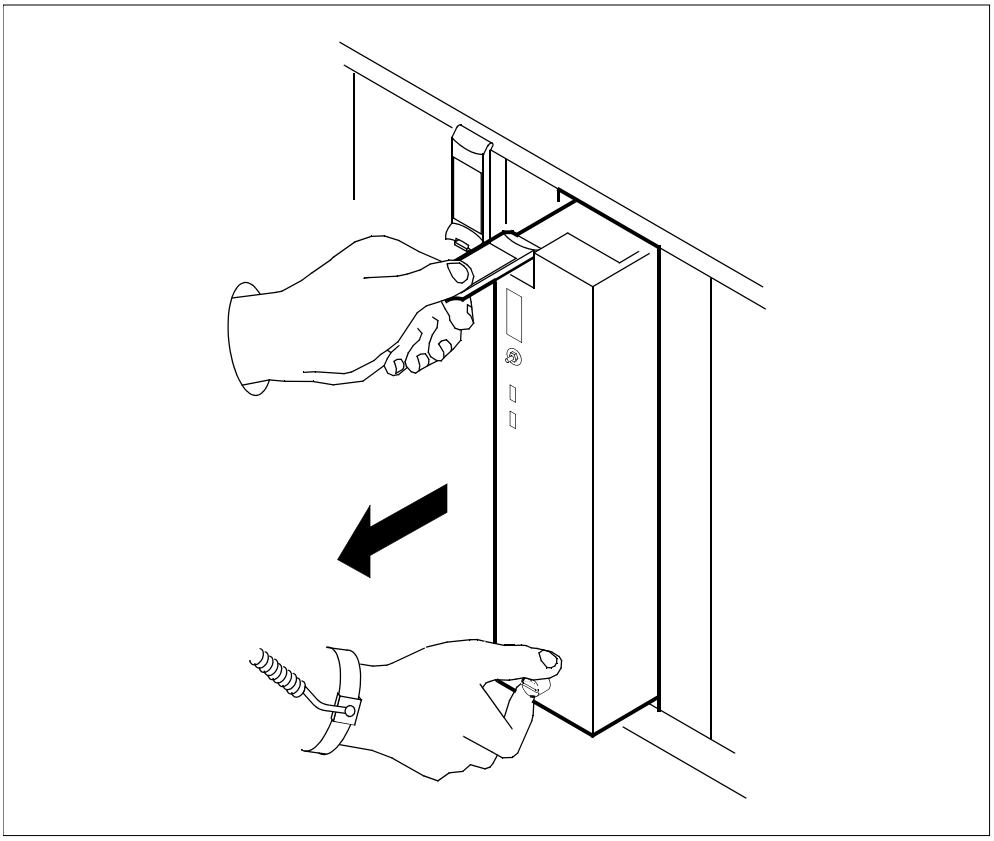
**11** Depress the tip of the locking lever on the face of the I/O controller module.



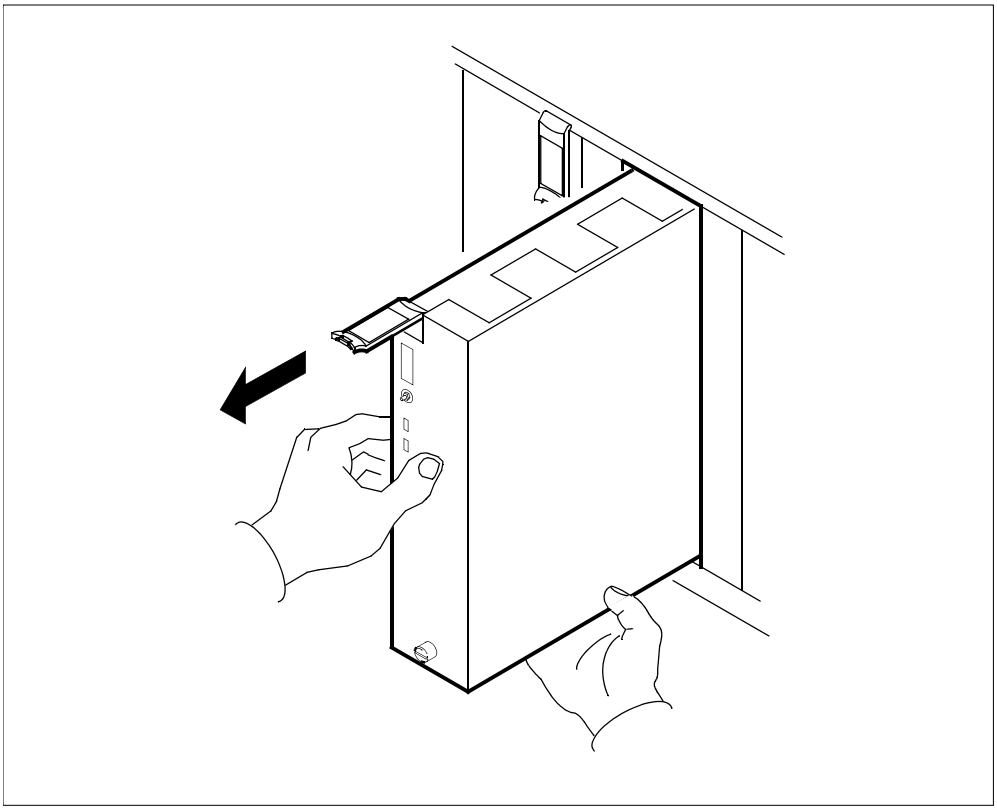
**12** Open the locking lever on the face of the module by moving the lever outwards.



**13** While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in (5 cm) from the CS 2000 Core Manager shelf.



**14** Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



**15** Place the module you have removed in an ESD protective container.

**16** Repeat steps 10 through 15 for the datavg controller module in domain 1.

### *At the VT100 console*

**17** When the data migration is completed, the system displays the following message:

```
Data on expansion chassis has been migrated to
main chassis with no error.
```

**18** Perform a system image backup. Use the procedure “Creating system image backup tapes (S-tapes)” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

***Note:*** During the backup procedure, you will be asked if you want to eject the S-tape from the drive. Enter **n** (no). Then, go back to the previous menu by typing **y**, and return to the admin

level by typing **0** (zero). Exit the maintenance interface by typing **quit all** and pressing the Enter key.

***At the MAP terminal***

**19** Access the SDM level of the MAP display:

```
> mapci;mtc;appl;sdm
```

**20** Busy the CS 2000 Core Manager:

```
> bsy
```

**21** Confirm the busy request:

```
> y
```

**22** Verify that each billing stream has entered the active backup mode by posting and querying each of your billing streams.

```
> sdmbil;post<stream>;query
```

***At the VT100 console***

**23** Disable the autoboot attribute for CPU 0 and CPU 1:

```
# autoboot -c 0 -o vb=n
# autoboot -c 2 -o vb=n
```

**24** Shut down the CS 2000 Core Manager:

```
# shutdown now
```

***At the modular supervisory panel (MSP)***

**25** Interrupt power to the CS 2000 Core Manager by turning off all four MSP breakers. The MSP breakers, located at the front of the MSP, supply power to the CS 2000 Core Manager.

***At the back of the CS 2000 Core Manager***

**26**

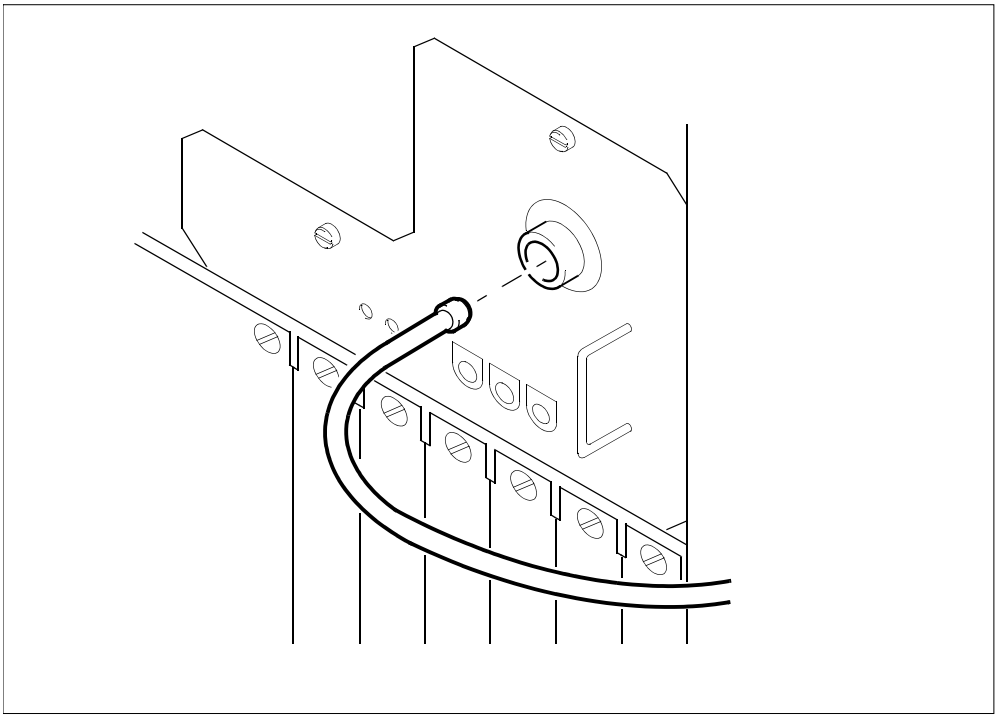


**WARNING**
**Static electricity damage**
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

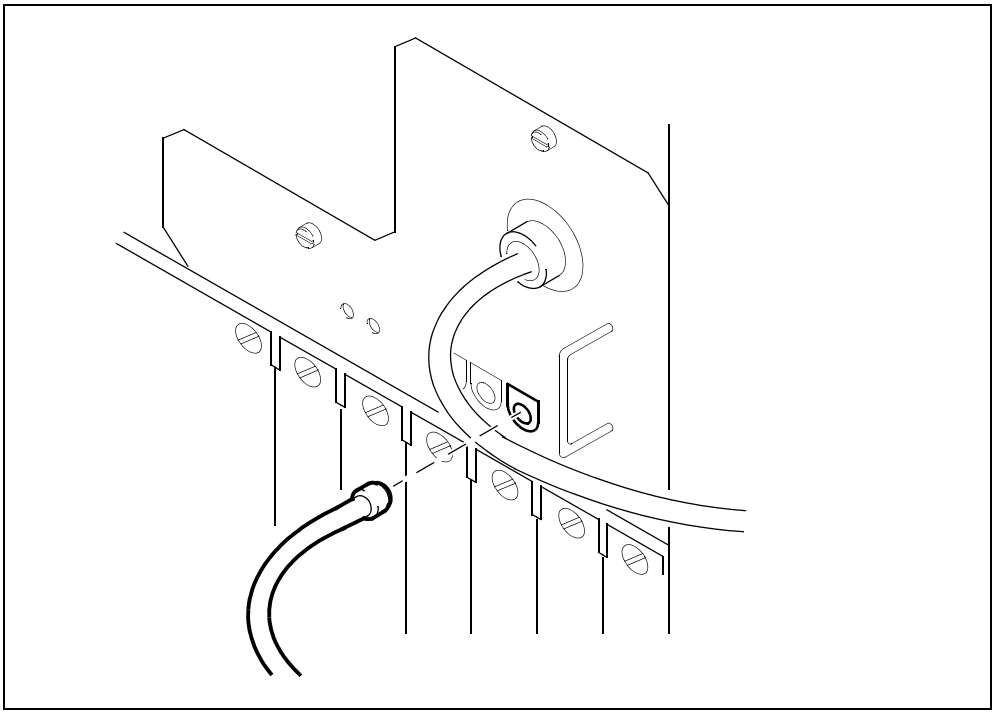
Put on an electrostatic discharge grounding wrist strap.

**27** Disconnect the power cables from the interconnect module (ICM) 0 and ICM 1 on both chassis.

***Note:*** Remove and store the power cables from the expansion chassis.



**28** If there are any alarm cables connected to the I/O expansion chassis, disconnect them.

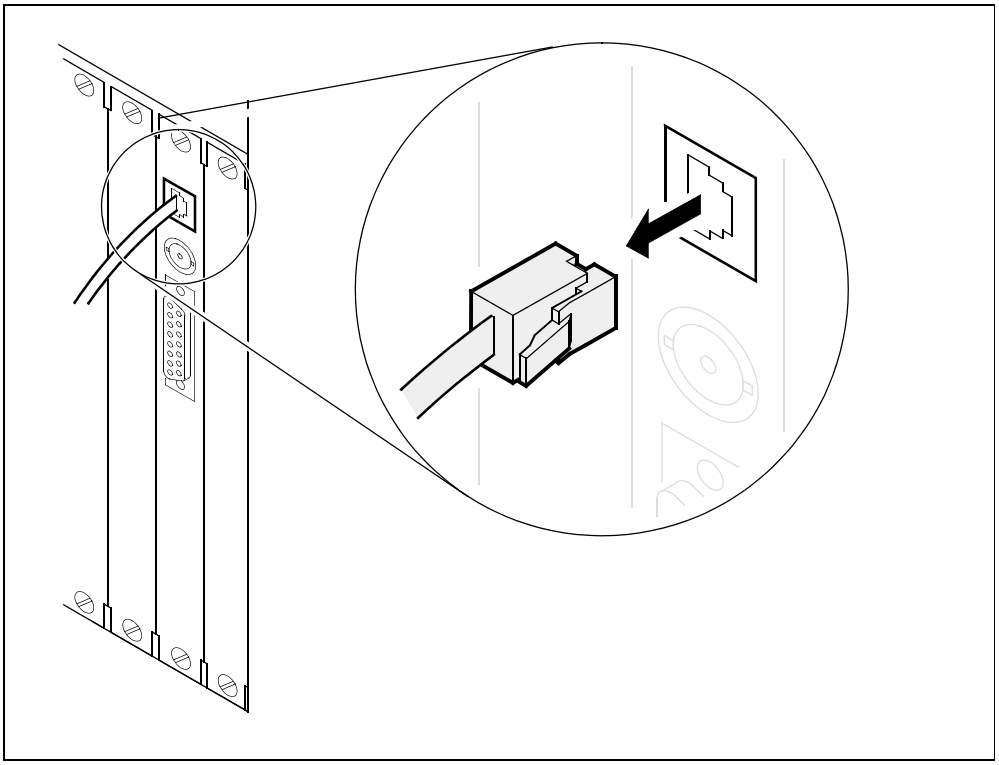


**29**

**CAUTION**
**Disconnecting transmit and receive cables**
Do not mix the transmit and receive cables for each domain. If you have not already done so, label these cables to ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Disconnect the four DS512 fiber cables from both DS512 personality modules (on the main shelf) by pressing the fiber cable in, and turning it a quarter-turn to the left.

**30** Disconnect the 10BASE-T cables from both LAN personality modules on the main shelf.



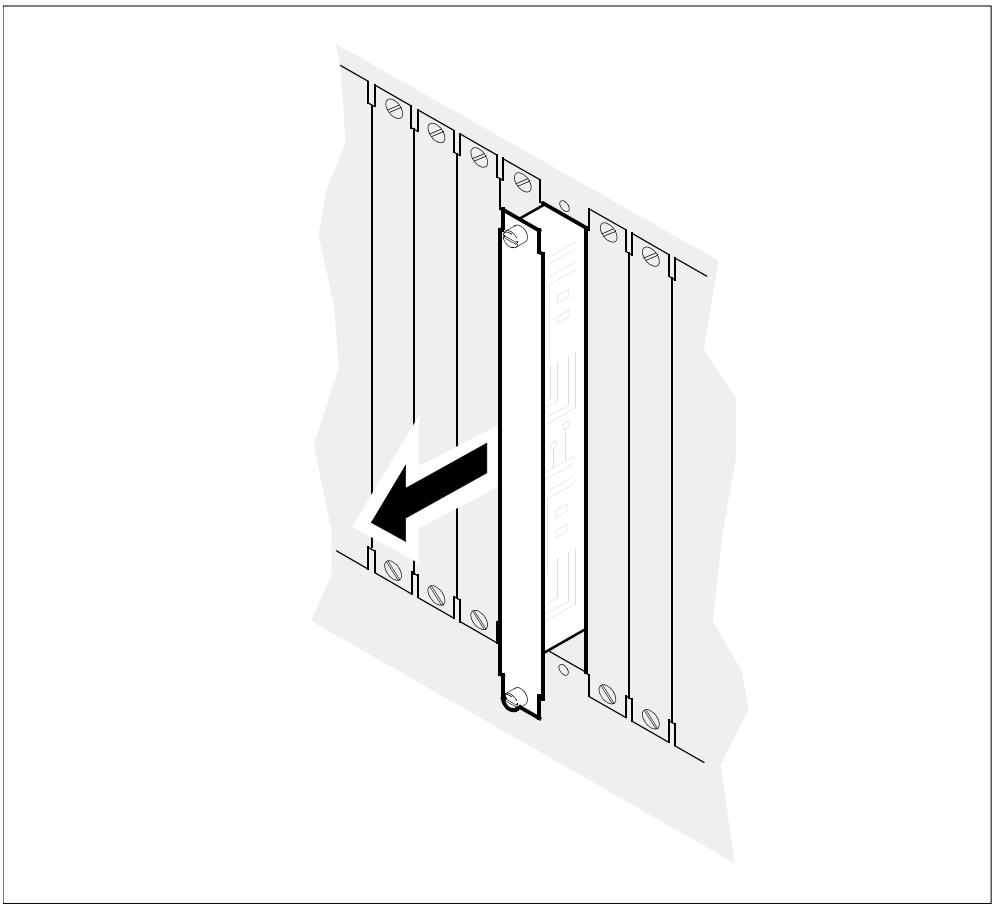
**31** To gain access to the flex cable, remove all personality modules and filler plates located in slots 1, 2, 3, 14, 15, and 16 on both chassis. Complete steps 32 through 34 for each personality module that you need to remove.

***Note:*** Record the slot number of each personality module and each filler plate that you are removing from the main shelf.

**32** Loosen the two thumbscrews located at the top and bottom of the personality module.

***Note:*** The thumbscrews are the captive type, and cannot be removed from the module.

**33** While grasping the thumbscrews, carefully pull the personality module out of the CS 2000 Core Manager shelf.



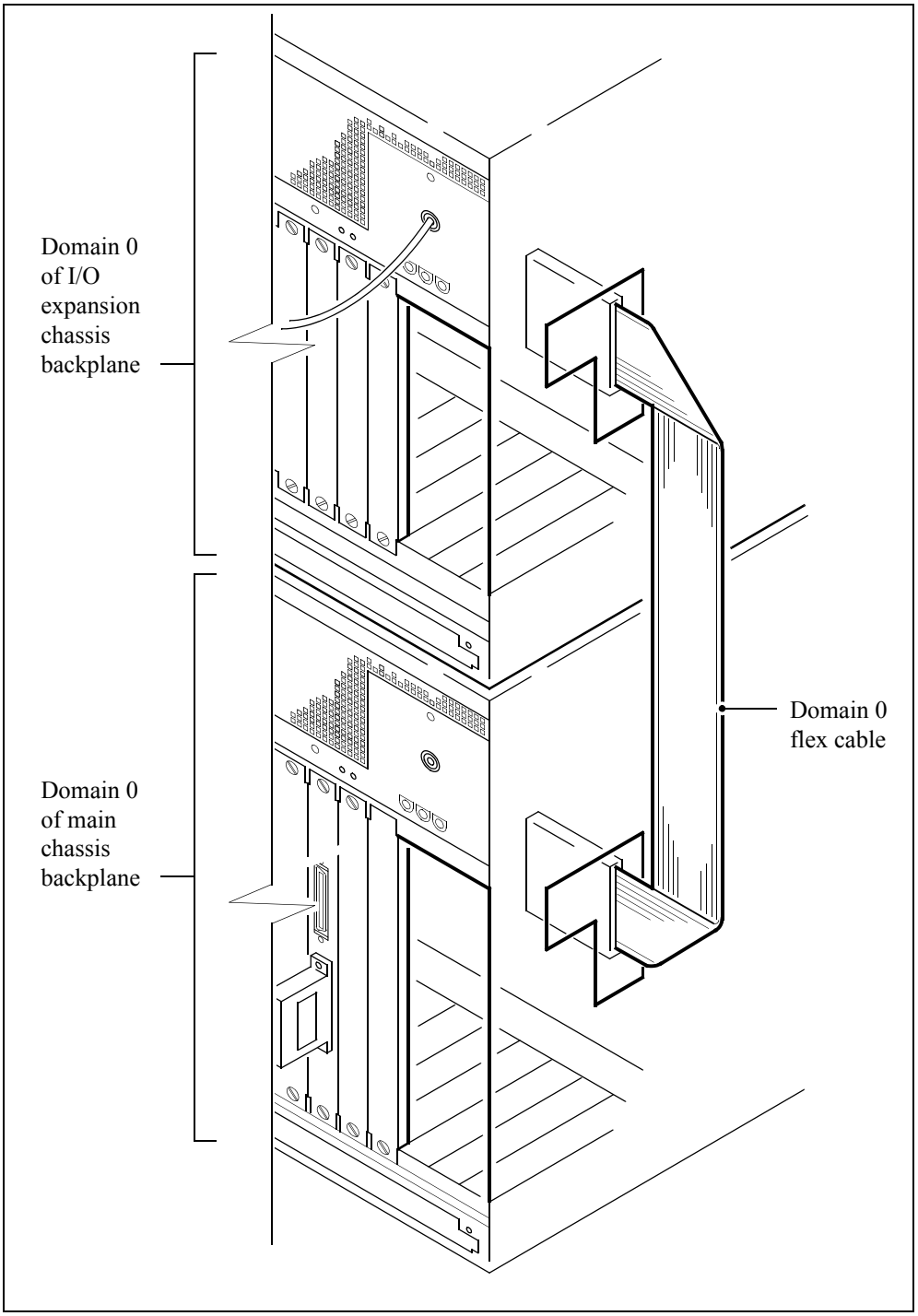
**34** Place the personality module you have removed in an ESD protective container.

**35** Remove the domain 0 and domain 1 flex covers that run from the outside of the main and I/O expansion chassis.

**36** Disconnect and remove the domain 0 flex cable (NTRX5088) from the I/O expansion chassis backplane side 0 and from the main chassis backplane side 0. Through the empty slots, reach the ends of the flex cable and pull them towards you. Once

disconnected from both chassis, remove the cable through the side opening.

Repeat the same operation on domain 1.



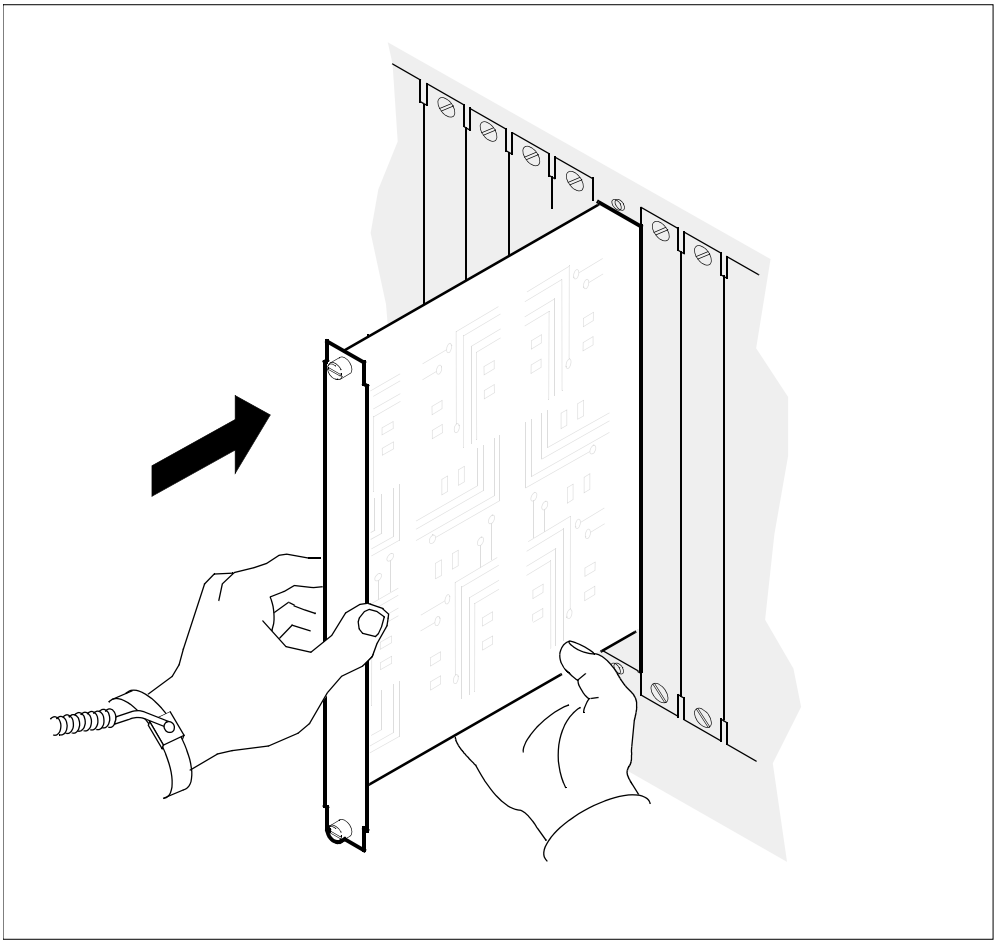
**37** Reinstall all personality modules and filler plates (on the main chassis only) that you removed in step 31.

***Note 1:*** Use your records from step 31 to make sure that you are placing each module in the same slot from which it was removed.

***Note 2:*** Reinstall all modules and filler plates in domain 0 first. Start from slot 2, and continue to the right. Repeat the same process on domain 1, starting from slot 16, and continuing to the left.

Complete steps 38 and 39 for each personality module that you need to reinstall.

**38** Carefully slide the personality module into the appropriate slot until it is fully inserted.



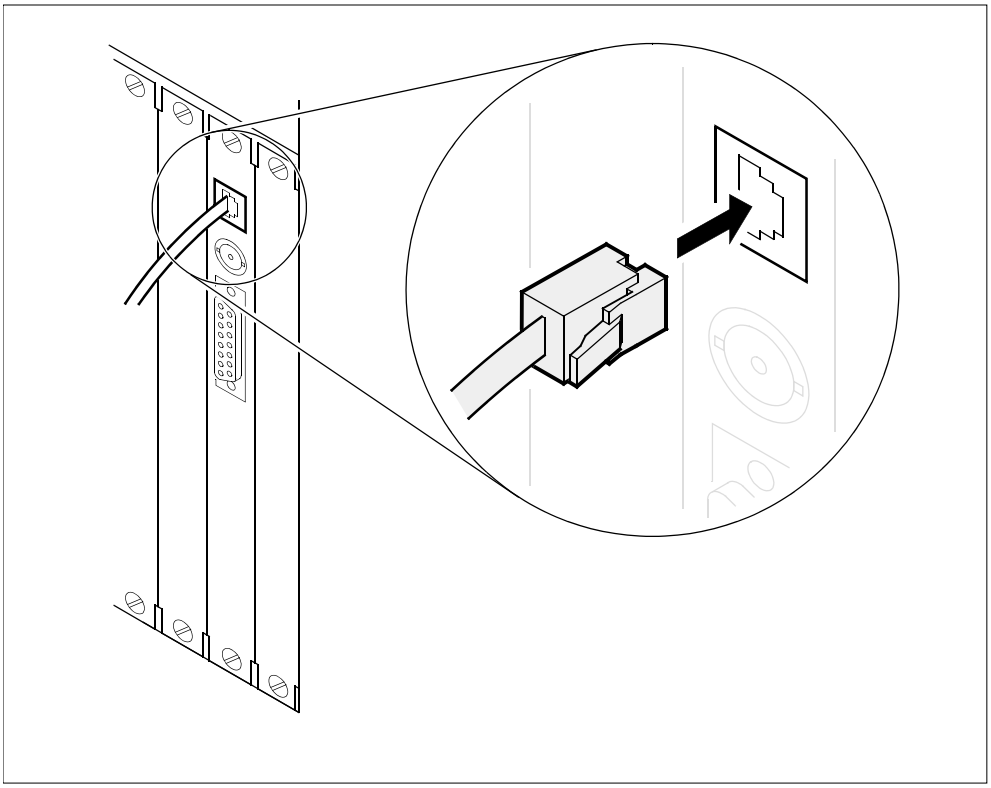
**39** Tighten the thumbscrews at the top and bottom of the personality module.

**40**

**CAUTION**
**Reconnecting transmit and receive cables**
Do not mix the transmit and receive cables for each domain. Ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Reconnect the four DS512 fiber cables on the DS512 personality module (on both domains) by pressing the fiber cable in, and turning it a quarter-turn to the right.

**41** Reconnect the 10BASE-T cable to the LAN personality module (on both domains).



**42** Reconnect the power cables to ICM 0 and ICM 1 in the main chassis.

***At the modular supervisory panel (MSP)***

**43** Restore power to the CS 2000 Core Manager by turning on the top two MSP breakers.

***At the VT100 console***

**44** Perform a full restore of the CS 2000 Core Manager software load from the system image backup tape (S-tape) that you created in step 18. Use the procedure “Performing a full restore of the software from S-tape” in the Fault Management document (starting with step 13).

***At the MAP terminal***

**45** Access the SDM level of the MAP display:

```
> mapci;mtc;appl;sdm
```

**46** Return the CS 2000 Core Manager to service:

```
> rts
```

***Note:*** It will take at least 5 minutes for the CS 2000 Core Manager to return to service on the Communication Server 2000 core side.

**47** Verify that the CS 2000 Core Manager status is InSv (in-service) or ISTb (in-service trouble).

**48** Verify that all billing stream are either in-service or in recovery by posting and querying each of your billing streams:

```
> sdmbil;post<stream>;query
```

***At the VT100 terminal***

**49** Enable the autoboot attribute for CPU 0 and CPU 1:

```
# autoboot -c 0 -o vb=y
```

```
# autoboot -c 2 -o vb=y
```

**50** Perform a system image backup. Use the procedure “Creating system image backup tapes (S-tapes)” in theSecurity and Administration document.

**51** You have completed this procedure.

# Installing and configuring the OM Data Delivery application

## Purpose

The OM Data Delivery application collects and stores operational measurement (OM) data from the switch. The application stores the data in comma separated value (CSV) files that are sent to the client operations support system (OSS).

The Tuple Number option allows you to activate or disable a tuple number so that it can be included in a CSV file with other OM information. You can activate or disable the Tuple Number option at the Config menu level on the CS 2000 Core Manager.

**ATTENTION**

You must busy (BSY) and return to service (RTS) the OM Data Delivery application for the Tuple Number option to be either activated or disabled.

## Prerequisites

If you are installing the OM Data Delivery application for the first time, ensure that the OM Access Service and Table Access Service application filesets are installed and in service on your CS 2000 Core Manager before executing this procedure.

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

## Procedures

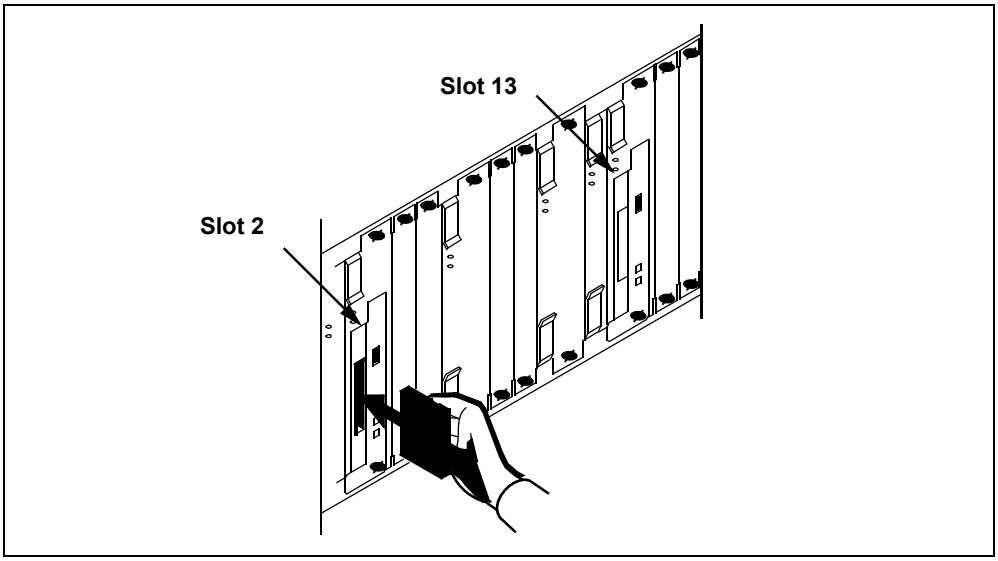
### Installing the OM Data Delivery application

***At the CS 2000 Core Manager***

**1** Insert tape CS2E00007 NCL 7.x (1 of 1) into one of the tape drives (slot 2 or slot 13) of the main chassis, as shown in the following figure.

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

**Tape drive in main chassis**




***At the maintenance interface***

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

| If you choose to install OM Data Delivery by | Do |
|---|---|
| logging onto a local VT100 terminal connected to the CS 2000 Core Manager | log on to the CS 2000 Core Manager as root user at the VT-100 terminal, and go to step 6 |
| using telnet from a remote UNIX workstation to the CS 2000 Core Manager | step 3 |

**3** Open a terminal window that is VT-100 compatible at the remote UNIX workstation.

***Note:*** To install the OM Data Delivery application using a remote UNIX workstation, verify that telnet is enabled on the CS 2000 Core Manager.

**4** Log onto the CS 2000 Core Manager from the terminal window prompt:

```
telnet <ip_address>
```

*where*

<ip_address> is the IP address of the CS 2000 Core Manager you want to install the OM Data Delivery application on.

**5** When prompted, enter the login ID and password for the root user.

**6** Access the maintenance interface level:

```
# sdmmtc
```

**7** Access the software inventory manager (SWIM) level:

```
> swim
```

The CS 2000 Core Manager lists the software applications currently installed.

**8** List the contents of the tape you previously inserted:

```
> apply <n>
```

*where*

**<n>**
is either 0 (slot 2) or 1 (slot 13).

**9** Locate the OM Data Delivery application fileset.

***Note 1:*** If necessary, use the up (type 12, u, or up) and down (type 13, d, or down) commands to locate the OM Data Delivery application fileset.

***Note 2:*** If you have a previous release of the OM Data Delivery application installed, its release number appears in the *Current* column, while the new version you are installing appears in the *Available* column.

**10** Select and install the new OM Data Delivery application fileset:

```
> apply <n>
```

*where*

**<n>**
is the number next to the OM Data Delivery application fileset.

Response:

```
You have selected to install the following new
filesets or fileset updates.OM Delivery
Application 19.0.xx.0. Do you wish to proceed?
Please confirm ("YES", "Y", "NO", or "N"):
```

**11** Confirm the apply command:

```
> y
```

Response:

```
Command in progress.
```

```
APPLYING fileset: 9
SDM_OMDD.OMD 19.0.XX.0
```

### Configuring the OM Data Delivery application

***At the CS 2000 Core Manager console***

**1** Access the Config menu:

```
# sdmmtc config
```

**2** Configure OM Data Delivery:

```
> config <n>
```

*where*

**<n>**
is the number next to OM Data Delivery under fileset description

Use the following table to determine your next step.

| If OM Data Delivery | Do |
|---|---|
| is being initially installed or upgraded to CS2E0070 | step 3 |
| has already been installed and is currently active | step 4 |
| has already been installed and is currently disabled | step 5 |

**3** The system indicates that the Tuple Number option is undefined.

*Example response:*

```
The Tuple number inclusion option is currently
  undefined.
Do you want the Tuple number to be provided with the
  OM Group information (Y/N) [N]?
```

***Note:*** For fresh installations or upgrades from releases prior to CS2E0070, the default value is *disabled (N)*.

| If you | Do |
|---|---|
| activate the Tuple Number option | type **y**, press the Enter key, and go to step 6 |
| do not want to activate the Tuple Number option | press the Enter key, and go to step 6 |

**4** The system indicates that the Tuple Number option is active.

*Example response:*

```
The Tuple number inclusion option is currently
  active.
Do you want the Tuple number to be provided with the
  OM Group information (Y/N) [Y]?
```

| If you | Do |
|---|---|
| want to disable the Tuple Number option | type **n**, press the Enter key, and go to step 6 |
| do not want to disable the Tuple Number option | press the Enter key, and go to step 6 |

**5** The system indicates that the Tuple Number option is disabled.

*Example response:*

```
The Tuple number inclusion option is currently
  disabled.
Do you want the Tuple number to be provided with the
  OM Group information (Y/N) [N]?
```

| If you | Do |
|---|---|
| want to activate the Tuple Number option | type **y**, press the Enter key, and go to step 6 |
| do not want to activate the Tuple Number option | press the Enter key, and go to step 6 |

**6** The system prompts you to confirm whether the MDM and SDM are integrated.

*Example response:*

```
Are the MDM and SDM integrated [Y|N]?
```

**7** When prompted, confirm the MDM and SDM are integrated:

**y**

and pressing the Enter key.

**8** Configure the CS 2000 Core Manager to communicate with the Preside MDM as follows:

**a** When prompted, enter the IP address of the first MDM, and press the Enter key.

**b** When prompted, enter the hostname of the first MDM, and press the Enter key.

**c** When prompted, enter the IP address of the second MDM, and press the Enter key.

**d** When prompted, enter the hostname of the second MDM, and press the Enter key.

**e** When prompted, enter the port for 5-minute PM data, and press the Enter key.

**f** When prompted, enter the port for 30-minute PM data, and press the Enter key.

**9** When prompted, indicate whether you want to use custom retry settings.

| If you | Do |
|---|---|
| do not want to use custom retry settings | type **n**, press the Enter key, and go to step 11 |
| want to use custom retry settings | type **y**, press the Enter key, and continue with step 10 |

**10** Respond to the prompts with your custom retry settings and press the enter key after each entry:

***Note:*** The retry setting values shown here are examples. Retry setting values are in seconds (values higher than 300 seconds are not recommended as they may adversely affect recovery time).

```
> Enter the first connection retry interval: 2

> Enter the number of retry attempts at that
interval: 10

> Enter the second connection retry interval: 10

> Enter the number of retry attempts at that
interval: 40

> Enter the third connection retry interval: 60
```

**11** When prompted, confirm the data:

```
> y
```

**12** Refer to the following table to determine your next step.

| If the OM Data Delivery application | Do |
|---|---|
| is ManB or Offl | step 13 |

| If the OM Data Delivery application | Do |
|---|---|
| is in any state *other* than ManB or Offl | step 14 |

**13** The system indicates that the configuration is complete.

*Response:*

```
Configuration complete. Please press Enter . . .
```

Press the Enter key, and go to step 15.

**14** The system indicates that the changes will take place after the OM Data Delivery application is restarted.

*Response:*

```
Changes will take effect after OM Delivery is restarted.
Configuration complete. Please press Enter . . .
```

Press the Enter key, and go to step 15.

**15** Exit the CS 2000 Core Manager maintenance interface:

```
> quit all
```

**16** You have completed this procedure.

# Installing or upgrading DDMS

Use this procedure to install and configure DDMS for the first time, which consists of Creating user IDs on the CM and Installing or upgrading DDMS filesets.

> ***Note:*** The following mandatory user IDs created on the CM must also be added when you configure DDMS: SDM01, SDM02, SDM03, SDM04. These user IDs are mandatory on the CM and DDMS.

If Enhanced Password Control is in effect on the CM, the DDMS software will manage automatic password changing on the CM before the passwords expire. You therefore do not have to manually change the passwords for users SDM01-SDM04 on the CM.

When DDMS software is returned to service (RTSd), it reads the ofpcopt and ofceng tables on the CM to determine whether Enhanced Password Control is in effect. If Enhanced Password Control is in effect, the software will read the password lifetime value and automatically change passwords one day before expiry. If you make manual changes to the password lifetime value or turn on/off Enhanced Password control, then these changes must be synchronized with the DDMS software by busying/returning to service (bsy/rts) the DDMS. However, if any of the SDM01-SDM04 passwords are changed on the CM manually, you need to apply the same password changes in the DDMS configuration file. Refer to Changing passwords in the DDMS configuration file.

Also use this procedure to upgrade DDMS prior to a CM one night process (ONP), which consists of Installing or upgrading DDMS filesets.

> ***Note:*** The DDMS application must be stopped before the CM Swact. Refer to procedure “Controlling SDM applications” in the Security and Administration section to stop DDMS. When the CM ONP is complete, restart DDMS using the same procedure.

Ensure you meet all the prerequisites listed below prior to installing or upgrading DDMS.

## Prerequisites for DDMS installation

Following are the prerequisites for a successful DDMS installation:

- Hardware requirements
  - CS 2000 Core Manager Fault Tolerant (FT) Platform
  - VT100 terminal
- Software requirements
  - Installed CS 2000 Core Manager base software including the OM access and table access applications, and the filesets associated with the log delivery application (refer to procedure “Installing and configuring the log delivery application” in the Configuration section).
  - The Log Delivery Service application must be in service.
- User privilege requirements
  - root access to the CS 2000 Core Manager
  - maintenance (maint) access to the CS 2000 Core Manager
  - execute access to ftp on the CS 2000 Core Manager

## Creating user IDs on the CM

The CS 2000 Core Manager requires you to create at least four user IDs on the CM.

### Creating user IDs on the CM

***At the CI prompt on the switch***

**1** Type each of the following commands and press Enter after each:

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

Where

**<sdm0n_pswd>**
is the CM password for user SDM0n

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

***Note 2:*** If Enhanced Password Control is in effect on the CM, and any of the SDM01-SDM04 passwords are changed on the CM, you need to apply the same password changes in the

DDMS configuration file. Refer to Changing passwords in the DDMS configuration file.

2 You have completed this procedure.

### Changing passwords in the DDMS configuration file

#### *At the CS 2000 Core Manager*

1 Log in to the CS 2000 Core Manager as the root user.

2 Access the maintenance interface by typing

```
# sdmmtc
```

and pressing the Enter key.

3 Access the application level by typing

```
> appl
```

and pressing the Enter key.

4 Locate and busy the OSS Comms Svcs application by typing

```
> bsy <n>
```

and pressing the Enter key.

**<n>**
is the number next to the OSS Comms Svcs fileset

5 Change the passwords in the DDMS configuration file as follows:

**a** Access the configuration level by typing

```
> config <n>
```

and pressing the Enter key.

**<n>**
is the number next to the OSS Comms Svcs fileset

**b** Perform steps 8 through 12 in Installing or upgrading DDMS filesets, which follows.

**c** Once you have completed the configuration, return the OSS Comms Svcs application to service by typing

```
> rts <n>
```

and pressing the Enter key.

**<n>**
is the number next to the OSS Comms Svcs fileset

6 You have completed this procedure.

# Installing DDMS filesets

The DDMS software is located in filesets on the CS 2000 Core Manager non-CM load (NCL) digital audio tape (DAT). The following table shows the names, descriptions and contents of the DDMS filesets. These filesets are automatically installed when the schema fileset appropriate for your switch is installed.

**DDMS contents of CS 2000 Core Manager NCL DAT tape**

| Fileset name | Fileset description | Contents |
|---|---|---|
| SDM_DDMS.ossaps | OSS and Application Svcs | OSSAPS<br>Transaction Manager (ddmstxmgr)<br>View Server (ddmsschema)<br>Data Input Handler (ddmsdih)<br>Data Change Notification Handler (ddmsdcnh)<br>Synchronizing Interface Module (ddmssimif) |
| SDM_DDMS.osscomms | OSS Comms Svcs | OSSCOMMS<br>Communications Manager (ddmscomms)<br>Passthru Interface Manager (ddmspim)<br>User Administration (ddmsuAdmin)<br>System Administration (ddmssysadm |

## Installing or upgrading DDMS filesets

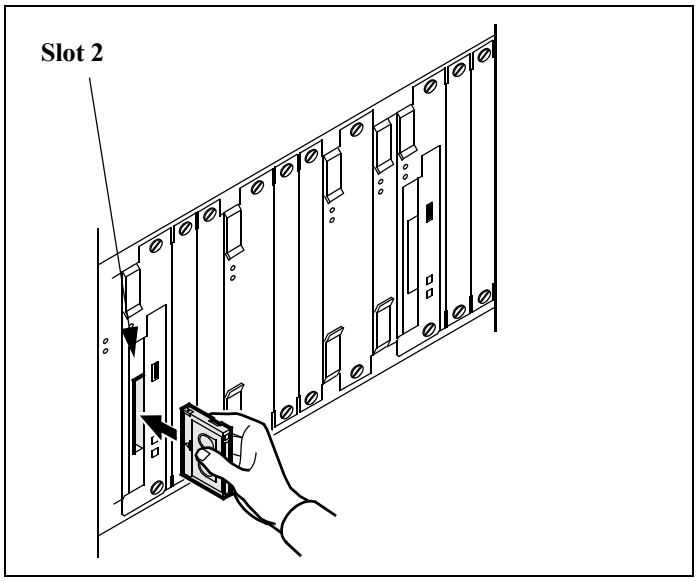
### *At the CS 2000 Core Manager*

**1** Log in to the CS 2000 Core Manager as the root user.

2 Use the following table to determine your next step.

| If the software is | Do |
|---|---|
| on tape | insert the tape labeled CS2E0070 7.x (1 of 1) into the tape drive in slot 2 as shown in the following figure, and continue with step 3<br>***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed. |
| in a directory | step 3 |

**Main chassis tape drive**




3 Access the maintenance interface by typing

```
# sdmmtc
```

and pressing Enter.

4 Use the following table to determine your next step.

| If the software is | Do |
|---|---|
| on tape | list the filesets by typing apply 0 and pressing the Enter key |
| in a directory | list the filesets by typing apply <directory path> and pressing the Enter key. |

5 Select the filesets to install or upgrade by typing

**> select <x>**

and pressing the Enter key.

Where

**<x>**
is the number next to the following filesets

- OSS Comms Svcs
- OSS and Application Svcs

Your selections are now highlighted.

6 Apply the selected filesets by typing

**> apply**

and pressing the Enter key.

The list of required filesets is displayed.

**> y**

and press the Enter key.

7 Confirm the Apply command by typing

**> y**

and pressing the Enter key.

Response:

```
Command in progress, 2 filesets to process.
Processing fileset 1
Applying OSS Comms Svcs 17.x.x.x
```

***Note:*** This can take up to 10 minutes to complete.

8 Press Enter to begin configuration of the OSS and Application Svcs, and the OSS Comms Svc filesets.

9 When prompted to enter the logroute tool, as shown in table DDMS logroute tool banner, press Enter.

The Logroute Main Menu appears, as shown in figure Logroute tool main menu.

**DDMS logroute tool banner**

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

**Logroute tool main menu**

```
                    Logroute Main Menu


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




Enter Option    ==>
```

**10** Set up a path and file to store DDMS customer logs as follows:

**a** Select the Device List menu by typing

```
> 1
```

and pressing the Enter key.

The Device List Menu screen is displayed.

| If the list | Do |
|---|---|
| includes device /data/logs/ossaps/ossapslog | sub-step l |
| does not include device /data/logs/ossaps/ossapslog | sub-step b |

**b** Begin to add a new device by typing

```
> 2
```

and pressing the Enter key.

**c** Select a file device by typing

```
> 3
```

and pressing the Enter key.

*Response:*

```
Enter file name ==> /data/logs/
```

**d** Complete the path name by typing

```
ossaps/ossapslog
```

and pressing the Enter key.

You have now set up the log routing for the DDMS.

**e** When prompted, enter the log format (from the range displayed), and press the Enter key.

***Note 1:*** Enter STD or SCC2 if you want the following information to be displayed in all log reports (otherwise, enter STD_OLD or SCC2_OLD):

- user-defined office ID, same for all logs and streams
- the name of the node (ECORE) from which the log is generated
- the sequence number in dual (global and device) format

***Note 2:*** The default format is STD.

**f** When prompted, set the ECORE option to ON or OFF, and press the Enter key.

***Note:*** Enter ON, if you want the log-generating node name to be displayed in all reports (the format must be STD or SCC2). Otherwise, enter OFF.

**g** Select addrep by typing

```
> a
```

and pressing the Enter key.

**h** Enter the log identifier by typing (in uppercase)

```
> DDMS
```

and pressing the Enter key.

**i** Save the new device by typing

```
> y
```

and pressing the Enter key.

Response:

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

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

**j** Return to the Device List Menu screen by typing

```
> 5
```

and pressing the Enter key.

**k** Return to the Device List Menu screen by typing

```
> 6
```

and pressing the Enter key.

**l** Exit logroute by typing

```
> 6
```

and pressing the Enter key.

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

The required CM users, SDM01-SDM04, for DDMS will be added to the DDMS configuration file. The passwords for these users should be the same as those entered in Creating user IDs on the CM in this procedure, during the NCL installation.

***Note:*** The userIDs and passwords are not case sensitive

**Example of DDMS CM user setup screen**

```
CM User Setup

0. QUIT
1. Add user
2. Delete user(by ID)
3. Update passwd(by ID)
4. Display users(ID)

Enter choice:
```

**11** Follow sub-steps a through c for each of the required userIDs:

**a** Add a new user by typing

```
> 1
```

and pressing the Enter key.

**b** When prompted, enter the user name (i.e. sdm01) and press Enter.

**c** When prompted enter the user password and press Enter.

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

**d** Exit the CM User Setup screen by typing

```
> 0
```

and pressing the Enter key.

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

**Example of DDMS Clients Configuration screen**

```
DDMS Clients Configuration

0. Quit
1. Add new clients
2. Remove existing clients
3. List existing clients

Enter choice:
```

**12** Follow sub-steps a through c to configure the DDMS clients.

***Note:*** The DDMS clients are the CS 2000 Management tools servers with the SESM load.

**a** Add a new client by typing

```
> 1
```

and pressing the Enter key.

**b** When prompted, enter the IP address for each of the CS 2000 Management tools servers. Press the Enter key after each entry and type “done” once you have entered all the IP addresses.

**c** Exit the DDMS clients configuration screen by typing

```
> 0
```

and pressing the Enter key.

**13** You have completed this procedure

# Installing or upgrading the GR740 TCP/IP Pass Through application

## Purpose

Use this procedure to install or upgrade the GR740 TCP/IP Pass Through application on the CS 2000 Core Manager.

## Prerequisites

To ensure a successful GR740 TCP/IP Pass Through operation:

- Ensure that the Distributed Computing Environment (DCE) is installed and configured, if you want to use the GR740 TCP/IP Pass Through application in secure mode.
- Ensure that the settings for office parameters “eadas_dc_interface” and “eadas_nm_interface” in table OFCVAR, and the settings for the EADAS SOCs (OAM00005 and OAM00006) are correct for your configuration.
- Ensure that OAM00004 for EADAS/DC is ON and that office parameters “eadas_mpc_and_link” and “netminder_mpc_and_link” are appropriately datafilled in table OFCVAR when BX25 connectivity is required.

The following table lists the supported configurations for EADAS GR740 TCP/IP.

**CM EADAS TCP/IP configurations**

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

The following table lists the channel assignments for EADAS. Note that DC EADAS channels 1, 2 and 3 support TR-740/746 compliant header and message. NM EADAS channels 1, 2 and 3 support SR3942 and TR746 to Netminder.

**EADAS channel assignments**

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

## Procedure

### Installing the GR740 TCP/IP Pass Through application

***At the CS 2000 Core Manager***

1 Log in to the CS 2000 Core Manager as the root user.

2 Use the following table to determine your next step.

| If the NCL filesets are | Do |
|---|---|
| on tape | insert the CS2E0070 7.x (1 of 1) tape in slot 2 of the tape drive, and continue with step 3<br>***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed. |
| in a directory | step 3 |

3 Access the maintenance interface:

```
# sdmmtc
```

The CS 2000 Core Manager maintenance menu appears, with menu selections highlighted in the left column.

4 Use the following table to determine your next step.

| If the NCL filesets are | Do |
|---|---|
| on tape | list the filesets: **> apply 0** |
| in a directory | list the filesets: **> apply <directory path>** |

5 Select the GR740 fileset:

**> select <x>**

*where*

**x** is the number next to the GR740 TCP/IP Pass Through fileset

6 Apply the GR740 fileset:

**> apply**

7 Confirm the **apply** command:

**> y**

*Response*

```
GR740 Pass Through Installation

Command in Progress, x filesets to process.
Processing fileset x.

APPLYING GR740 Pass Through xx.xx.xx.xx

Since the following filesets were applied to the system
for the first time, their configuration programs will
now be executed.
```

8 Press Enter to begin configuration.

| If | Do |
|---|---|
| you are not configuring GR740 TCP/IP Pass Through in secure mode | enter **n** |
| you are configuring GR740 TCP/IP Pass Through in secure mode | enter **y** |

The system displays a response indicating successful installation.

9 You have completed this procedure.

# Installing or upgrading Reach Through SPM

## Purpose

This procedure provides instructions on how to install or upgrade the Reach Through SPM application on the CS 2000 Core Manager.

## Procedure

### Installing Reach Through SPM

***At the CS 2000 Core Manager***

**1** Log on to the CS 2000 Core Manager as the root user.

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

| If the software is | Do |
|---|---|
| on tape | insert the CS2E0070 7.x (1 of 1) tape into slot 2 of the tape drive, and go to step 3<br>***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed. |
| in a directory | step 3 |

**3** Access the maintenance interface:

```
# sdmmtc
```

**4** Use the following table to determine your next step.

| If the software is | Do |
|---|---|
| on tape | list the filesets: **`apply 0`** |
| in a directory | list the filesets: **`apply <directory path>`** |

**5** Select the Reach Through SPM fileset:

```
> select <n>
```

*where*

<n> is the number next to the Remote Registration System fileset.

**6** Apply the selected fileset:

```
> apply
```

7 Confirm the apply command:

```
> y
```

8 You have completed this procedure.

# Installing or upgrading OpenSSH

## Purpose

The following procedure provides instructions on how to install the OpenSSH fileset. For more information on OpenSSH, refer to "OpenSSH overview" in the Basics document.

## Procedure

***At the CS 2000 Core Manager***

1 Log on to the CS 2000 Core Manager using the root user ID and password.

2 Use the following table to determine your next step.

| If the software is | Do |
|---|---|
| on tape | insert the tape labeled CS2E0070 7.x (1 of 1) into the tape drive in slot 2, and continue with step 3<br>***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed. |
| in a directory | step 3 |

3 Access the maintenance interface:

```
# sdmmtc
```

4 Use the following table to determine your next step.

| If the software is | Do |
|---|---|
| on tape | list the filesets: **`apply 0`** |
| in a directory | list the filesets: **`apply <directory path>`** |

5 Select the latest version of the OpenSSH fileset:

```
> select <x>
```

*where*

<x> is the number next to the OpenSSH fileset.

6 Apply the selected fileset:

```
> apply
```

7 Confirm the apply command:

```
> y
```

8 You have completed this procedure.

# Removing CS 2000 Core Manager application filesets

## Purpose

This procedure provides instructions on how to remove application filesets that reside on the CS 2000 Core Manager.

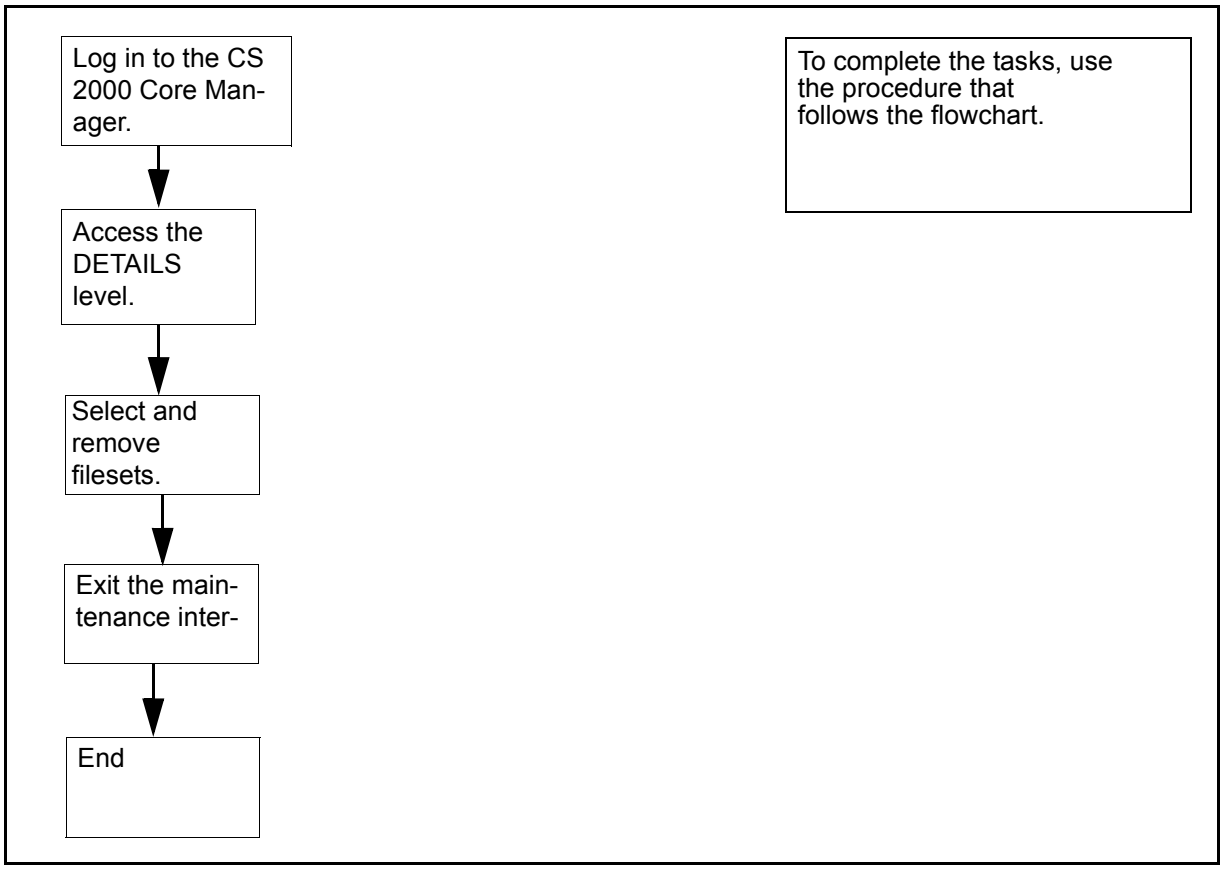
You can display the list of application filesets available on the CS 2000 Core Manager at the Details level, which includes the version and status of each application fileset. An application fileset can be in one of the following states:

- APPLIED—the CS 2000 Core Manager is using the software. If a previous version of the fileset exists in the archived state, the applied fileset may be removed. In that case, the previous version is restored.
- ARCHIVED -— a backup version of the fileset is available and can be restored.
- FAILED— the fileset failed and must be reinstalled before use.
- OBSOLETED—the fileset is no longer active

## Task flow diagram

The following task flow diagram summarizes the process. To complete the tasks, use the instructions in the procedure that follows the flowchart.

### Task flow for Removing application filesets




## Procedure

### Removing application filesets

***At the local or remote VT100 console:***

**1** Log in to the CS 2000 Core Manager as the root user.

**2** Access the DETAILS level of the maintenance interface:

```
# sdmmtc details
```

**3** Remove one or more filesets:

```
> remove <#>
```

*where*

**<#>**
is the number next to the fileset you want to remove

***Note:*** You can specify as many numbers as you want, to remove multiple filesets at one time.

4 When prompted, confirm the remove command:

```
> y
```

5 Exit the maintenance interface:

```
> quit all
```

6 You have completed this procedure.

# Removing DDMS filesets

## Purpose

Use this procedure to remove the DDMS filesets, as well as the DDMS logical volumes, only if DDMS is no longer required.

## Procedure

### Removing DDMS filesets

***At the local VT100 console***

**1** Log into the CS 2000 Core Manager using the root user ID and password.

**2** Access the SWIM level of the maintenance interface:

```
# sdmmtc swim
```

**3** Access the Details level:

```
> details
```

**4** Remove the DDMS filesets:

```
> remove  <n>
```

*where*

**<n>**
is the number next to each of the following DDMS filesets

- OSS and Application Svcs
- OSS Comms Svcs

**5** When prompted, confirm the remove command:

```
> y
```

**6** Delete the file log device for DDMS. Start the log delivery commissioning tool if it does not automatically appear:

```
# logroute
```

The Logroute Main Menu screen appears.

```
                Logroute Main Menu


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



Enter Option ==>
```

**7** Access the Device List Menu:

```
> 1
```

The Device List Menu screen appears.

```
                Device List Menu


          1 - View Device
          2 - Add Device
          3 - Delete Device
          4 - Modify Device
          5 - Help
          6 - Return to Main Menu



Enter Option ==>
```

**8** Access the Delete Device menu screen:

**> 3**

The system displays the list of configured devices and prompts you to enter the number of the device that you want to delete.

*Example response*

```
                  Delete Device Menu
Enter ABORT to return to Device List Menu
          Devices:                                    Type:
          1 - HOST: any           PORT: 8551          TCPIN
          2 - HOST: 10.102.4.4    PORT: 14450         TCP
          3 - /data/logs/faults                       FILE




 Enter device number to delete ==>
```

**9** Delete the file log device for DDMS:

**> <x>**

*where*

**<x>**
is the number next to the file log device for DDMS (/data/logs/ossaps/ossapslog)

*Response*

```
Device will be deleted permanently.
Continue... (Y/N)[N]:
```

**10** Confirm that you want to delete the selected device:

**> y**

*Response*

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

**11** Return to the Device List menu screen:

**> abort**

**12** Return to the Logroute Main menu screen:

**> 6**

**13** Quit the logroute tool:

```
> 6
```

**14** List the DDMS logical volumes:

```
# df -k
```

The logical volumes you need to remove are

- /osscomms
- /ossapslog
- /ossaps

**15** Proceed with the removal:

```
# cd /
# unmount /ossaps
# unmount /ossapslog
# unmount /osscomms
# rmfs /ossaps
# rmfs /ossapslog
# rmfs /osscomms
# rmdir /ossaps
# rmdir /ossapslog
# rmdir /osscomms
# rm /data/logs/ossaps
# rm /data/ossaps
# rm /data/ossapslog
# rm /data/osscomms
# cd /sdm
# rm -rf osscomms
# rm -rf ossaps
```

**16** You have completed this procedure.

# Removing I/O controller modules

## Purpose

Use this procedure to delete the following hardware modules from the CS 2000 Core Manager:

- NTRX50FU - I/O controller module with two 2-GByte disk drives and Ethernet
- NTRX50GP - I/O controller module with two 4-GByte disk drives and Ethernet

***Note:*** This procedure can also be followed by the procedure Adding I/O controller modules on page 1401 to change or correct the physical location. The I/O controller modules (NTRX50GN) in slots 2 and 3, and 13 and 14, of the main chassis are mandatory for system operation and cannot be removed.



**CAUTION**
**Removing a module**
Do not delete modules that are part of a volume group. If the module is not part of a volume group, you can continue with this procedure.



**CAUTION**
**Re-using an I/O controller module**
An I/O controller module must be manually busied and deleted before it can be re-used in a different slot.

## Prerequisites

To perform this procedure, you must know the following information:

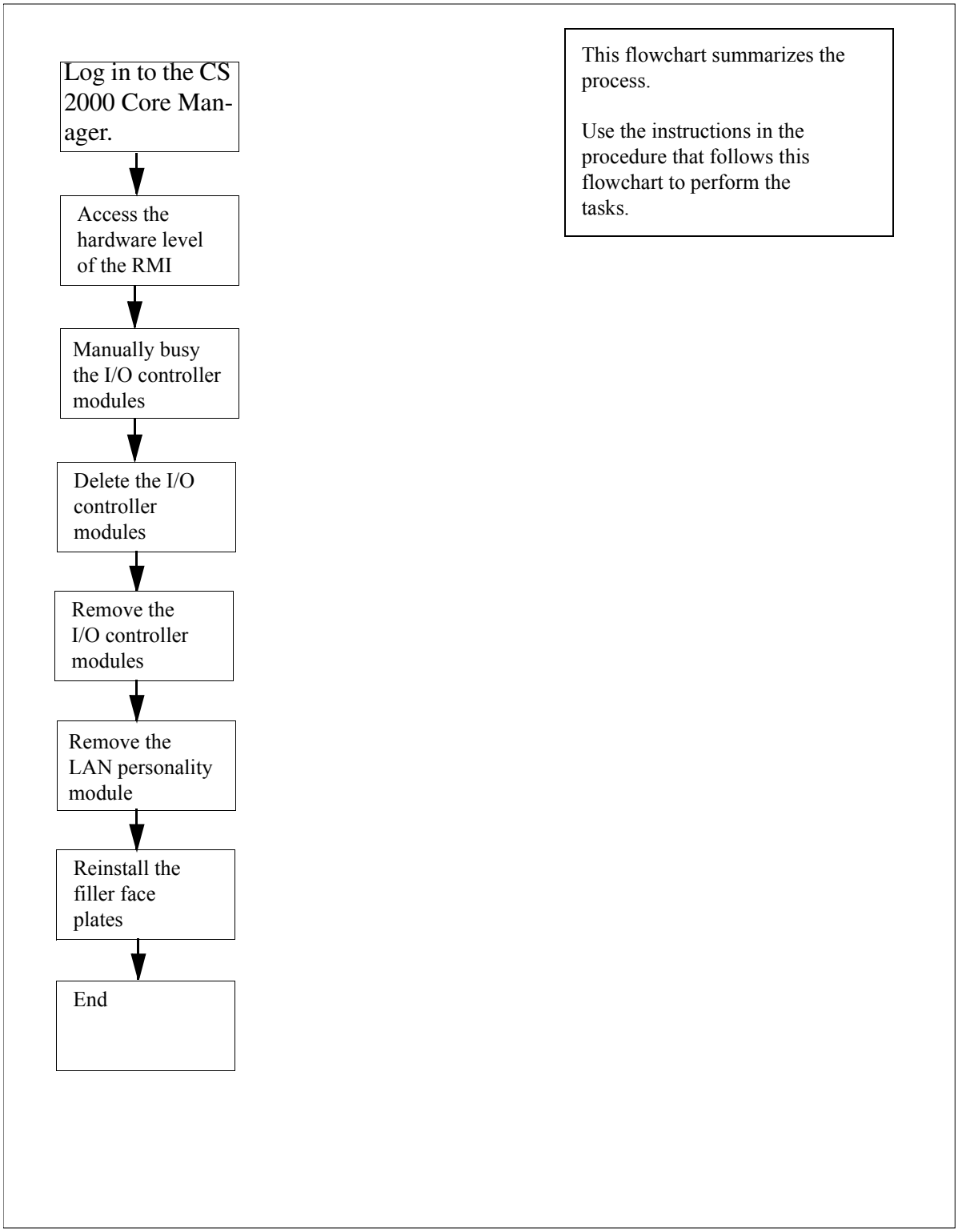
- the chassis (SDMM for main chassis; SDME for I/O expansion chassis)
- the I/O controller module's slot number (from 1 to 16)

***Note:*** Nortel Networks recommends that you contact Nortel Networks personnel before you remove any I/O controller modules. You cannot remove I/O controller modules until Nortel Networks deletes the data volume group (datavg) to which the module belongs. Nortel Networks also recommends that you remove I/O controller modules in pairs.

## Task flow diagram

The following task flow diagram provides an overview of the process. Use the instructions in the procedure that follows the flowchart to perform the task.

## Task flow for Removing I/O controller modules



## Procedure

### Removing I/O controller modules

***At the local or remote VT100 console***

1 Log in to the CS 2000 Core Manager as the root user.

2 Access the top menu level of the remote maintenance interface (RMI):

```
# sdmmtc
```

3 Access the hardware (Hw) menu level:

```
> hw
```

4 Determine the devices on the I/O controller module:

```
> locate
```

5



**CAUTION**
**Deleting an I/O controller module**
Deleting an I/O controller module requires you to put the module in both domains in ManB state. These modules will not be in service.

Manually busy the module in each domain:

```
> bsy <domain> dsk <n>
```

*where*

***<domain>>***
is the domain (0 or 1) of the I/O controller module that you are replacing

***<n>>***
is the disk number that you are replacing (Use the Locate command to determine the disk number of the module.)

Use the following list to determine the domain number. The domain number is

- 0 if the module is located in slots 4 and 5 of the main chassis
- 1 if the module is located in slots 15 and 16 of the main chassis

- 0 if the module is located in any two slots from 1 to 8 in the I/O expansion chassis
- 1 if the module is located in any two slots from 9 to 16 of the I/O expansion chassis

*Example response*

```
Hardware Bsy - Domain 1 Device DSK2
Busying DSK2(1) will also busy DSK3(1).

Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N"):
```

**6** Confirm the Bsy command:

```
> y
```

**7** After you confirm the Bsy command, the following is displayed:

*Example response*

```
Hardware Bsy: Domain 1 Device DSK2 - Command
initiated.
Please wait...
```

When the Bsy command is finished, the "Please wait..." message and the command confirmation disappear. The word "initiated" also changes to "submitted", then changes to "complete".

*Example response*

```
Hardware Bsy: Domain 1 Device DSK2 - Command
complete.
```

**8** Repeat steps 5 through 7 for the other domain. Once you have manually busied the module in both domains, go to step 9.

***Note:*** After you see the response to the Bsy command, the I/O controller module's state changes to "M" at the hardware level.

**9** Use the Locate command to determine the chassis and slot number of the module you wish to delete:

```
> locate
```

*Example response*

```
Site Flr RPos Bay_id Shf   Description    Slot
EQPEC
HOST 00  00   CSDM   SDME   DSK2(0),DSK3(0)  02
 NTRX50FU   FRNT
```

***Note:*** The example shown only displays part of the information generated from the Locate command. Press the Enter key to scroll through the display.

**10** Delete the module:

**> delete *<chassis>* *<slot>***

*where*

***<chassis>***
is the chassis where the module is located (SDMM for the main chassis or SDME for the I/O expansion chassis)

***<slot>***
is the slot number (from 1 to 16) where the module is located

***Note:*** The module in the corresponding slot of the other domain will also be deleted.

*Example response*

```
Module in slot 4 of SDMM will be deleted.
DSK2(0), DSK3(0) will be deleted.
Module in slot 15 of SDMM will also be deleted.

Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N"):
```

**11** Confirm that you want to delete the module:

**> y**

The DEL command may take several minutes to complete. When the command is finished, the following message is displayed:

```
Hardware Del Module - Command complete.
```

Within a few seconds, the module disappears from the listing shown at the hardware level, and the device numbers change on the screen display.

***At the front of the CS 2000 Core Manager***

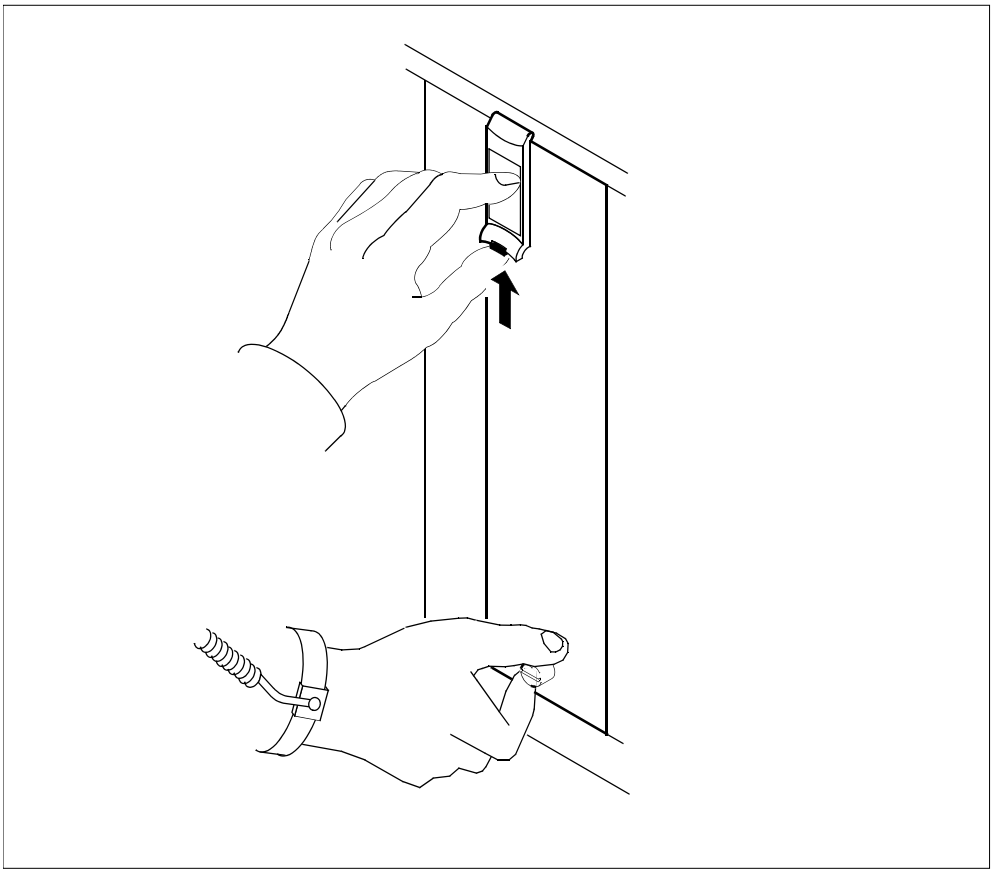
**12**

**WARNING**
**Static electricity damage**
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

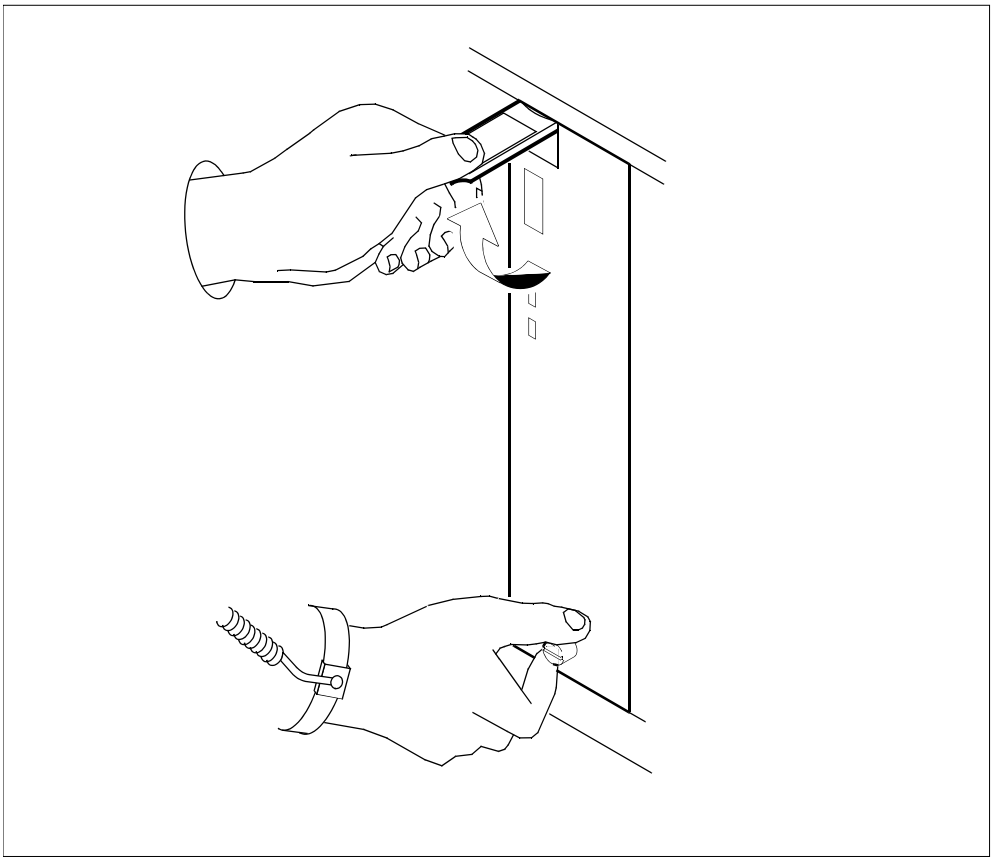
Put on an electrostatic discharge grounding wrist strap.

**13** Undo the thumbscrews located on the top and the bottom of the I/O controller module. The thumbscrews are the captive type, and cannot be removed from the module.

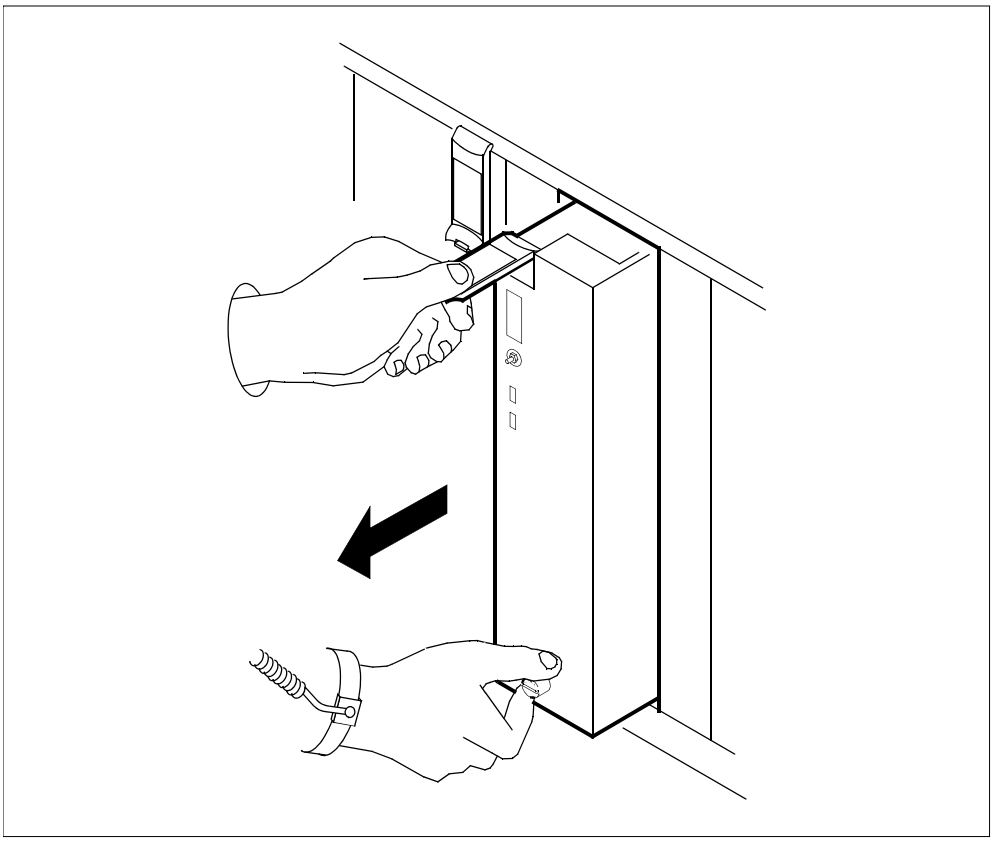
**14** Depress the tip of the locking lever on the face of the I/O controller module.



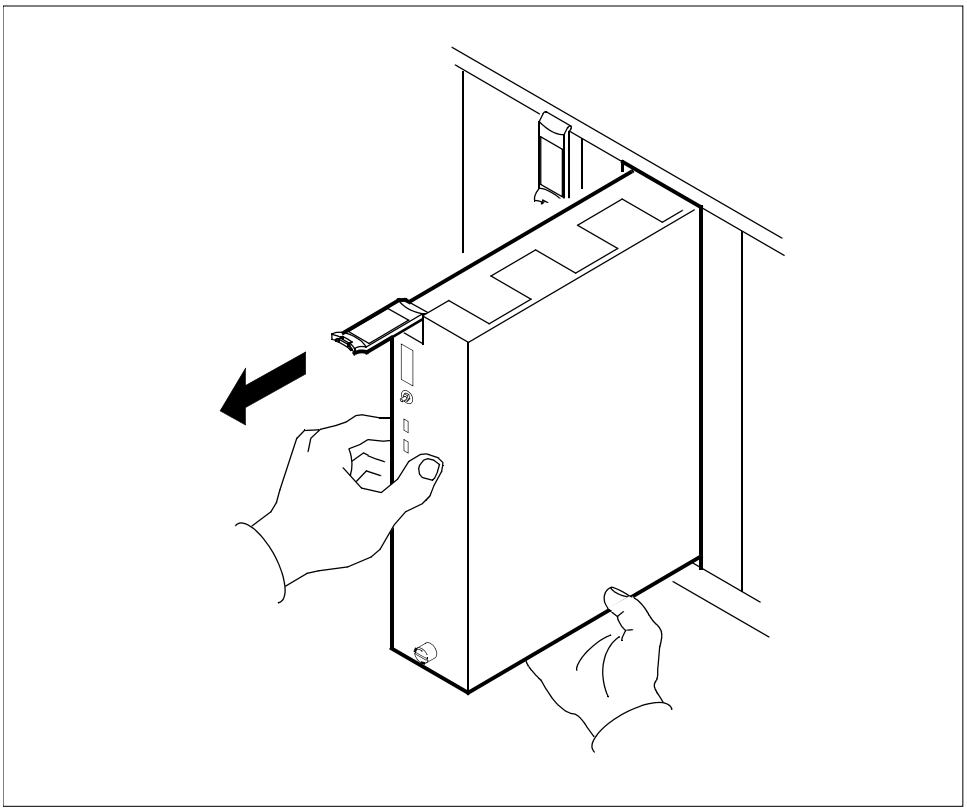
**15** Open the locking lever on the face of the module by moving the lever outwards.



**16** While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



**17** Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



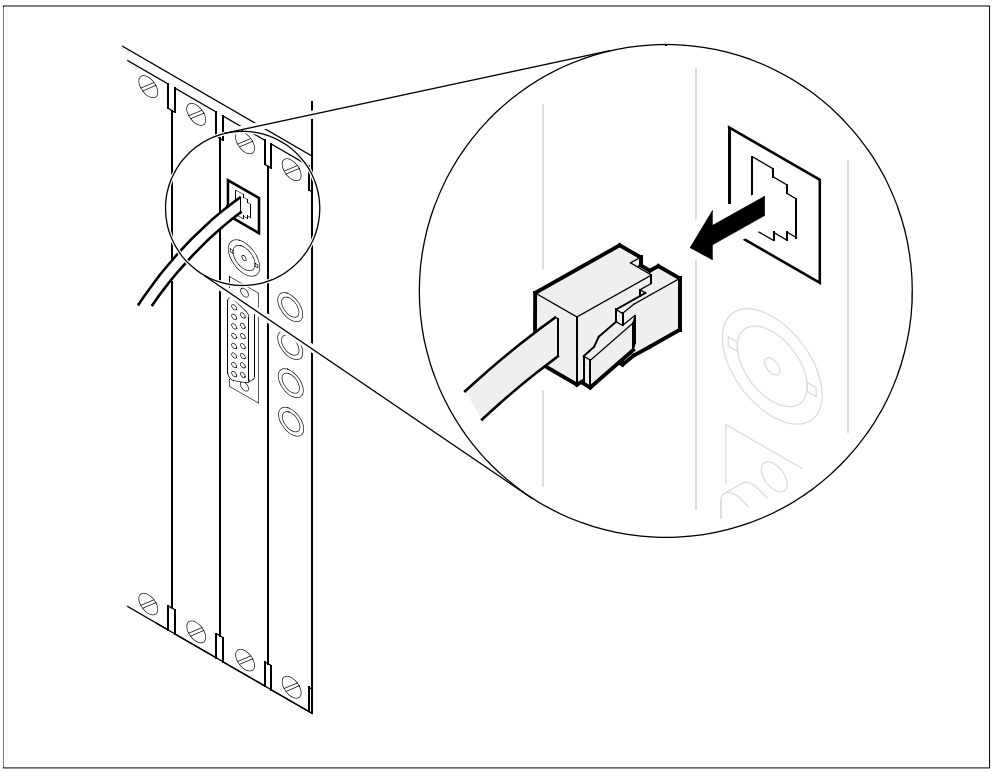
**18** Place the module you have removed in an ESD protective container.

***At the back of the CS 2000 Core Manager***

**19** Determine what kind of hardware module your CS 2000 Core Manager has.

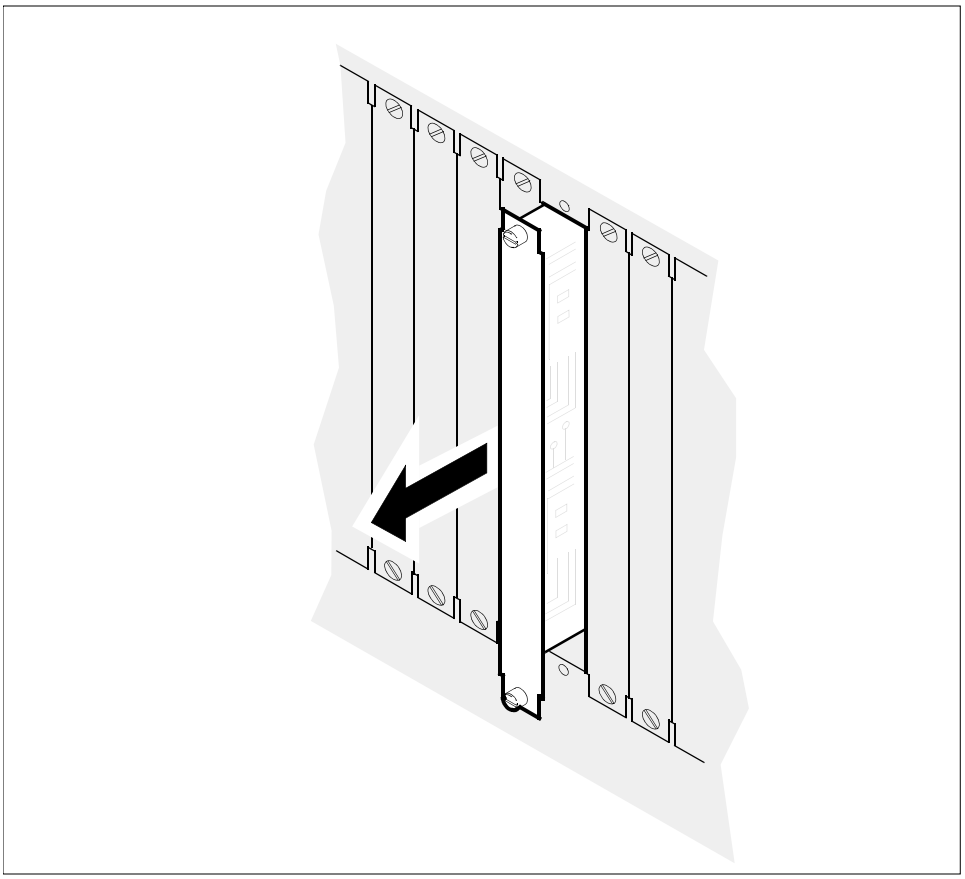
| If you have | Do |
|---|---|
| NTRX50GN | step 20 |
| NTRX50FU and NTRX50GP | step 21 |

**20** Disconnect the 10BASE-T cable from the corresponding LAN personality module, as shown in the following diagram.

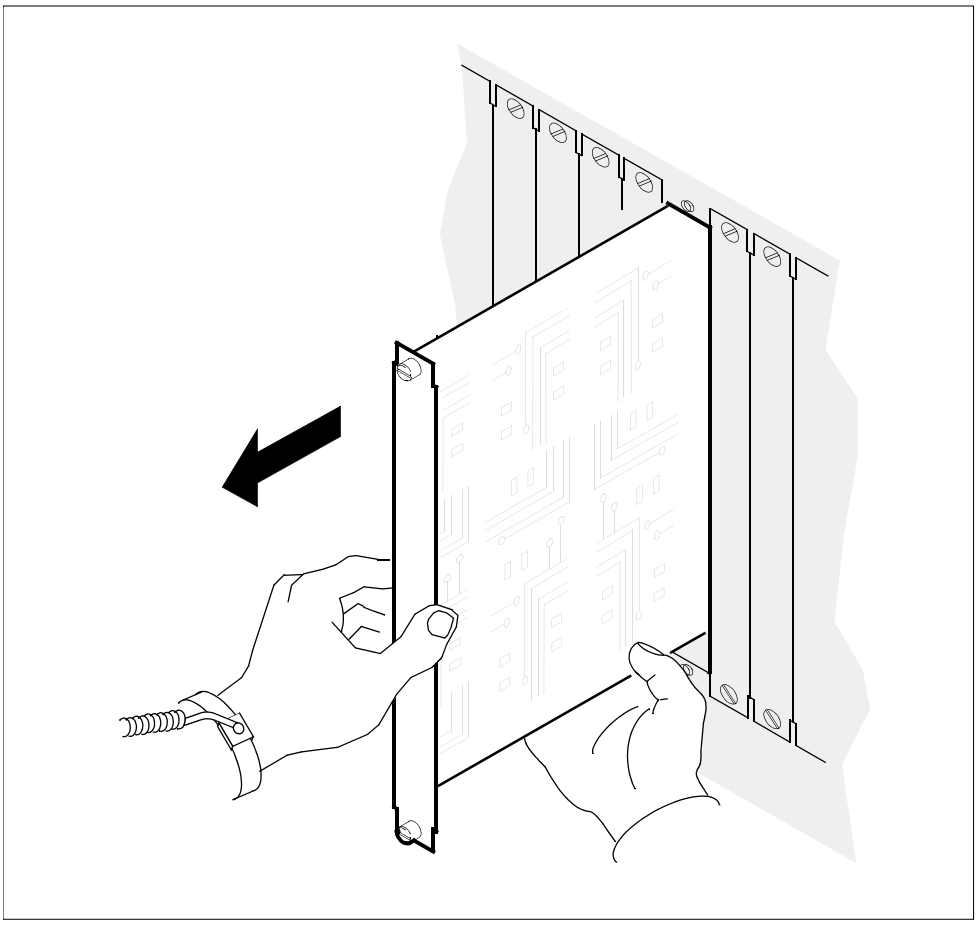


**21** Loosen the two thumbscrews located at the top and the bottom of the LAN personality module. The thumbscrews are the captive type, and cannot be removed from the module.

**22** While grasping the thumbscrews, gently pull the LAN personality module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



**23** Hold the LAN personality module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



**24** Place the LAN personality module you have removed in an ESD protective container.

**25** Reinstall the filler plates covering the slots from which you removed the modules.

**26** You have completed this procedure.

# Upgrading from an X.25 SYNC card to a UMFIO X.25 card

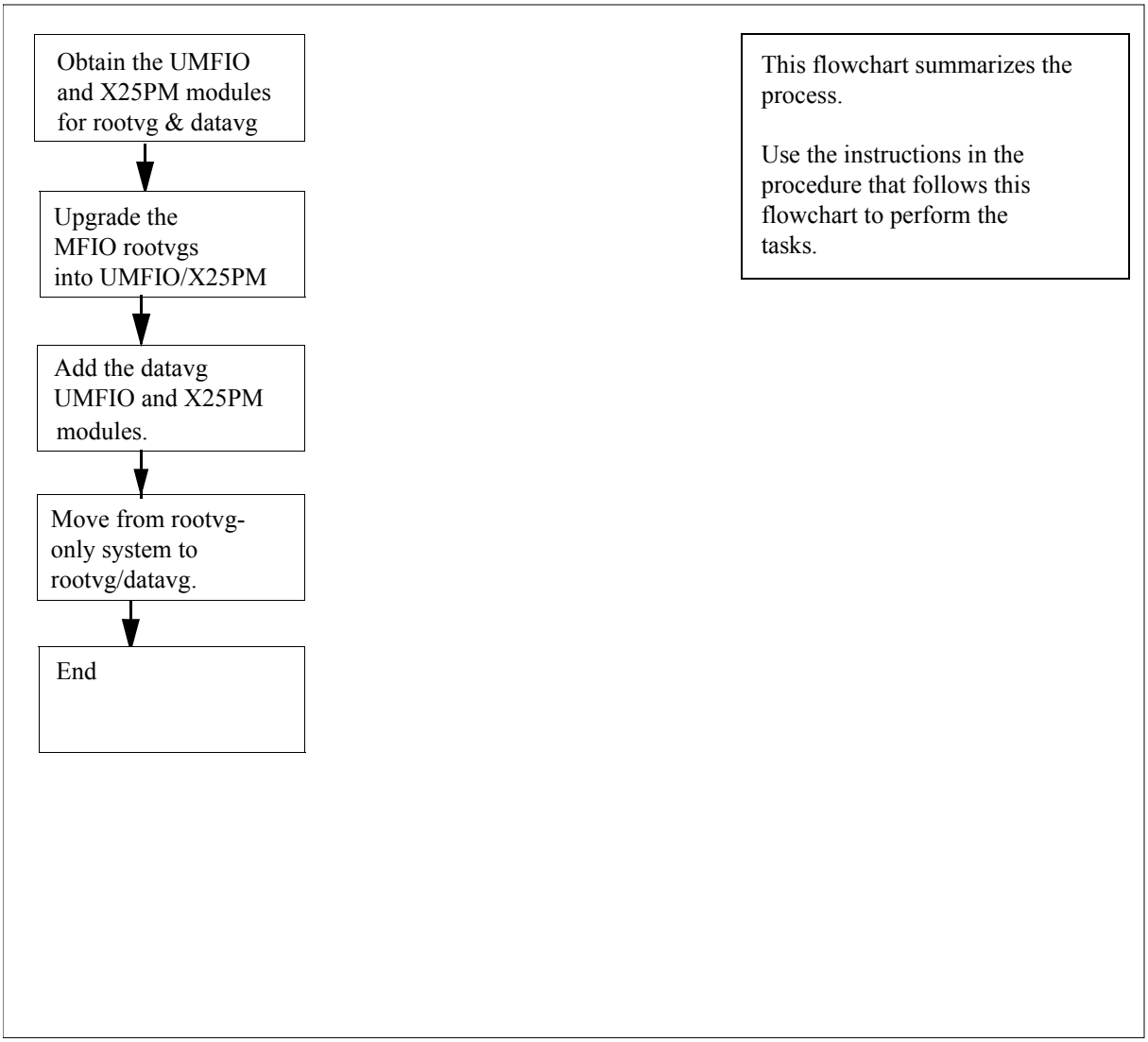
## Purpose

Use this procedure to move a system from a rootvg-only system with SYNC X25 into a rootvg/datavg system with UMFIO/X25PM.

## Task flow diagram

The following task flow diagram provides a summary of the process. To move from a rootvg-only system to a rootvg/datavg with X25, use the instructions in the procedure that follows the flowchart.

### Task flow for upgrading from an X.25 SYNC card to a UMFIO X.25 card



## Upgrading from an X.25 SYNC card to a UMFIO X.25 card

### *At the CS 2000 Core Manager*

1 Upgrade from rootvg MFIO with SYNC X.25 to UMFIO/X25PM. Obtain the UMFIO controller modules for rootvg and the X25PM modules. Ensure that the upgraded modules have the correct product engineering code (NTRX50NM for rootvg UMFIO and NTRX50NN for X25PM). The PEC is written on the module's top locking lever.

2 Perform the procedure Upgrading the rootvg MFIO to MFIO or UMFIO on page 1478, to upgrade from rootvg MFIO with SYNC X25 into rootvg UMFIO/X25PM for both domains.

3 Add the datavg UMFIO and X.25 PM to the system. Obtain the UMFIO controller modules for datavg and the X25PM modules. Ensure that the upgraded modules have the correct product engineering code (NTRX50NL for datavg UMFIO and NTRX50NN for X25PM). The PEC is written on the module's top locking lever.

4 Perform the procedure Adding I/O controller modules on page 1401, to add the datavg UMFIO and X25PM modules for both domains to the system.

5 Perform the procedure Migrating from a rootvg system to a rootvg/datavg system on page 1474, to move from a rootvg-only system to a rootvg datavg system.

6 You have completed this procedure.

# Migrating from a rootvg system to a rootvg/datavg system

## Purpose

**ATTENTION**
This procedure must be performed by a trained AIX system administrator who has root user privileges to access the CS 2000 Core Manager.

**ATTENTION**
Perform this procedure after you have installed the required I/O controller modules (in pairs) in the appropriate slots in the main or I/O expansion chassis. If you have not installed the required modules, refer to the procedure “Adding I/O controller modules” in the Upgrades section.

**ATTENTION**
This procedure requires that your system is MANB. Nortel Networks recommends that you add a datavg when you upgrade the CS 2000 Core Manager.

**ATTENTION**
A maximum of 16-Gbyte storage capacity is supported for datavg.

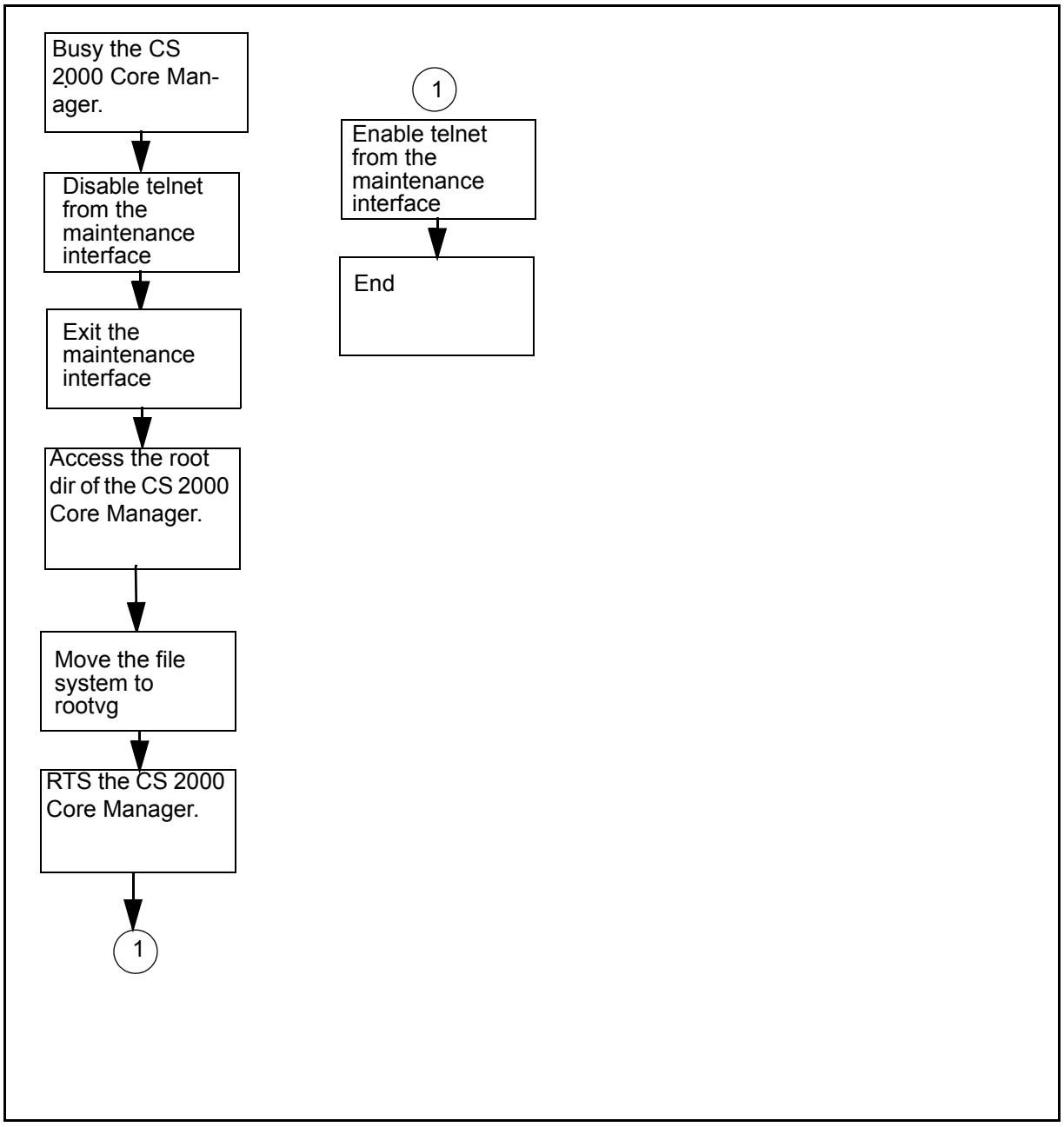
Use this procedure to move from a rootvg system to a system with both rootvg and datavg. This procedure creates datavg, and moves logical volumes from rootvg to datavg.

Logical volume data can be stored in the root volume group (rootvg) or the data volume group (datavg). Nortel recommends that you create datavg for logical volumes with large amounts of data. If you do not create datavg, the system stores logical volume data in rootvg.

## Task flow diagram

The following task flow diagram provides an overview of the process. Use the instructions in the procedure that follows the flowchart to perform the task.

## Task flow for migrating from a rootvg system to a rootvg/datavg system



# Procedure

### Creating a data volume group

***At the SDM level of the MAP display***

**1** Busy the CS 2000 Core Manager:

```
> bsy
```

***At the local or remote VT100 console***

**2** Log into the CS 2000 Core Manager as the root user.

**3** Access the administration (Admin) level:

```
> admin
```

**4** Access the Access level:

```
> access
```

The CS 2000 Core Manager displays the state of the telnet service. If telnet is already disabled, proceed to step 17.

**5** Disable telnet to ensure that no other user has access to CS 2000 Core Manager during the volume group migration:

```
> change
```

**6** Confirm the command:

```
> y
```

**7** Exit the maintenance interface:

```
> quit all
```

**8** Access the root directory:

```
# cd /
```

**9** Move the file system from rootvg to datavg:

```
# movevg
```

***Note 1:*** The movevg process takes some time to complete. When the process is complete, the system returns to the # prompt.

***Note 2:*** It may be several minutes after the movevg command is completed before datavg is displayed as “Mirrored” under the storage level.

***At the SDM level of the MAP display***

**10** Return the CS 2000 Core Manager to service:

```
> rts
```

***At the local or remote VT100 console***

**11** Log into the CS 2000 Core Manager as the root user.

**12** Access the administration (Admin) level:

```
> admin
```

**13** Access the Access level:

```
> access
```

**14** Enable telnet:

```
> change
```

**15** Confirm the command:

```
> y
```

**16** Exit the maintenance interface:

```
> quit all
```

**17** You have completed this procedure.

Refer to the procedure “Adding disks and creating a logical volume in datavg” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

# Upgrading the rootvg MFIO to MFIO or UMFIO

## Purpose

Use this procedure to upgrade from a 4GB + DAT Multifunction Input/Output (MFIO) module to a 9GB + DAT MFIO module.

You can also use this procedure to perform the following tasks:

- upgrade from a 4GB + DAT MFIO module or a 9GB + DAT MFIO module to a 36GB + DAT Ultra-Multifunction Input/Output (UMFIO) module
- upgrade to any other supported combinations. For the list of supported combinations, refer to the table “Supported MFIO and UMFIO, datavg and rootvg configurations” in *Upgrading the CS 2000 Core Manager,* NN10060-461.
- revert a rootvg I/O module to the original hardware configuration, but only if the rootvg I/O module in a single domain was upgraded. Before reverting back, confirm that the storage system has regained full mirroring

**ATTENTION**

Do not use this procedure to revert to the original rootvg I/O module if you have successfully upgraded the rootvg I/O module in both domains, or if you have upgraded from an MFIO with SYNC X.25 to a UMFIO with X.25 PMs

***Note:*** As of the 15.2 release, the system allows you to gracefully back out of an MFIO upgrade.

### Pre-upgrade requirements

If you are upgrading to UMFIO, you must check your system for UMFIO readiness prior to the upgrade. To check for UMFIO readiness, type the following:

**# umfiocheck**

The following example shows the output for a system that is UMFIO ready.

**Example**

```
1+0 records in.
1+0 records out.
1+0 records in.
1+0 records out.
This system is UMFIO ready.
```

If the UFMIO is not ready, you must perform a backup and restore. Perform the backup using the procedure “Creating system image backup tapes (S-tapes) manually” in *CS 2000 Core Manager Administration and Security*, NN10170-611. Perform the restore using the procedure “Performing a full restore of the software from S-tape” in the Fault Management document.

Once you have completed the backup and restore, rerun the ufmiocheck command. If your system is still not UMFIO ready, contact your next level of support.

**ATTENTION**

Have the correct UMFIO LAN PM.

In order to upgrade to the UMFIO, you must have either the UMFIO LAN personality module (NTRX50NK) or the X25 personality module (NTRX50NN) available.



**CAUTION**

Back up the system before you begin this procedure. If SBA is installed, make sure you back up the billing data. Also, make sure there is no tape in the MFIO DAT drive.

The following table lists the product engineering codes (PEC).

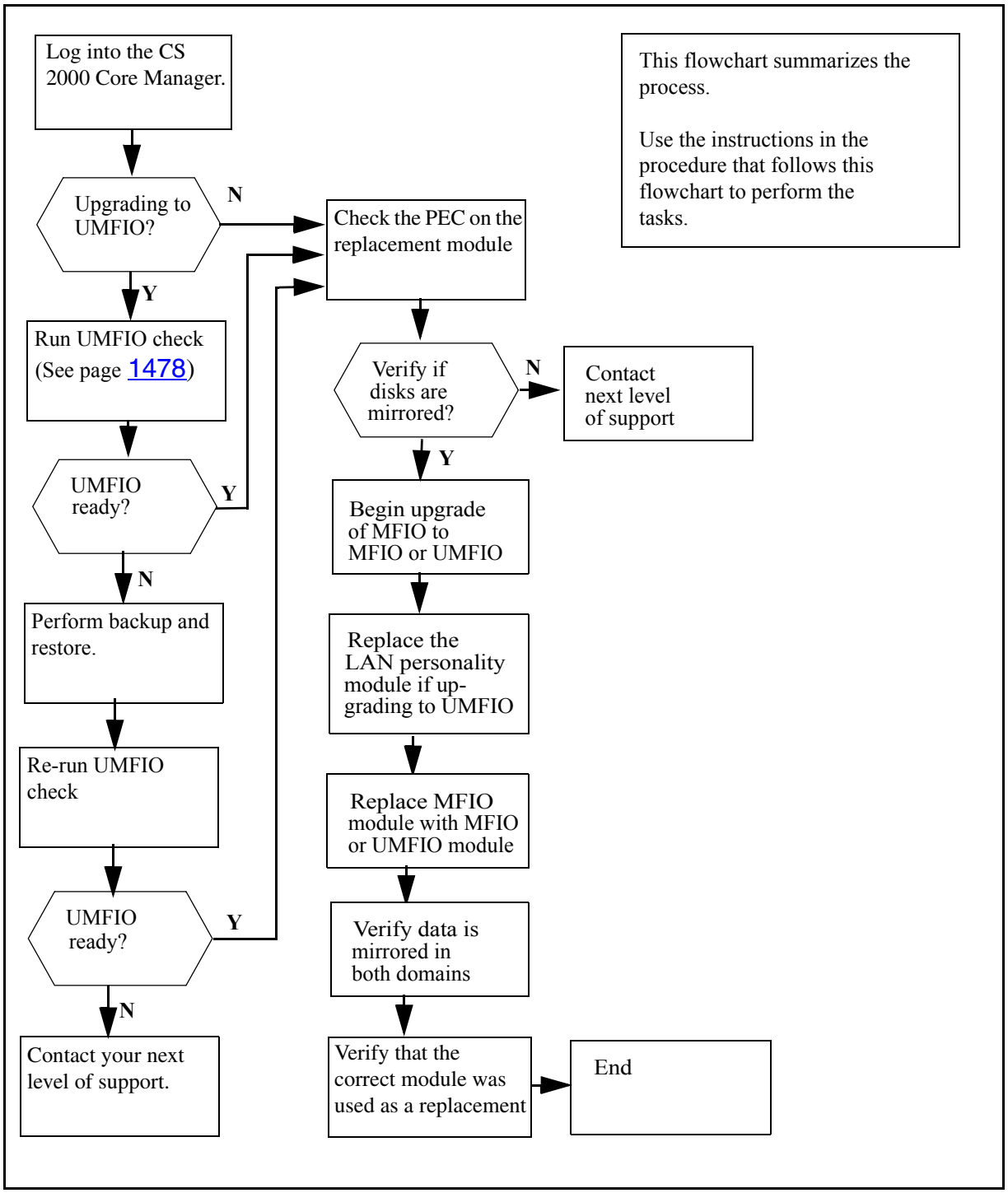
| Nortel PEC | Name |
|---|---|
| NTRX50FS | LAN personality module for MFIO |
| NTRX50GN | 4GB + DAT rootvg MFI |

| Nortel PEC | Name |
|---|---|
| NTRX50ND<br><br>***Note:*** Replacements for the NTRX50ND will be filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004, the NTRX50NM will be the replacement for the NTRX50ND | 9GB + DAT rootvg MFIO |
| NTRX50NK | LAN personality module for UMFIO |
| NTRX50NN | X25 personality module for UMFIO |
| NTRX50NM | 36GB + DAT rootvg UMFIO |

## Task flow diagram

The following task flow diagram provides a summary of this process. Use the instructions in the procedure that follows the flowchart to perform the tasks.

## Task flow for Upgrading the rootvg MFIO to MFIO or UMFIO



## Procedure

### Upgrading the rootvg MFIO to MFIO or UMFIO

***At the VT100 console***

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

**2** Check the label on the module that you want to use as a replacement. Make sure that label shows the product engineering code (PEC) that you want to use for your upgrade.

**3** Access the storage level:

**# sdmmtc storage**

**4** Use the following table to determine your next step.

| If the State of both volumes is | Do |
|---|---|
| Mirrored | step 5 |
| not Mirrored | contact your next level of support |

**5** Access the hardware level under RMI:

**> hw**

**6** Upgrade the MFIO:

> **upgrade <chassis> <slot> <pec>**

*where*

**<chassis>**
is sdmm since both rootvg MFIOs are located in the main chassis

**<slot>**
is slot 2 if you are upgrading domain 0 or slot 13 if you are upgrading domain 1

**<pec>**
is the product engineering code of the MFIO or UMFIO controller module you want to add

**Example**

```
upgrade sdmm 2 NTRX50NM
```

This example indicates an upgrade to the 36GB + DAT UMFIO in slot 2 of the main chassis.

**7** Use the following table to determine your next step.

| If you are | Do |
|---|---|
| prompted to delete the x25 sync module configuration | step 8 |
| not prompted to delete the x25 sync module configuration | step 9 |

**8** Confirm the deletion of the X25 SYNC module configuration:

```
> y
```

**9** You can replace the MFIO, or exit the upgrade when you see the following system response:

***Note 1:*** DO NOT enter 1 until you have first replaced the MFIO.

***Note 2:*** Enter 99 to exit the procedure. The system gracefully backs you out of the upgrade procedure if you choose to exit the upgrade at this point without replacing the hardware.

*Example response*

```
Transitioning forward from START to INFO_RETRIEVED

Volume group = rootvg on hdisk0
Physical partition size 16 with max partitions 3048

Transitioning forward from INFO_RETRIEVED to OFFLINED
Transitioning forward from OFFLINED to DEPENDENCIES_REMOVED
Transitioning forward from DEPENDENCIES_REMOVED to REPLACED

Replace ORIGINAL MFIO I/O-2 (c1-f2) with UPGRADED MFIO

Enter 1 to continue, 99 to exit:
```

The following response may be displayed as the MFIO upgrade progresses.

```
0516-1193 chvg: WARNING, once this operation is
completed, volume group rootvg cannot be
```

```
imported into AIX 430 or lower versions.
Continue (y/n)?
```

| If this response is | Do |
|---|---|
| displayed | step 10 |
| not displayed | step 11 |

**10** Confirm the operation:

```
> y
```

*Response*

```
0516-1164 chvg: Volume group rootvg changed.
With given characteristics rootvg can include up
to 10 physical volumes with 3048 physical
partitions each.
```

***At the front of the CS 2000 Core Manager***

**11**



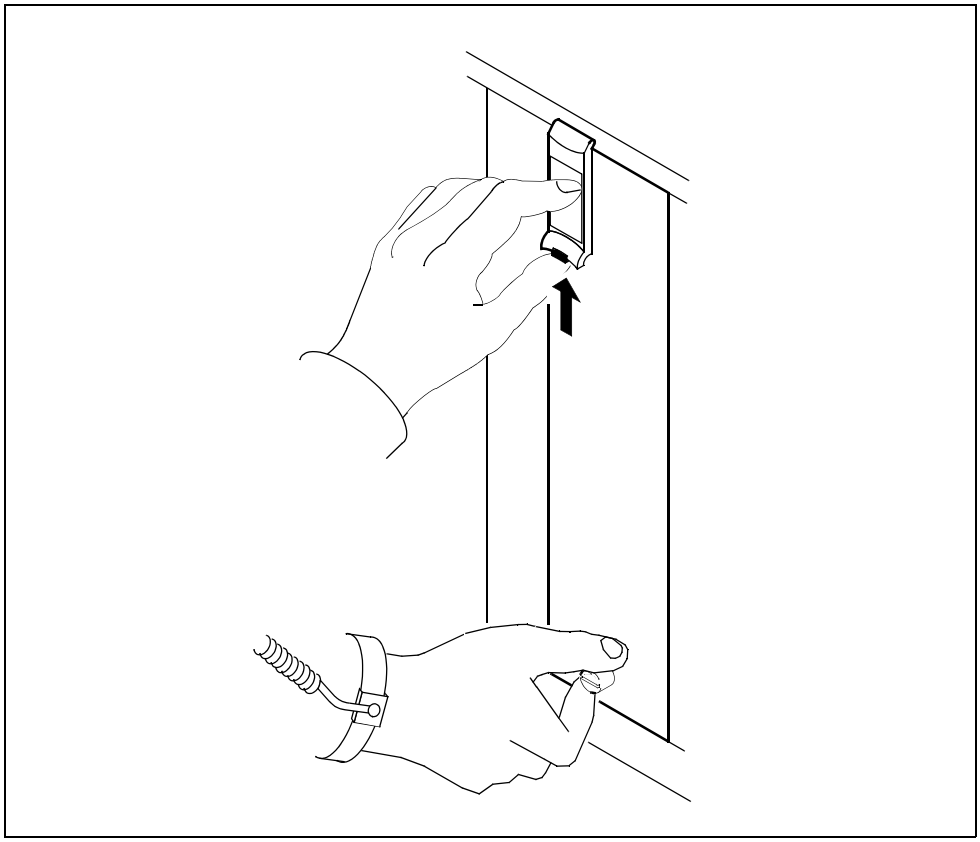
**WARNING**
**Static electricity damage**
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge grounding wrist strap.

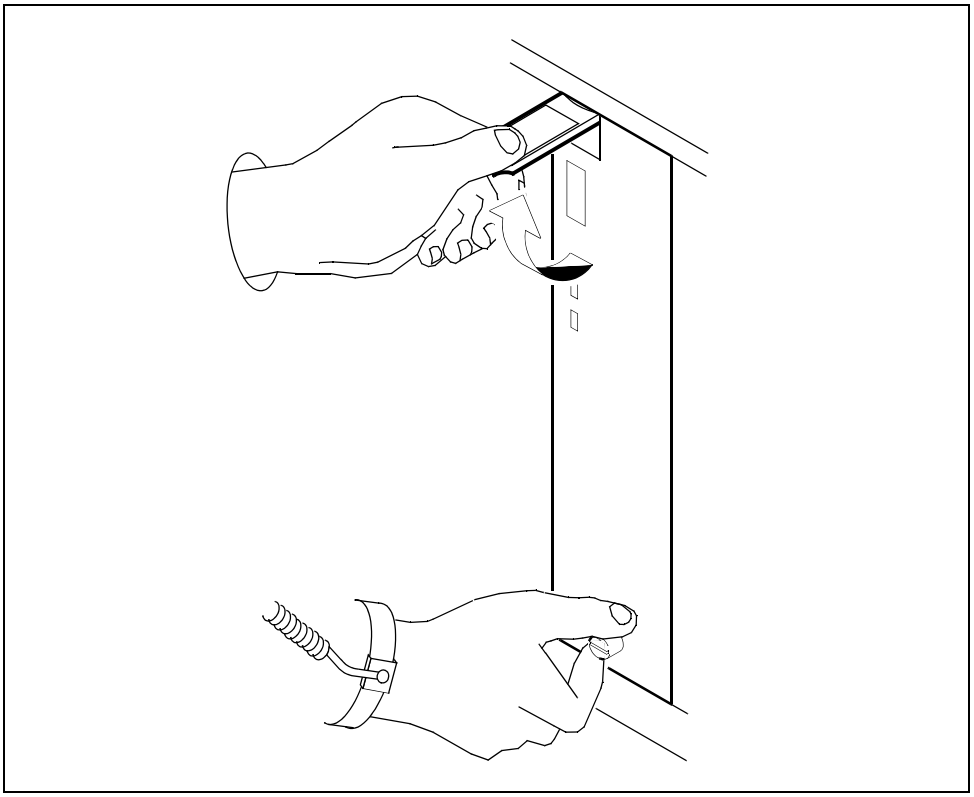
**12** Undo the thumbscrews located on the top and the bottom of the MFIO controller module to be upgraded. The thumbscrews are the captive type, and cannot be removed from the module.

***Note:*** Make sure the LED of the module you want to upgrade is either red or off before you remove it.

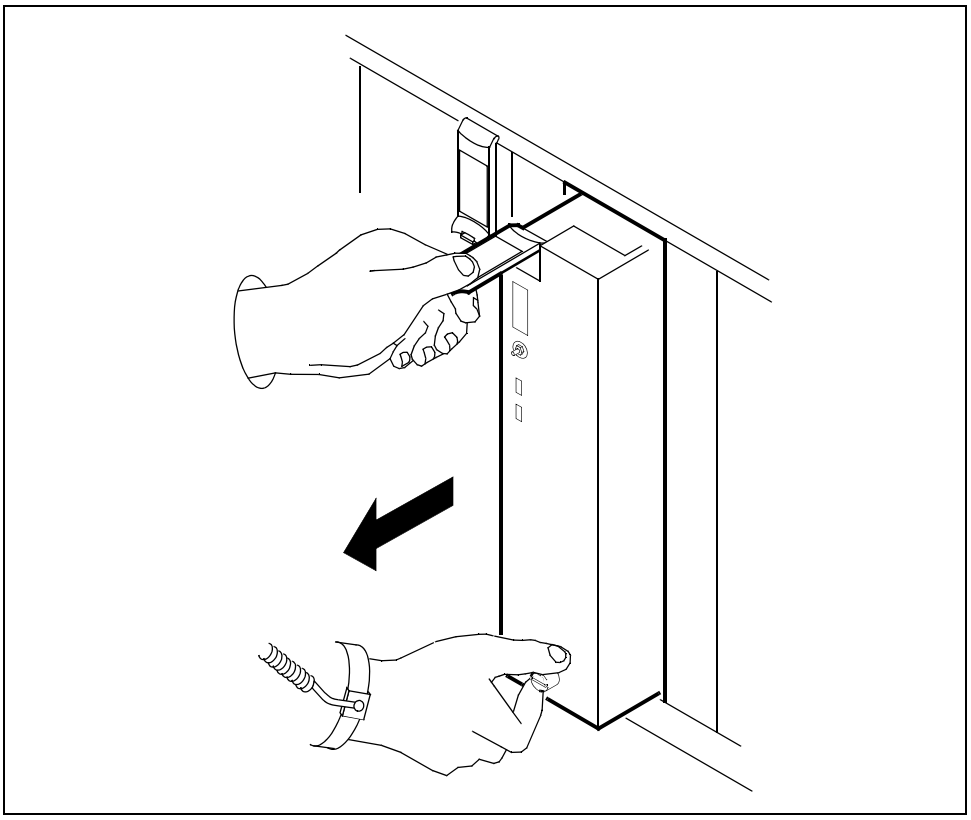
**13** Depress the tip of the locking lever on the face of the MFIO controller module.



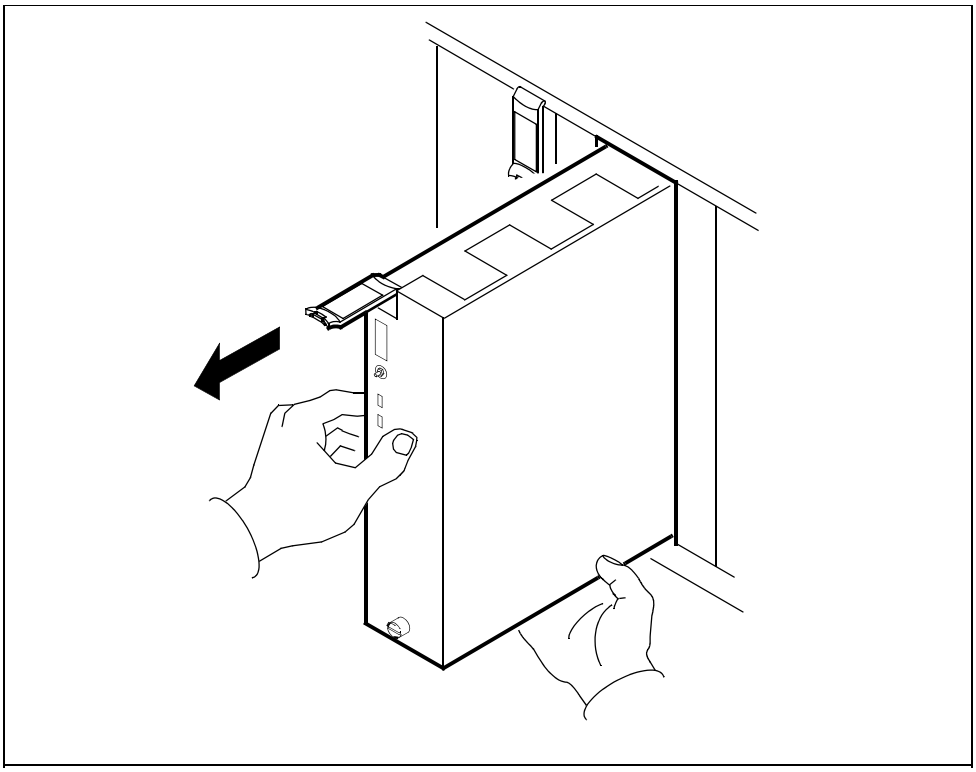
**14** Open the locking lever on the face of the module by moving the lever outwards.



**15** While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



**16** Hold the card by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



**17** Place the module you have removed in an ESD protective container.

***At the back of the CS 2000 Core Manager***

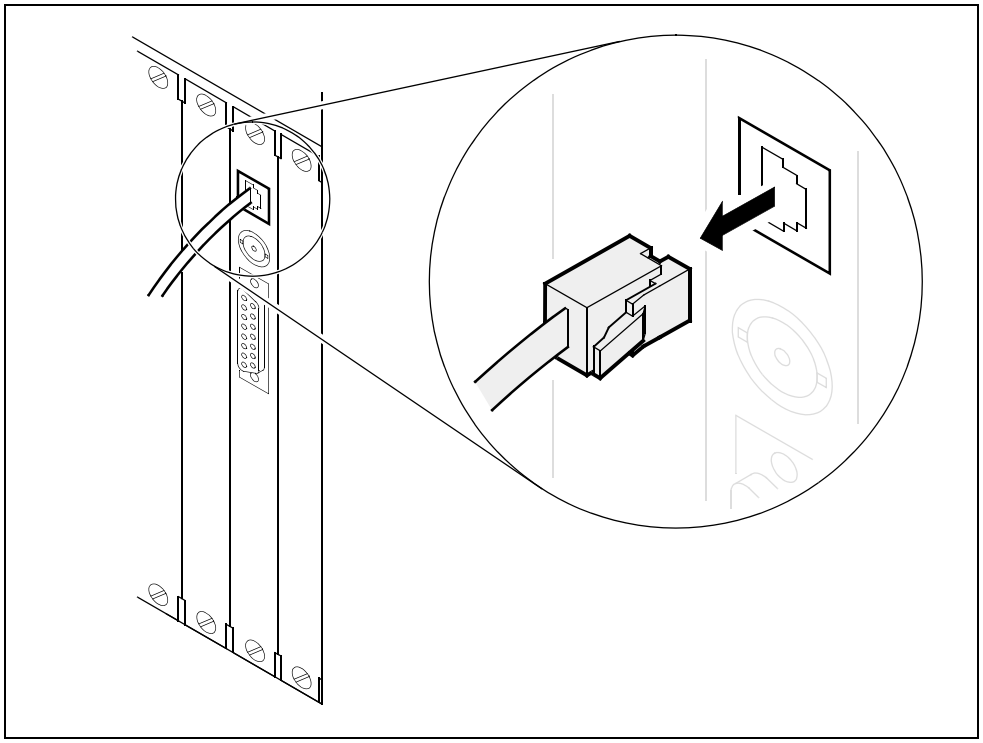
**18** Use the following table to determine your next step.

| If you are | Do |
|---|---|
| upgrading to the UMFIO | step 19 |
| not upgrading to the UMFIO | step 30 |

**19** You will now be removing the existing LAN personality module and replacing it with the new personality module (NTRX50NK or NTRX50NN) that came with the new UMFIO module. This must be done before inserting the new UMFIO module. It is located at the rear of the I/O controller module to be upgraded.

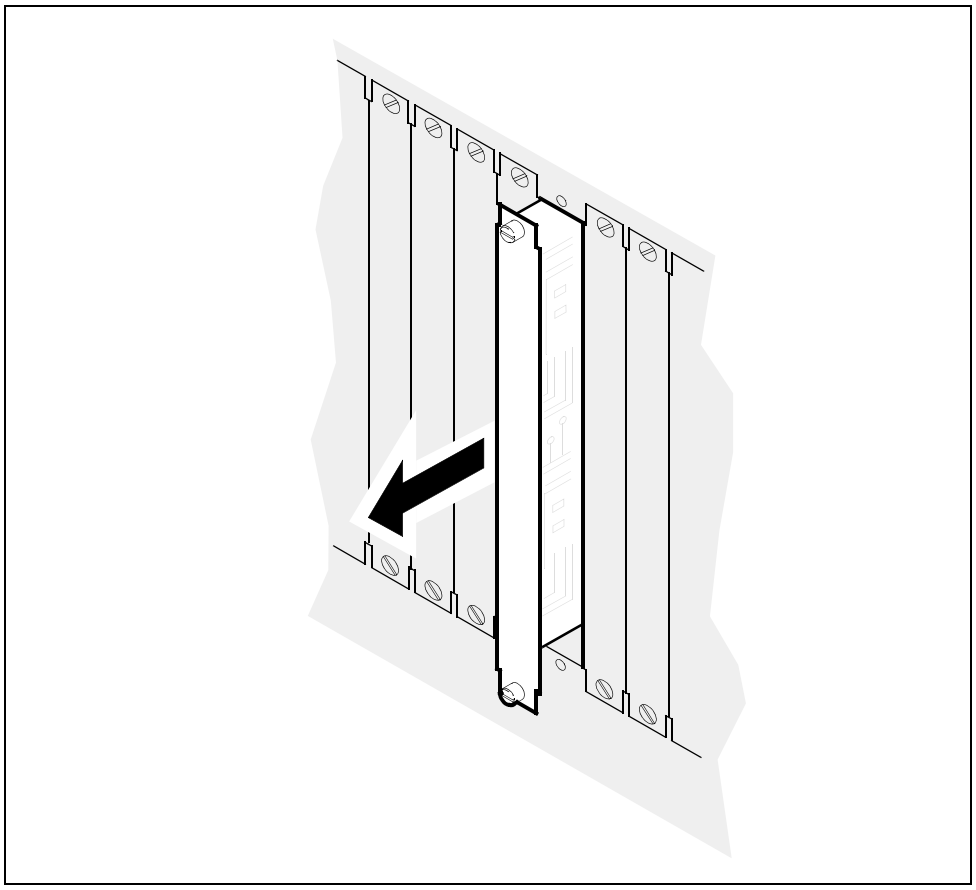
**20** Label the Ethernet cable connected to the LAN personality module you wish to replace.

**21** Disconnect the Ethernet cable, as shown in the following diagram.

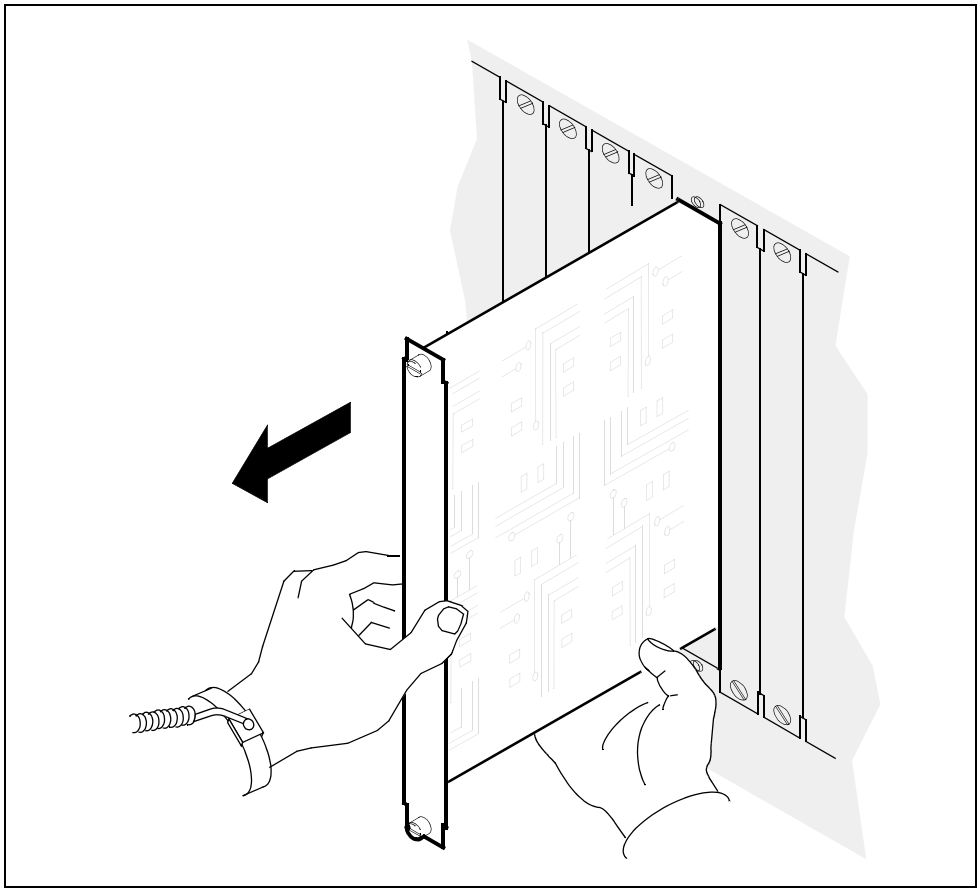


**22** Loosen the two thumbscrews located at the top and the bottom of the LAN personality module. The thumbscrews are the captive type, and cannot be removed from the module.

**23** While grasping the thumbscrews, gently pull the LAN personality module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



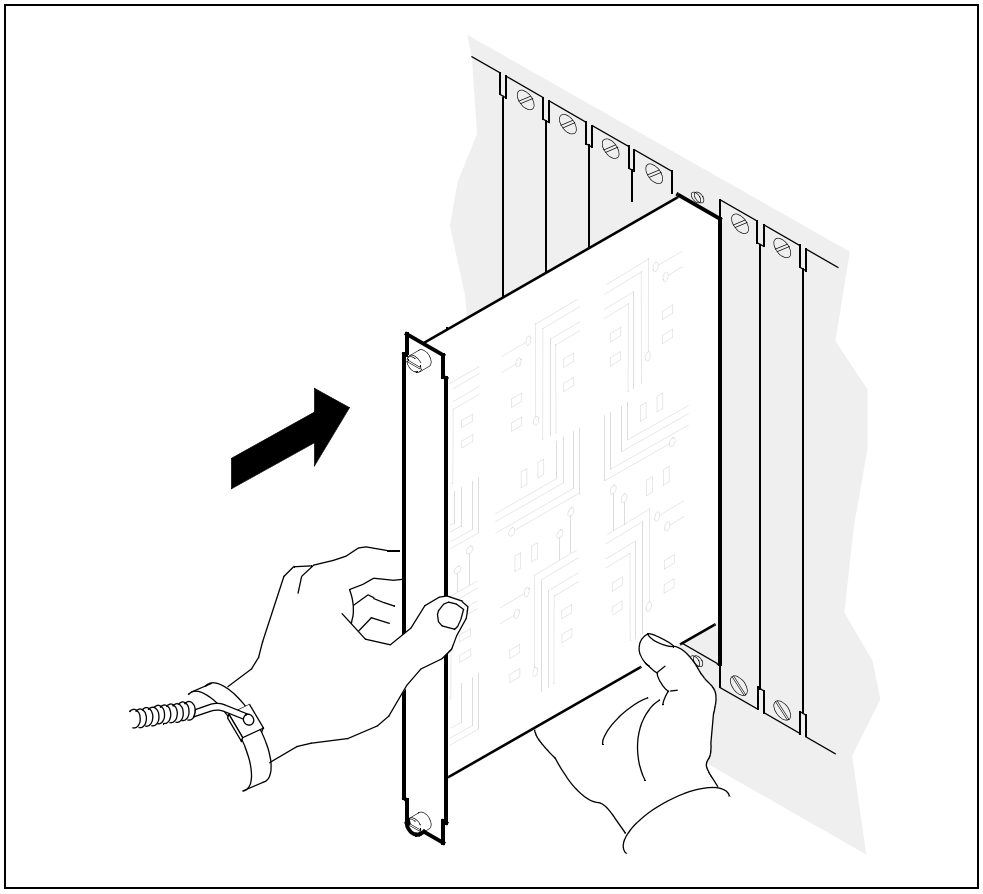
**24** Hold the LAN personality module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



**25** Place the LAN personality module you have removed in an ESD protective container.

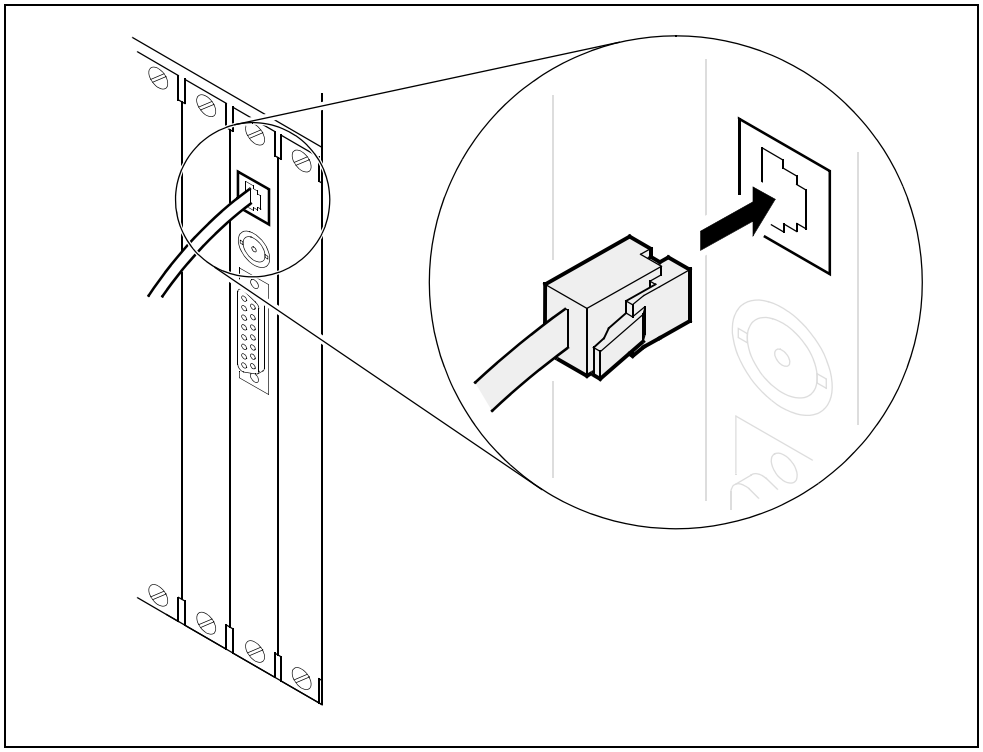
**26** Insert the new personality module (NTRX50NK or NTRX50NN) into the CS 2000 Core Manager shelf.

**27** Gently slide the LAN personality module into the shelf until it is fully inserted.



**28** Tighten the thumbscrews at the top and the bottom of the LAN personality module.

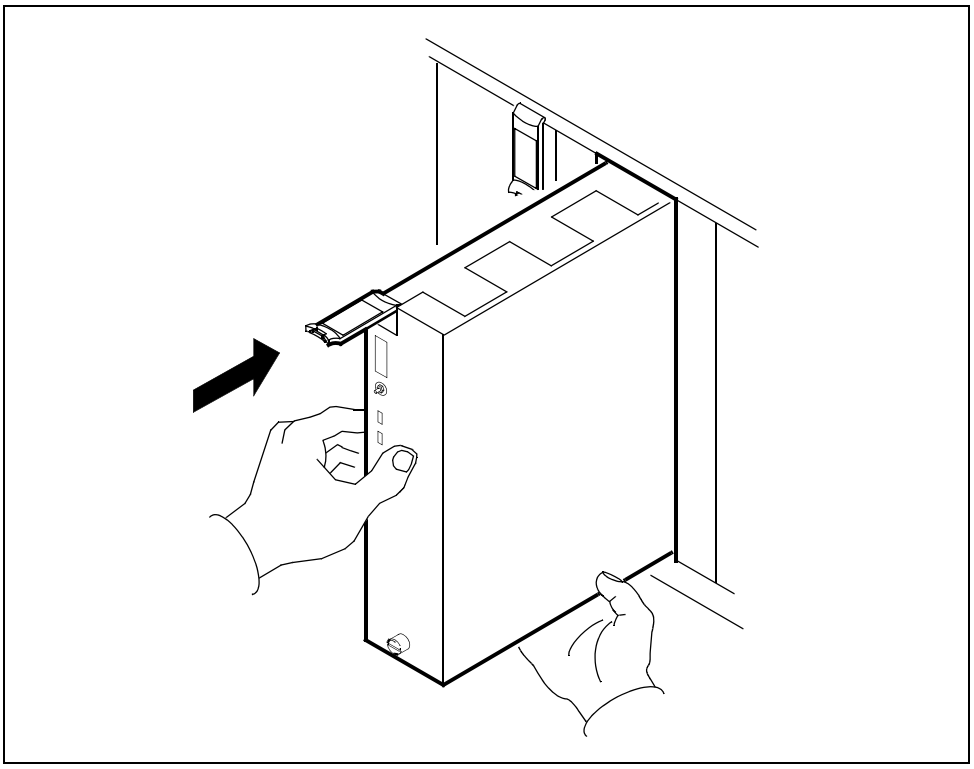
**29** Reconnect the Ethernet cable to the LAN personality module. You may remove the label that you put on the cable in step 20.



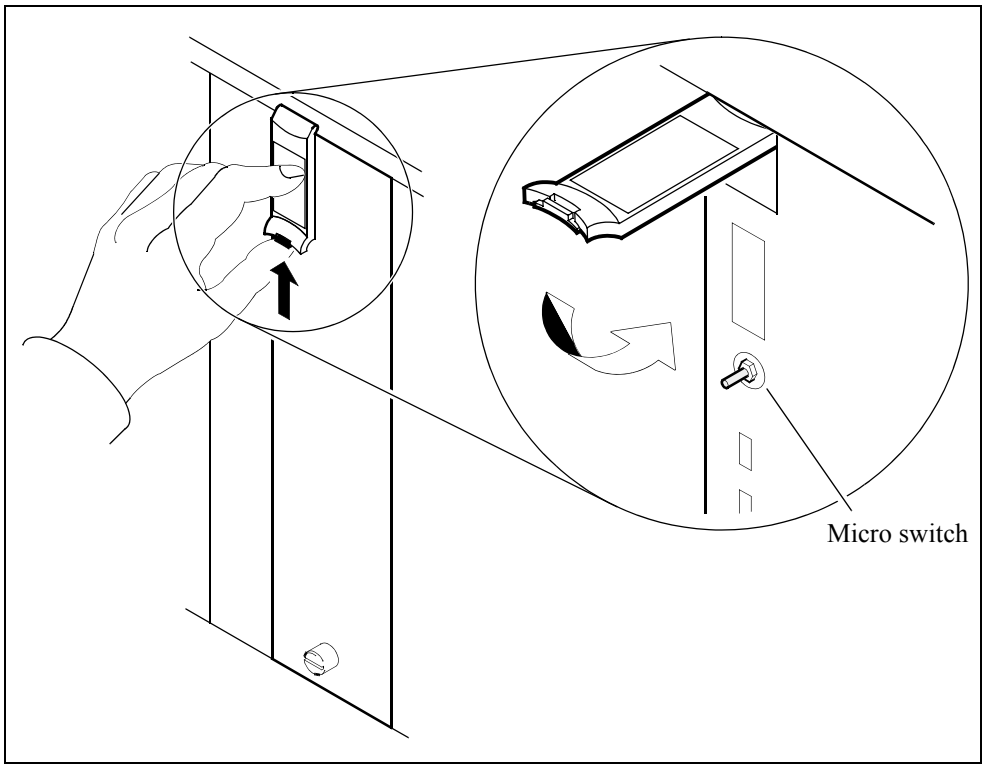
***At the front of the CS 2000 Core Manager***

**30** Insert the PEC MFIO or PEC UMFIO module into the CS 2000 Core Manager shelf.

**31** Gently slide the module into the shelf until it is fully inserted.



**32** Close the locking lever to secure the module. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.




**33** Tighten the thumbscrews on the module.

**34** Continue the upgrade:

> **1**

*Response*

```
Transitioning forward from REPLACED to ONLINED
Transitioning forward from ONLINED to DEPENDENCIES_ADDED
Transitioning forward from DEPENDENCIES_ADDED to OFFLINED_AFTER_UPGRADE
Transitioning forward from OFFLINED_AFTER_UPGRADE to ONLINED2
Transitioning forward from ONLINED2 to COMPLETE
>
```

**35** Use the following table to determine your next step.

| If the system | Do |
|---|---|
| prompts you to remove the X25 SYNC module from slot <n> | step 36 |

| If the system | Do |
|---|---|
| does not prompt you to remove the X25 SYNC module from slot <n> | step 38 |

**36** Remove the X25 SYNC module from the slot indicated in the display.

*Example response*

```
Please wait while the configuration for SYNC-0 is deleted...

Please remove the X.25 SYNC module from the main chassis
slot 4.

Enter 1 to continue when ready:("1"):
```

**37** Once you have removed the X25 SYNC module, continue the upgrade:

```
> 1
```

**38** You are automatically returned to the sdmmtc Hw level. Wait until the system completes the reintegration.

***Note:*** X25 users who are upgrading to UMFIO with X25PM need to re-configure the X25 ports as part of the UMFIO. This can be done during system integration. To configure the X25 ports, refer to the procedure Commissioning X.25 connectivity on page 628.

Once the system completes the reintegration, the status of the volume group changes to `Mirrored`.

**39** Verify that the correct module was used as a replacement:

```
> locate
```

The system displays a list of hardware. Confirm that the correct PEC is listed for the newly upgraded module.

**40** Upgrade the MFIO /UMFIO module in the other domain by repeating steps 4 through 39.

**41** You have completed this procedure.

# Upgrading a datavg MFIO to MFIO or UMFIO

## Purpose



**CAUTION**
**Possible loss of intercept service**
If the MFIO to be upgraded supports lawful intercept through an X.25 interface, this procedure removes lawful intercept from service for a short period of time. After you complete the upgrade procedure, you must restart the lawful intercept application.

Use this procedure to perform the following Multifunction Input/Output (MFIO) to MFIO or Ultra-Multifunction Input/Output (UMFIO) upgrades:

- 4GB + 4GB MFIO to 9GB + 9GB MFIO
- 4GB + 4GB MFIO to 36GB + 36GB UMFIO
- 9GB + 9GB MFIO to 36GB + 36GB UMFIO

***Note 1:*** You can also use this procedure to upgrade to any other supported combinations. For the list of supported combinations, refer to the table “Supported MFIO and UMFIO, datavg and rootvg configurations” in *Upgrading the CS 2000 Core Manager,* NN10060-461.

***Note 2:*** You can use this procedure to revert to the original MFIO in a single domain, but only once the procedure is complete and you have confirmed that the storage system has regained full mirroring. Do not use this procedure to revert to the original MFIO if you have successfully upgraded the MFIO in both domains.

***Note 3:*** As of the 15.2 release, the system allows you to gracefully back out of an MFIO upgrade.

Refer to the following table for the product engineering codes.

| Nortel PEC | Name |
|---|---|
| NTRX50FS (back) | LAN personality module for MFIO |
| NTRX50GP (front) | 4GB + 4GB datavg MFIO |

| Nortel PEC | Name |
|---|---|
| NTRX50NC (front)<br><br>***Note:*** Replacements for the NTRX50NC will be filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NL will be the replacement for the NTRX50NC. | 9GB + 9GB datavg MFIO |
| NTRX50NK (back) | LAN personality module for UMFIO<br><br>***Note:*** The NTRX50NK is required if you want to use the datavg UMFIO (NTRX50NL) for LAN access. If you intend to use the datavg UMFIO for storage only, or if you do not currently have LAN cards, you do not need to install the NTRX50NK. |
| NTRX50NN (back) | X25 personality module for UMFIO |
| NTRX50NL (front) | 36GB + 36GB datavg UMFIO |

## Prerequisites and guidelines

**ATTENTION**
Perform a backup of your billing files before starting this procedure. Also, ensure that an S-tape (System Image Tape) of your CS 2000 Core Manager is made prior to starting the upgrade procedures.

**ATTENTION**
Upgrading a mirrored pair of MFIOs can require a full maintenance window to complete. If an expansion chassis is provisioned, the upgrade of additional mirrored pairs of MFIOs may require multiple maintenance windows.

**ATTENTION**
You must have root user access to the CS 2000 Core Manager to perform this procedure.

**ATTENTION**
A UMFIO upgrade requires the UMFIO LAN personality module (NTRX50NK) or the X25 personality module (NTRX50NN).

No CS 2000 Core Manager should be populated with more than 2 MFIOs per I/O domain (for any combination) as part of datavg.

If a CS 2000 Core Manager is equipped with more than 2 MFIOs per side (prior to upgrading to CS2E0004), it is not possible to upgrade regular MFIOs to UMFIOs, or to upgrade to CS2E0004 without first contacting a Nortel-qualified craftsperson. Operating a CS 2000 Core Manager with more than 2 MFIOs (called large volume support) is possible but not supported in CS2E0004. Additionally, Nortel Networks does not support an upgrade path to UMFIOs with such a configuration.

If your system is already configured with more than 2 MFIOs per I/O domain, and you wish to upgrade to CS2E0004, you must contact Nortel Networks before attempting to upgrade to CS2E0004.

Nortel Networks recommends that the MFIOs in the main chassis be upgraded first, starting with domain 1 and ending with domain 0. After upgrading the main chassis, proceed to upgrade the expansion

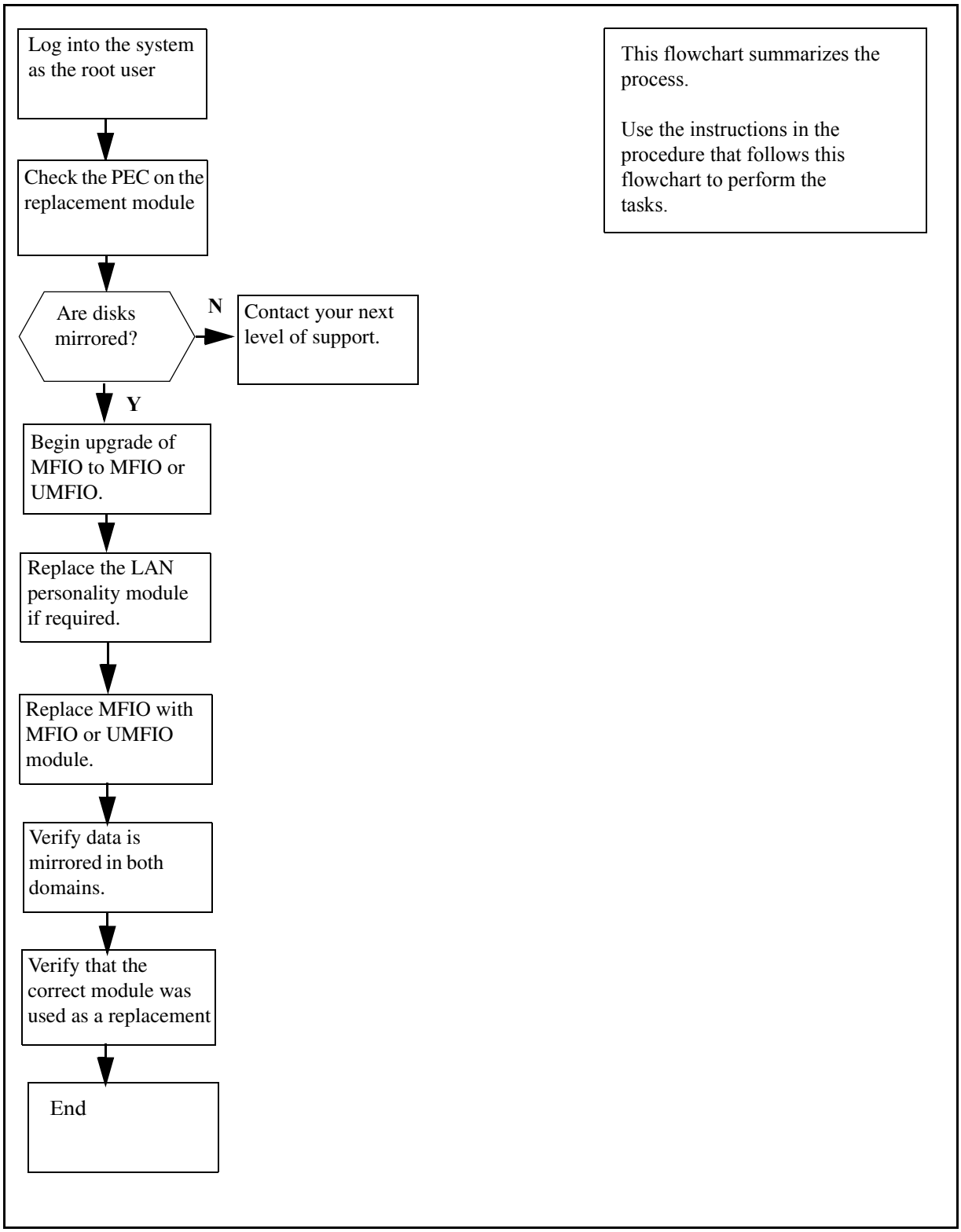
chassis, if there is one. Datavg modules must be upgraded in pairs. For example, if you upgrade the MFIO in slot 4 of the main chassis, you must also upgrade the MFIO module in slot 15 of the main chassis.

| Upgrade Sequence | Domain 0 | Domain 1 | MFIO davavg pairing location |
|---|---|---|---|
| 1 | slot 4 | slot 15 | main chassis |
| 2 | slot 1 | slot 9 | expansion chassis |
| 3 | slot 3 | slot 11 | expansion chassis |
| 4 | slot 5 | slot 13 | expansion chassis |
| 5 | slot 7 | slot 15 | expansion chassis |

## Task flow diagram

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedure that follows the flowchart to perform the tasks.

## Task flow for Upgrading a datavg MFIO to MFIO or UMFIO (datavg)



# Procedure

## Upgrading a datavg MFIO to MFIO or UMFIO

### *At the VT100 console*

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

**2** Check the label on the module that you want to use as a replacement. Make sure that label shows the product engineering code (PEC) that you want to use for your upgrade.

**3** Determine the physical location of the hard disk drives:

```
# locate
```

*Example response*

| Site | Flr | RPos | Bay_id | Shf | Description | Slot | EqPEC |
|---|---|---|---|---|---|---|---|
| HOST | 01 | A02 | CSDM | SDMM | 512(0) | 01 | NTRX50GA FRNT |
| HOST | 01 | A02 | CSDM | SDMM | | 01 | NTRX50FS BACK |
| HOST | 01 | A02 | CSDM | SDMM | ETH(0),DSK1(0),DAT(0) | 02 | NTRX50GN FRNT |
| HOST | 01 | A02 | CSDM | SDMM | | 02 | NTRX50FS BACK |
| HOST | 01 | A02 | CSDM | SDMM | DSK2(0),DSK3(0) | 04 | NTRX50GP FRNT |
| HOST | 01 | A02 | CSDM | SDMM | CPU(0) | 06 | NTRX50FK FRNT |
| HOST | 01 | A02 | CSDM | SDMM | | 06 | NTRX50FD BACK |
| HOST | 01 | A02 | CSDM | SDMM | CPU(1) | 10 | NTRX50FK FRNT |
| HOST | 01 | A02 | CSDM | SDMM | 512(1) | 12 | NTRX50GA FRNT |
| HOST | 01 | A02 | CSDM | SDMM | | 12 | NTRX50GH BACK |
| HOST | 01 | A02 | CSDM | SDMM | ETH(1),DSK1(1),DAT(1) | 13 | NTRX50GN FRNT |
| HOST | 01 | A02 | CSDM | SDMM | | 13 | NTRX50FS BACK |
| HOST | 01 | A02 | CSDM | SDMM | DSK2(1),DSK3(1) | 15 | NTRX50GP FRNT |
| HOST | 01 | A02 | CSDM | SDMM | FAN1(0) | -- | NTRX50FE FRNT |
| HOST | 00 | A02 | CSDM | SDMM | FAN1(1) | -- | NTRX50FF FRNT |
| HOST | 01 | A02 | CSDM | SDME | ICM1(0) | -- | NTRX50FG BACK |
| HOST | 01 | A02 | CSDM | SDME | ICM1(1) | -- | NTRX50FH BACK |
| HOST | 01 | A02 | CSDM | SDME | DSK4(0), DSK5(0) | 01 | NTRX50FU FRNT |

**4** Record the physical location of all hard disk drives in order to avoid removing the wrong drive, and record the chassis, slot, and PEC of the IO module you want to upgrade

*where*

**chassis**
is the chassis where the IO module you want to upgrade is located. The main chassis is identified as ‘sdmm’. The expansion chassis is identified as ‘sdme’. The chassis identifier is displayed under the “Shf” heading in the output from the *locate* command.

**slot**
is the slot number (1-16) in the chassis where the IO module to be upgraded is located. The slot number is

displayed under the “slot” heading in the output from the *locate* command.

**pec**
is the product engineering code for the IO controller module you want to add (either NTRX50NC or NTRX50NL).

***Note:*** Replacements for the NTRX50NC will be filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004, the NTRX50NL will be the replacement for the NTRX50NC.

**5** Ensure that the datavg logical volumes are in sync:

```
# lsvg -l datavg
```

From the output, confirm that all logical volumes have a status of “open/syncd” under column “LV State”, and that each logical volume has “2” physical volumes under column “PVs”.

| If | Do |
|---|---|
| all logical volumes show LV State as “open/syncd” and PVs as “2” | step 6 |
| not all logical volumes show LV State as “open/syncd” or PVs as “2” | contact your next level of support |

**6** Access the storage level:

```
# sdmmtc storage
```

**7** Use the following table to determine your next step.

| If the status of the datavg disks is | Do |
|---|---|
| mirrored | step 8 |
| not mirrored | contact your next level of support |

**8** Access the hardware level:

**> hw**

**9** Upgrade the MFIO:

**> upgrade <chassis> <slot> <pec>**

*where*

**chassis**
is the chassis where the MFIO module to be upgraded is located. The main chassis is identified as ‘sdmm’. The expansion chassis is identified as ‘sdme’.

**slot**
is the slot number (1-16) in the chassis where the MFIO module to be upgraded is located

***Note:*** For slots 1-9 you are not required to enter a 0 (zero) before the slot number. For instance, to enter slot 5, type “5” rather than “05”.

**pec**
is the product engineering code for the MFIO or the UMFIO controller module you want to add (either NTRX50NC or NTRX50NL)

***Note:*** Replacements for the NTRX50NC will be filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004, the NTRX50NL will be the replacement for the NTRX50NC.

**Example**

```
> upgrade sdmm 4 NTRX50NL
```

This example indicates an upgrade to the 36GB + 36GB UMFIO in slot 4 of the main chassis.

| If you are | Do |
|---|---|
| prompted to delete an X.25 interface | step 10 |
| not prompted to deleted an X.25 interface | step 15 |

**10** Confirm the deletion of the X.25 interface:

```
> y
```

**11**

**ATTENTION**

If you wish to continue the upgrade, do not enter 1 at this step of the procedure. Follow the procedure and enter 1 after you have replaced the MFIO.

Wait for the system to generate the following response:

*Example of response*

```
Transitioning forward from START to INFO_RETRIEVED

Volume group = datavg on hdisk4
Physical partition size 16 with max partitions 3048

Volume group = datavg on hdisk5
Physical partition size 16 with max partitions 3048

Transitioning forward from INFO_RETRIEVED to OFFLINED
 Transitioning forward from OFFLINED to DEPENDENCIES_REMOVED
 Transitioning forward from DEPENDENCIES_REMOVED to REPLACED

 Replace ORIGINAL MFIO I/O-1 (c1-f15) with UPGRADED MFIO

 Enter 1 to continue, 99 to exit:
```

| If you want to | Do |
|---|---|
| exit the upgrade | step 12 |
| continue the upgrade | step 13 |

**12** Exit the upgrade:

```
> 99
```

*Response*

*The system gracefully backs you out of the upgrade procedure.*

**13** Begin the replacement of the MFIO. During the upgrade process you may receive the following response:

```
0516-1193 chvg: WARNING, once this operation is
completed, volume group datavg cannot be
imported into AIX 430 or lower versions.
Continue (y/n)?
```

| If you | Do |
|---|---|
| receive the response | step 14 |
| do not receive the response | step 15 |

**14** Confirm the operation:

**> y**

*Example of response*

```
0516-1164 chvg: Volume group datavg changed.
With given characteristics datavg can include up
to 10 physical volumes with 3048 physical
partitions each.
```

***At the front of the CS 2000 Core Manager***

**15**



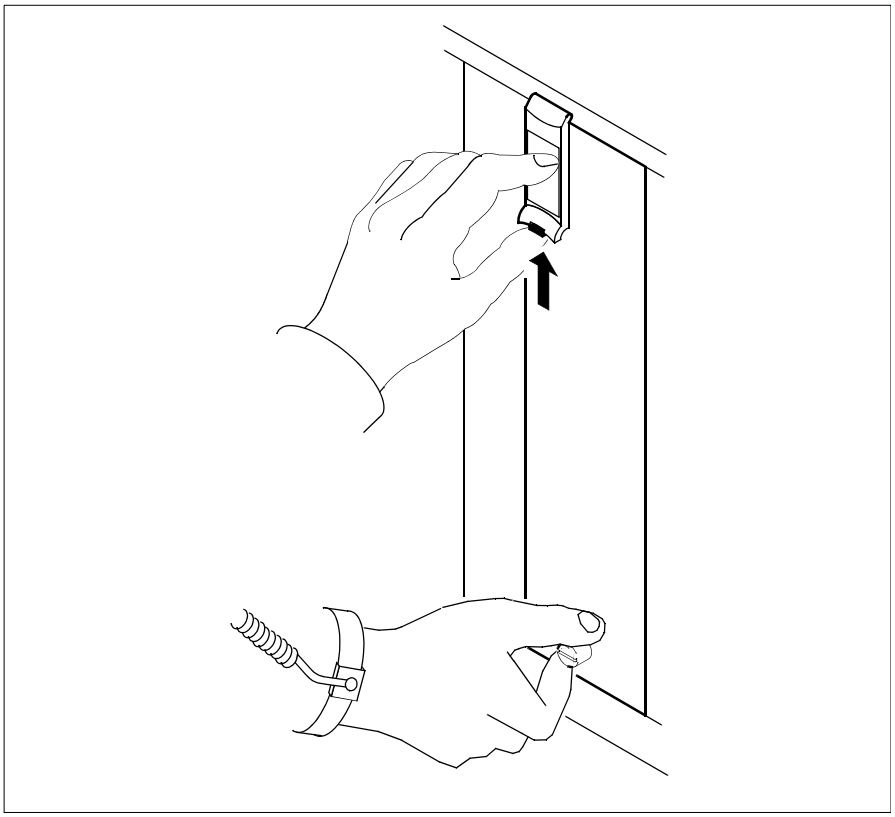
**WARNING**
**Static electricity damage**
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge grounding wrist strap.

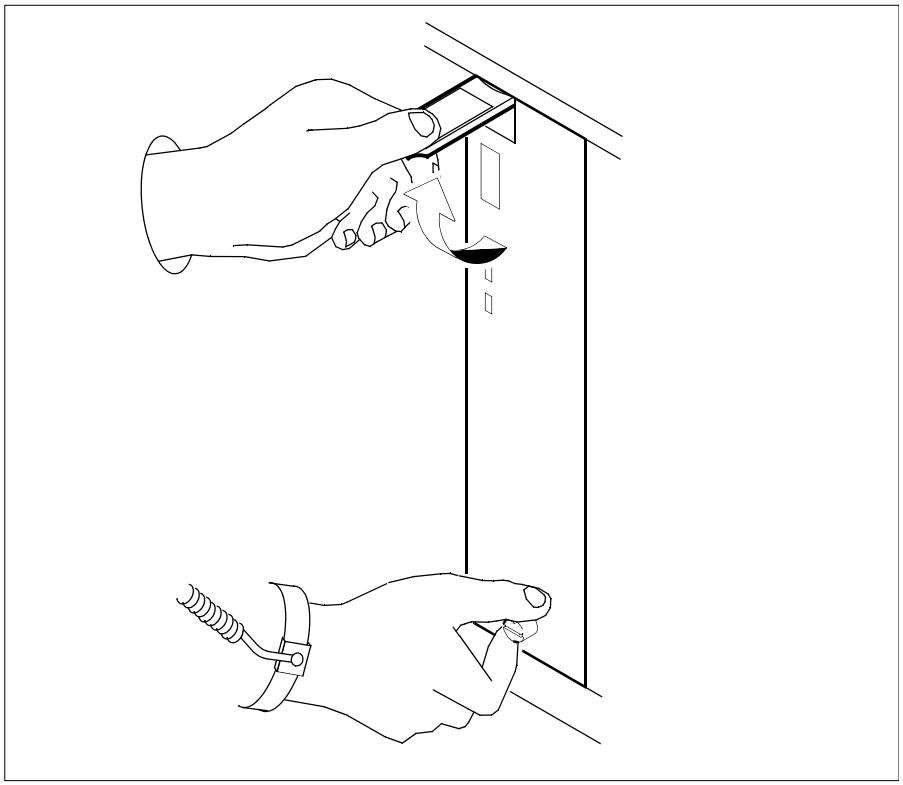
**16** Undo the thumbscrews located on the top and the bottom of the MFIO controller module to be upgraded. The thumbscrews are the captive type, and cannot be removed from the module.

***Note:*** Make sure the LED of the module you want to upgrade is either red or off before you remove it.

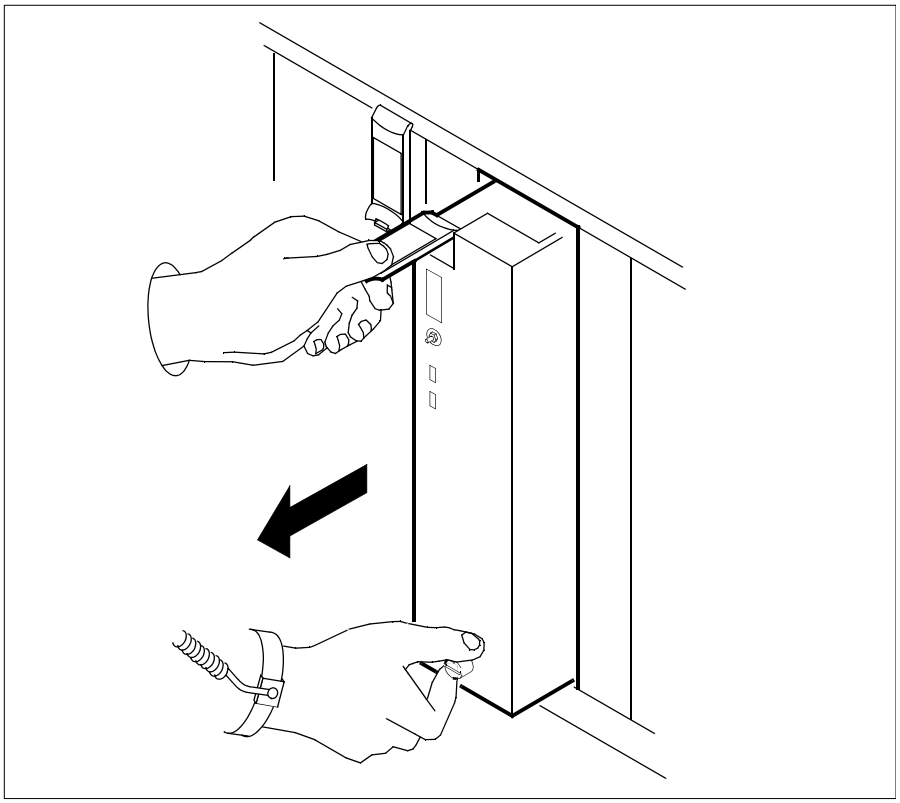
**17** Depress the tip of the locking lever on the face of the MFIO controller module.



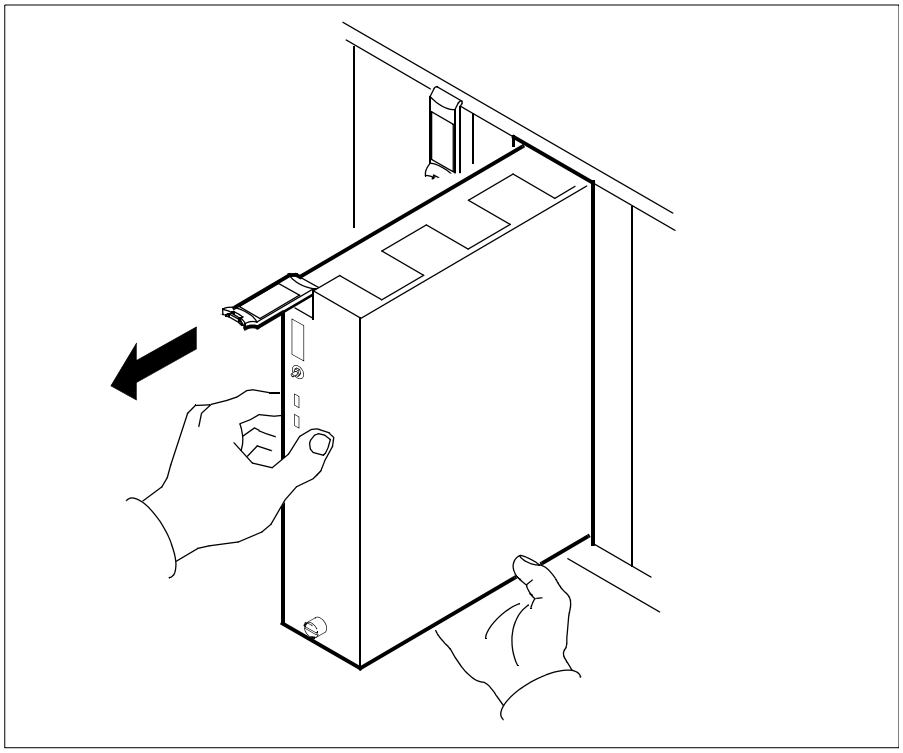
**18** Open the locking lever on the face of the module by moving the lever outwards.



**19** While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the shelf.



**20** Hold the card by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



**21** Place the module you have removed in an ESD protective container.

***At the back of the CS 2000 Core Manager***

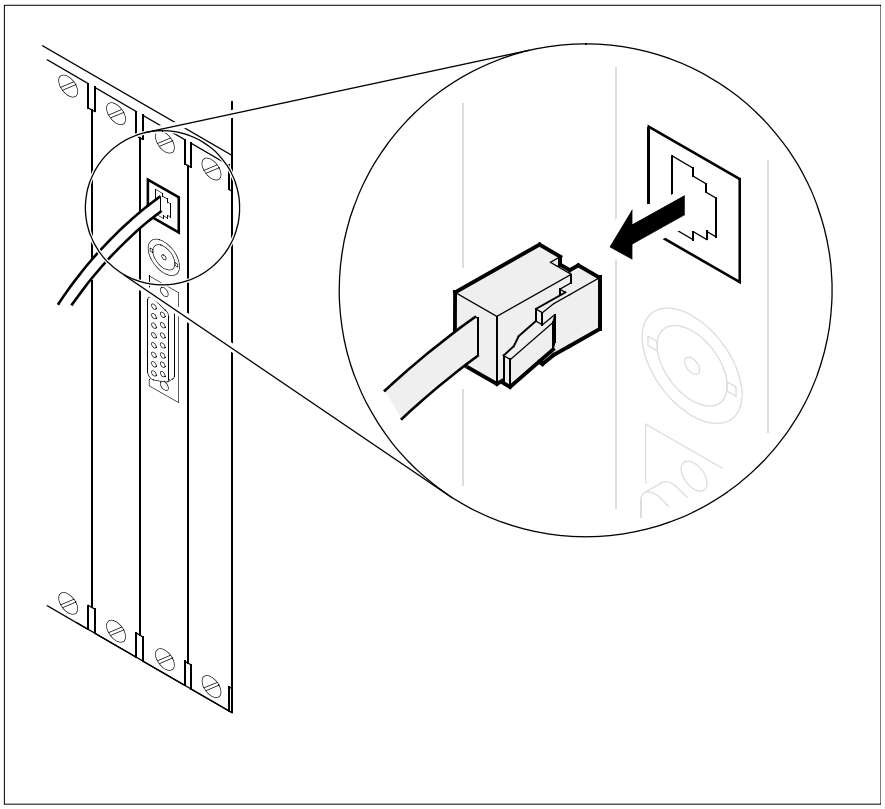
**22** Use the table below to determine your next step.

| If you are | Do |
|---|---|
| upgrading to UMFIO | step 23 |
| not upgrading to UMFIO | step 34 |

**23** You will now be removing the existing LAN personality module and replacing it with the new personality module (NTRX50NK or NTRX50NN) that came with the new UMFIO module. This must be done before inserting the new UMFIO module. It is located at the rear of the I/O controller module to be upgraded.

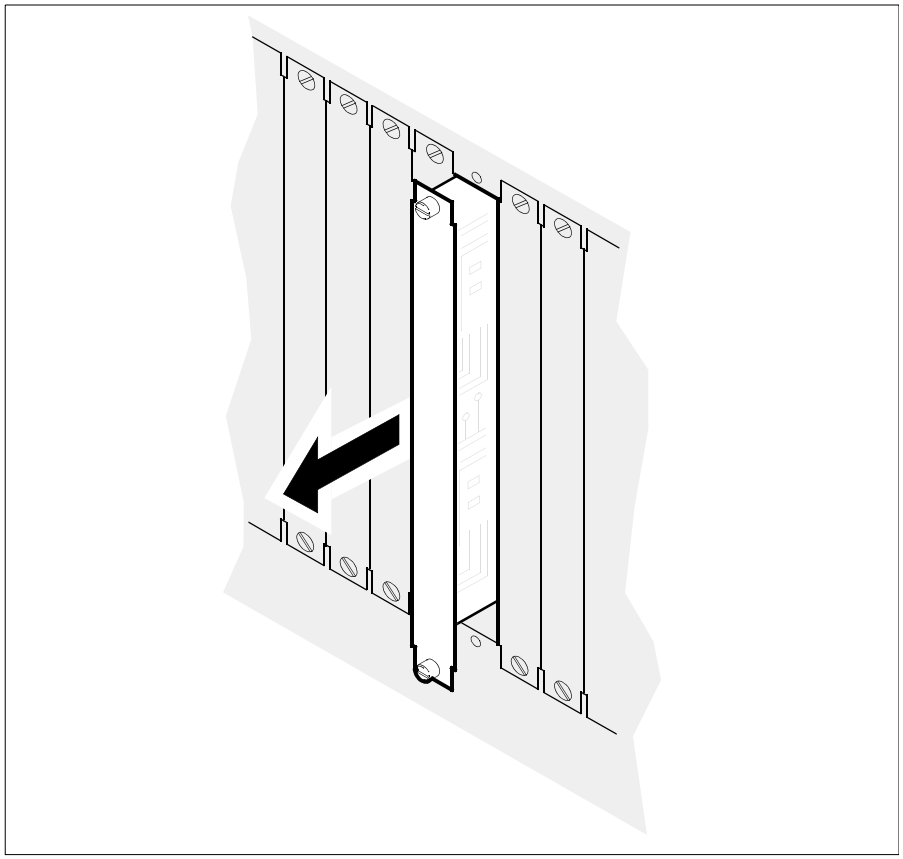
**24** Label the Ethernet cable connected to the LAN personality module you want to replace.

**25** Identify the correct LAN module (slot and PEC code) you wish to remove and disconnect the Ethernet cable, as shown in the following diagram.

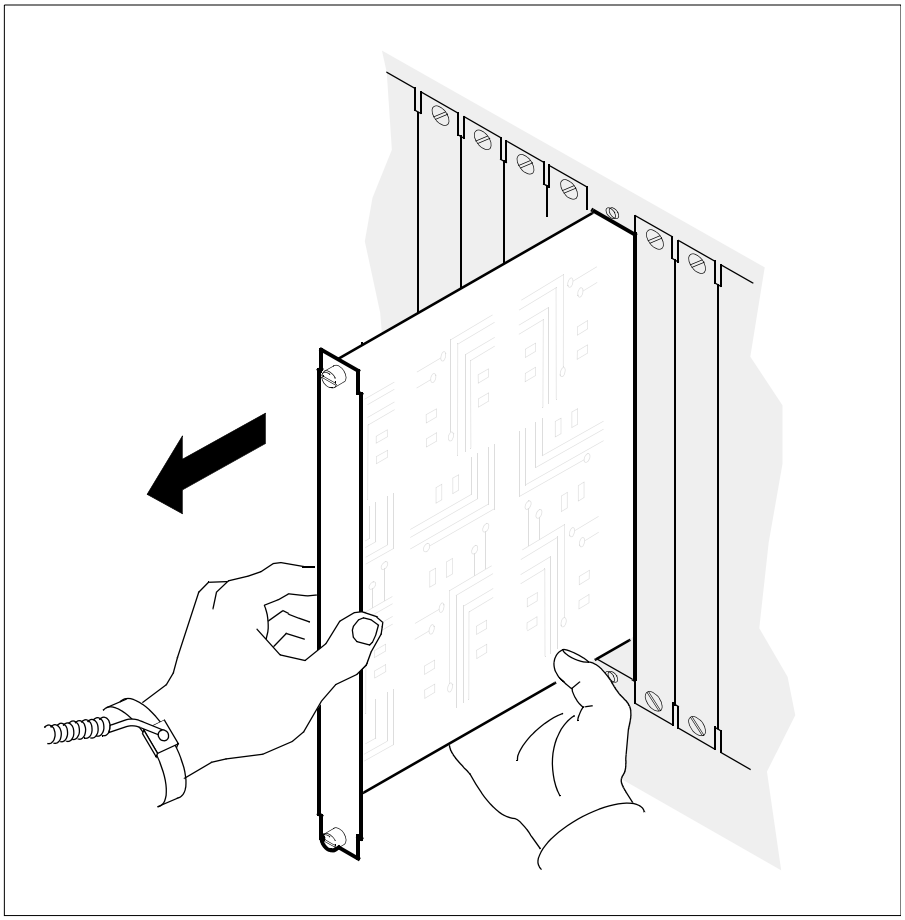


**26** Loosen the two thumbscrews located at the top and the bottom of the LAN personality module. The thumbscrews are the captive type, and cannot be removed from the module.

**27** While grasping the thumbscrews, gently pull the LAN personality module towards you until it protrudes about 2 in. (5 cm) from the shelf.



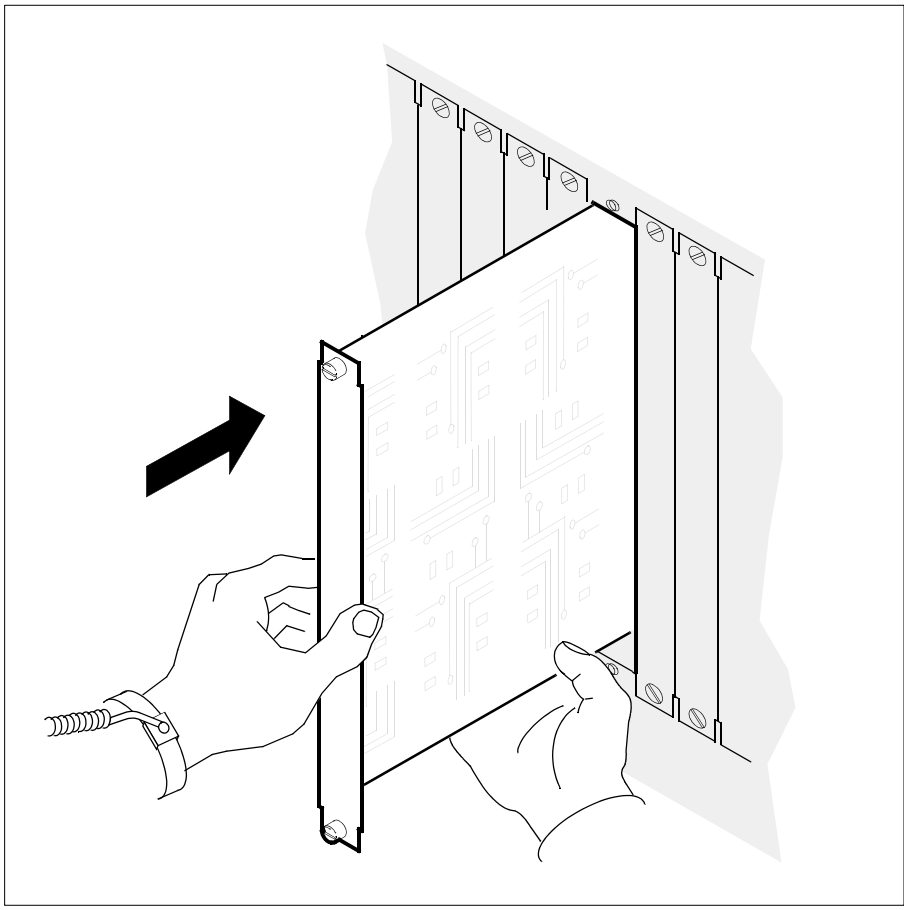
**28** Hold the LAN personality module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



**29** Place the LAN personality module you have removed in an ESD protective container.

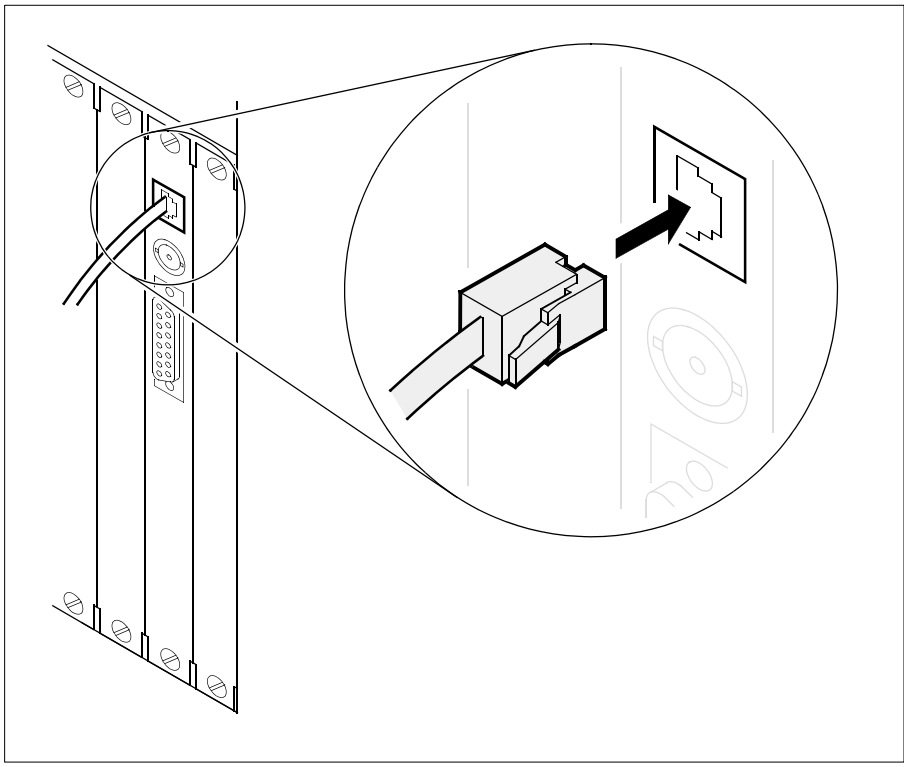
**30** Insert the new LAN personality module (NTRX50NK or NTRX50NN) into the shelf.

**31** Gently slide the LAN personality module into the shelf until it is fully inserted.



**32** Tighten the thumbscrews at the top and the bottom of the LAN personality module.

**33** Reconnect the Ethernet cable to the LAN personality module. You may remove the label you put on the cable in step 24.

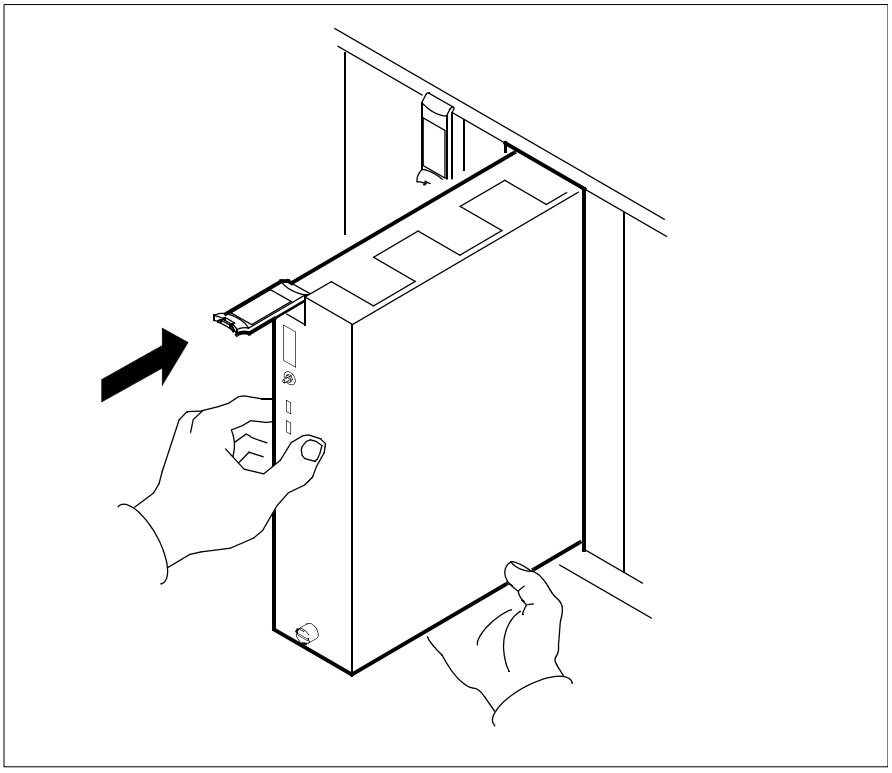


***At the front of the CS 2000 Core Manager***

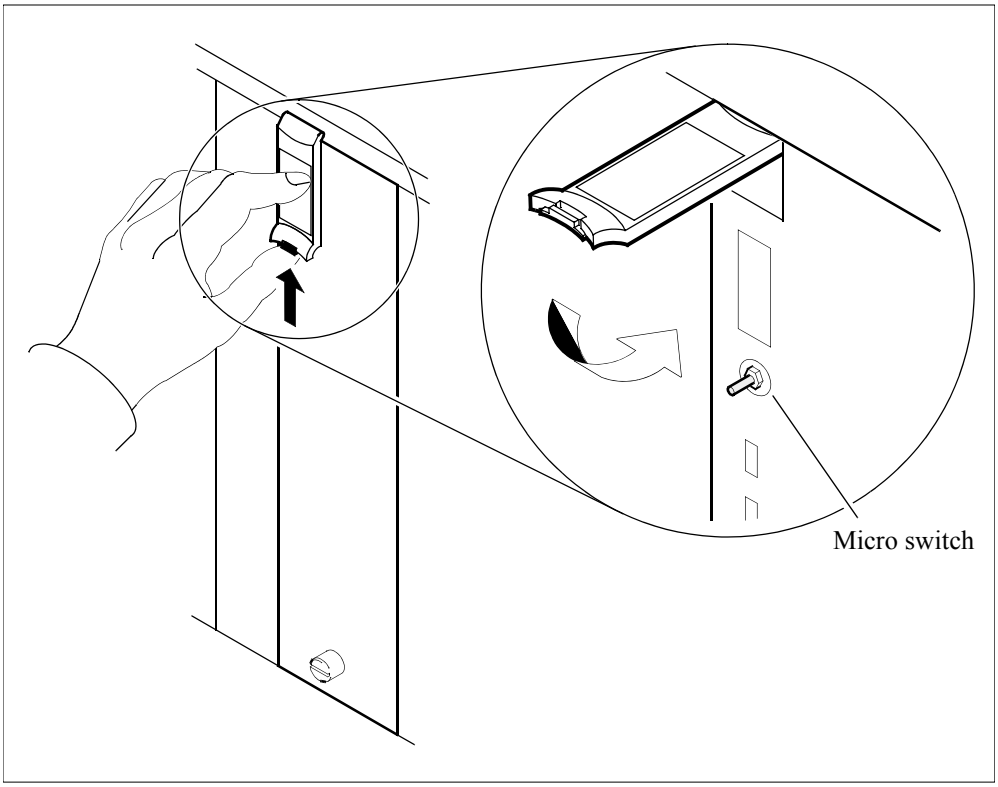
**34** Insert the NTRX50NC MFIO / NTRX50NL UMFIO module into the shelf.

***Note:*** Replacements for the NTRX50NC will be filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004, the NTRX50NL will be the replacement for the NTRX50NC.

**35** Gently slide the module into the shelf until it is fully inserted.



**36** Close the locking lever to secure the module. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.




**37** Tighten the thumbscrews on the module.

**38** Continue the upgrade:

> **1**

*Response*

```
Transitioning forward from REPLACED to ONLINED
Transitioning forward from ONLINED to DEPENDENCIES_ADDED
Transitioning forward from DEPENDENCIES_ADDED to OFFLINED_AFTER_UPGRADE
Transitioning forward from OFFLINED_AFTER_UPGRADE to ONLINED2
Transitioning forward from ONLINED2 to COMPLETE
>
```

**39** You are automatically returned to the sdmmtc Hw level. Wait until the system completes the reintegration.

While the system integrates, you will see the following responses at the hardware menu level and the storage menu levels:

### Hardware menu level

```
          SDM    CON   LAN    APPL    SYS    HW      CLLI : FCC1
           ISTb    .     .      .      ISTb   ISTb    Host : SDM1
                                                     Fault Tolerant

Hw
 0 Quit
 2                          I  I  F  F C E E  D D D D D D 5
 3                          C C  A A  P T T  S  S  S S S  A 1
 4 Logs                      M M N N U H H K K K K K K T 2
 5                         1  2  1 2    1 2 1  2 3 4  5
 6                  Domain 0 .  .  .  .  .  .  I  .  I  I  .  .  .  .
 7 Bsy              Domain 1 .  .  .  .  .  .  I  .  I  I  .  .  .  .
 8 RTS
 9
10
11
12
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh

  root
Time  19:48 >
```

## Storage menu level

```
          SDM    CON   LAN    APPL    SYS    HW       CLLI : FCC1
          ISTb    .      .       .      ISTb   ISTb     Host : SDM1
                                                        Fault Tolerant

Storage
 0 Quit
 2                  Volume Group        Status                Free (MB)
 3                     rootvg           Mirrored              31856
 4                     datavg           Integrating (28%)     43360    !
 5
 6                  Logical Volume      Location     Size(MB) % full/ threshold
 7                        1 /           rootvg        88          11/ 80
 8                        2 /usr        rootvg       600          29/ 90
 9                        3 /var        rootvg       200           5/ 70
10                        4 /tmp        rootvg        24           5/ 90
11                        5 /home       rootvg       304           4/ 70
12 Up                     6 /sdm        rootvg       504          24/ 90
13 Down                   7 /data       datavg       208           5/ 80
14                                                 Logical volumes showing: 1 to 7 of 7
15
16
17 Help
18 Refresh


 root
Time  19:48  >
```

**40** Once the system completes the reintegration, the status of the volume group changes to `Mirrored`.

### Storage menu level

```
          SDM    CON   LAN    APPL    SYS    HW       CLLI : FCC1
            .      .     .       .      .     .        Host : SDM1
                                                      Fault Tolerant

Storage
 0 Quit
 2                  Volume Group        Status          Free (MB)
 3                       rootvg         Mirrored         31856
 4                       datavg         Mirrored         43360
 5
 6                  Logical Volume      Location        Size(MB) % full/ threshold
 7                        1 /            rootvg           88          11/ 80
 8                        2 /usr         rootvg          600          29/ 90
 9                        3 /var         rootvg          200           5/ 70
10                        4 /tmp         rootvg           24           5/ 90
11                        5 /home        rootvg          304           4/ 70
12 Up                     6 /sdm         rootvg          504          24/ 90
13 Down                   7 /data        datavg          208           5/ 80
14                                                 Logical volumes showing: 1 to 7 of 7
15
16
17 Help
18 Refresh


 root
Time  19:48 >
```

**41** Verify that the correct module was used as a replacement:

```
> locate
```

The system displays a list of hardware. Confirm that the correct PEC is listed for the newly upgraded module.

**42** Upgrade the MFIO / UMFIO module in the other domain by repeating steps 1, 2, and 4 through 43 inclusive.

**43** You have completed this procedure.

# Removing SBA NA100 script files

**ATTENTION**
Use this procedure only if you have been directed here from the Preparing to upgrade the CS 2000 Core Manager procedures . Perform this procedure prior to a software upgrade.

As of SDM14, the NA100 version of the SDM billing application was converted to the DMS500 version. During the conversion, NA100 script files were removed with the exception of three NA100 script files.

This procedure provides instructions on how to verify whether the three NA100 script files are present on your system, and how to remove these files if they are present.

## Removing SBA NA100 script files

### *At the CS 2000 Core Manager*

1 Log in to the CS 2000 Core Manager as the root user.

2 Access the directory where SBA script files are located by typing

```
# ls /usr/lpp/SDM_SBA/deinstl
```

and pressing the Enter key.

***Note:*** The last character in the command string is the letter "l".

3 Verify whether the following SDM_SBA.NA100 files are present:

- SDM_SBA.NA100.al
- SDM_SBA.NA100.unconfig
- SDM_SBA.NA100.inventory

| If the NA100 script files | Do |
|---|---|
| are present | step 4 |
| not present | you have completed this procedure and can return to the upgrade procedure that directed you here |

4 Remove each of the NA100 script files by typing

```
# rm SDM_SBA.NA100.al
```

and pressing the Enter key.

```
# rm SDM_SBA.NA100.unconfig
```

and pressing the Enter key.

```
# rm SDM_SBA.NA100.inventory
```

and pressing the Enter key.

| If you | Do |
|---|---|
| could not remove one or more of the NA100 script files | contact your next level of support |
| successfully removed all three NA100 script files | you have completed this procedure and can return to the upgrade procedure that directed you here |

# Upgrading the DS512 controller module from NTRX50GA to GX

## Purpose

Use this procedure to perform the DS512 controller module upgrade from an NTRX50GA to an NTRX50GX module.

The NTRX50GA and NTRX50GX DS512 controller modules function identically. The NTRX50GX DS512 controller module has increased buffer memory with 16 kilobytes per link.

This procedure allows the CS 2000 Core Manager applications to continue without interruption. During this procedure, one of the two DS512 controller modules remains in service while the other is being replaced. The state of applications running on the CS 2000 Core Manager is not a factor in this procedure. However, Nortel Networks recommends that you perform this procedure during a roughage period.

## Prerequisites

The NTRX50GX DS512 controller module requires software version SDMN0010 (or higher).

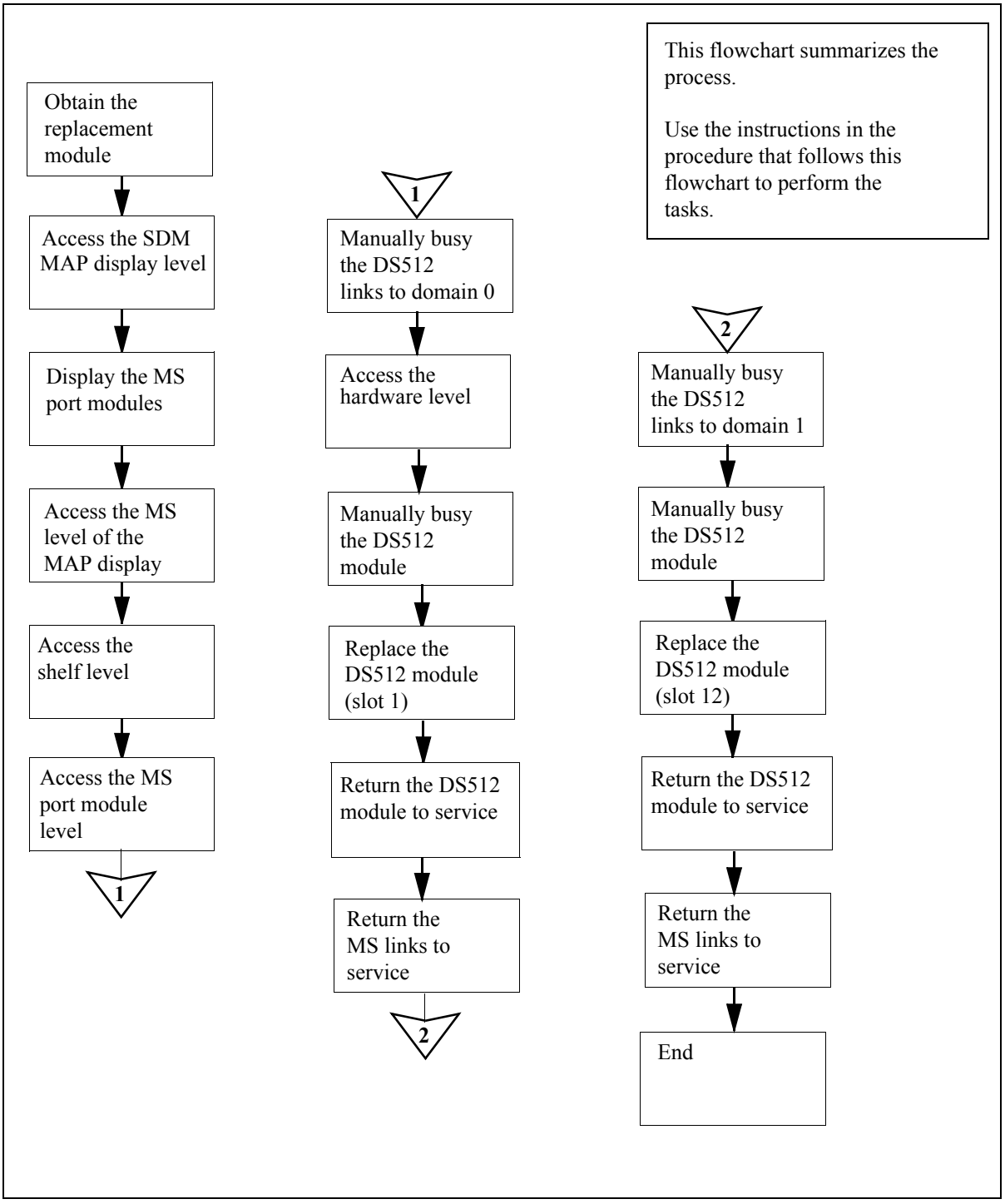
Before you begin this procedure, you must have:

- two NTRX50GX controller modules
- packaging material in which to return the two NTRX50GA controller modules
- login capability for both the DMS MAP and CS 2000 Core Manager

## Task flow diagram

The following task flow diagram provides a summary of the process. To upgrade the DS512 controller module, use the instructions in the procedure that follows the flowchart.

## Task flow for Upgrading the DS512 controller module from NTRX50GA to NTRX50GX



## Upgrading the DS512 controller module

1 Obtain an NTRX50GX DS512 controller module. Make sure that the upgrade module has the correct product engineering code (PEC). The PEC is written on the top locking lever of the module.

***At the MAP display***

2 Access the SDM level:

```
> mapci;mtc;appl;sdm
```

3 Display the card numbers that provide the DS512 links to the CS 2000 Core Manager:

```
> trnsl
```

*Example response*

```
SDM 0 DOMAIN 0 PORT 0 (MS 0:15:0) OK  MsgCnd:Open
SDM 0 DOMAIN 0 PORT 1 (MS 1:15:0) OK  MsgCnd:Open
SDM 0 DOMAIN 1 PORT 0 (MS 0:15:1) OK  MsgCnd:Open
SDM 0 DOMAIN 1 PORT 1 (MS 1:15:1) OK  MsgCnd:Open
```

4 Record the card number associated with the CS 2000 Core Manager DS512 links. The card number is the middle number shown in the parentheses.

***Note:*** In the example response shown in step 3, the card number is 15.

5 Access the MS level of the MAP display:

```
> ms
```

6 Access the shelf level:

```
> shelf
```

7 Access the card number level that is associated with the CS 2000 Core Manager DS512 links:

```
> chain <card_number>
```

*where*

**<card_number>**
is the card number you recorded in step 4.

8 Manually busy the DS512 link between MS plane 0 and the CS 2000 Core Manager DS512 controller module or domain 0:

```
> bsy 0 link 0
```

*Example response:*

```
Request to MAN BUSY MS:0 shelf:0 chain:15 link:0
submitted.
Request to MAN BUSY MS:0 shelf:0 chain:15 link:0
passed.
```

***Note:*** The state for the DS512 link changes to “M" for MS plane 0.

**9** Manually busy the DS512 link between MS plane 1 and the CS 2000 Core Manager DS512 controller module on domain 0:

**> bsy 1 link *0***

*Example response*

```
Request to MAN BUSY MS: 1 shelf: 0 chain:15
link:  0 submitted.
Request to MAN BUSY MS: 1 shelf: 0 chain:15
link: 0 passed.
```

***Note:*** The state for the DS512 link changes to “M" for MS plane 1.

***At the local or remote VT100 console***

**10** Log in to the CS 2000 Core Manager as the root or maint user.

**11** Access the maintenance interface:

**# sdmmtc**

**12** Access the hardware (Hw) level:

**> hw**

**13** Busy the DS512 controller module:

**> bsy 0 512**

| If you are | Do |
|---|---|
| prompted to confirm the busy command | step 14 |
| not prompted to confirm the busy command | step 16 |

**14** Confirm the busy command:

**> y**

***At the front of the CS 2000 Core Manager***

**15**



**WARNING**
**Static electricity damage**
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge (ESD) grounding wrist strap.

**16** Locate the NTGX50GA card in slot 1.

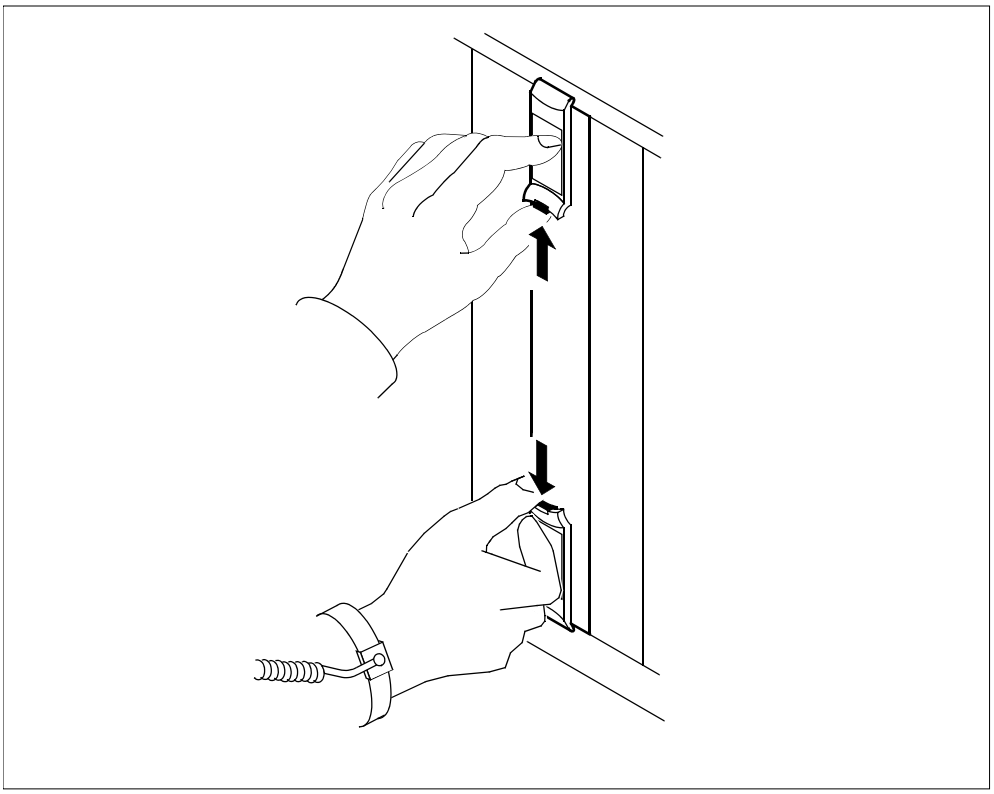
**17**



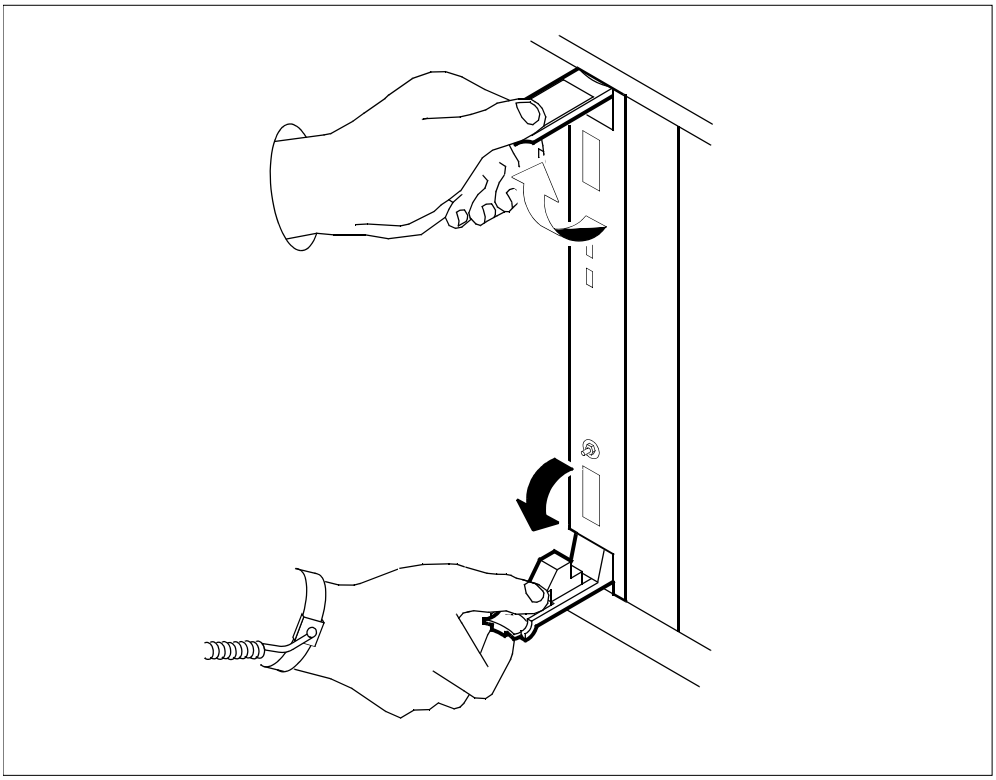
**CAUTION**
**Potential service interruption**
Unseat only the DS512 controller module that you busied, and not the corresponding DS512 controller module in the other I/O domain. The in-service LED on the busied module is off, and the out-of-service LED is on (red). If you remove the remaining in-service DS512 controller module, you will isolate the CS 2000 Core Manager from the computing module (CM).

Undo the thumbscrews located on the top and bottom of the DS512 controller module. The thumbscrews are the captive type, and cannot be removed from the module.

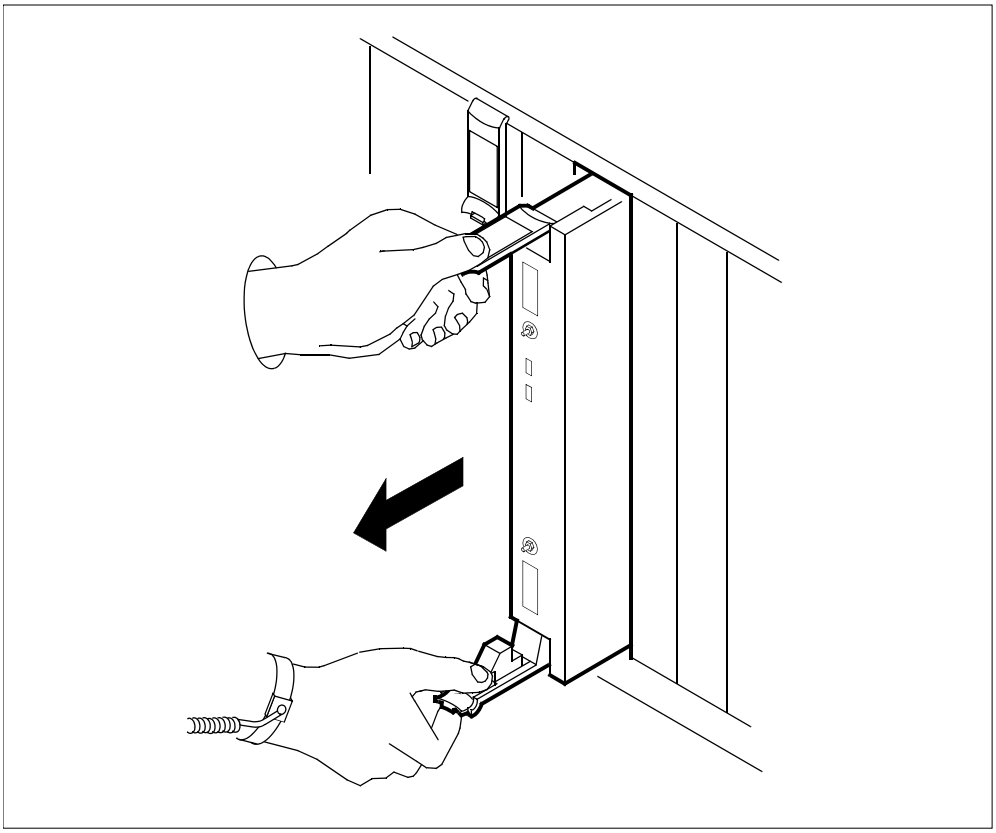
**18** Depress the tips of the locking levers on the face of the DS512 controller module.



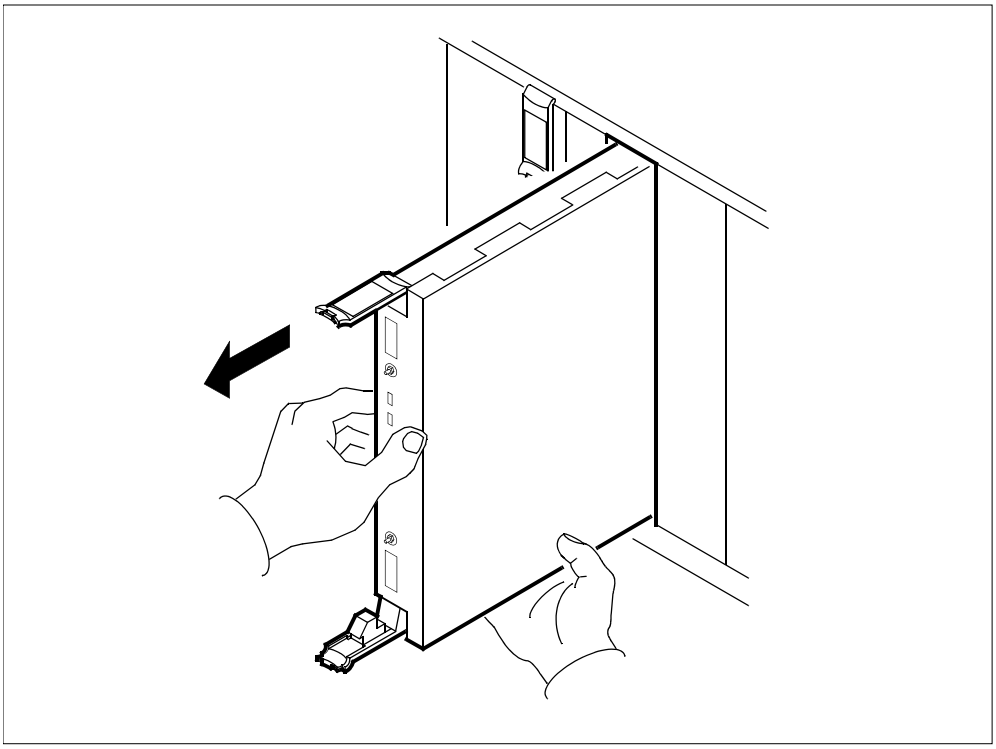
**19** Open the locking levers on the face of the module by moving the levers outwards.



**20** While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



**21** Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



**22** Place the module you have removed in an ESD protective container.

***At the local or remote VT100 console***

**23** Exit the maintenance interface:

```
> quit all
```

**24** For the DS512 module you have removed, delete the information from the CS 2000 Core Manager configuration database:

```
# ftds512clean <n>
```

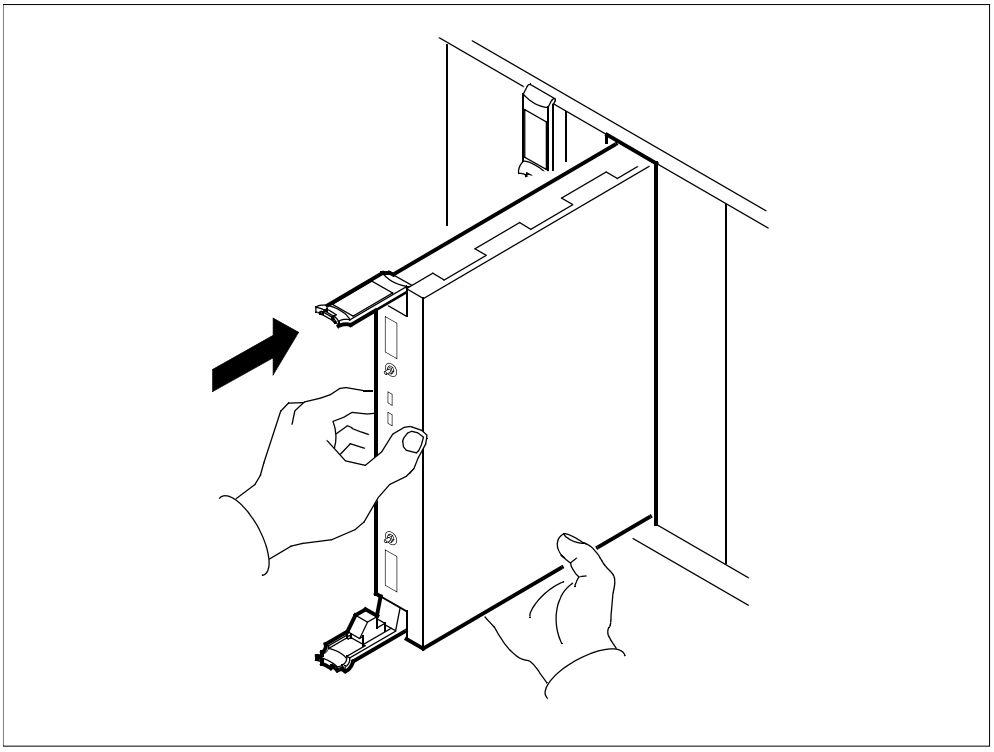
*where*

**<*n*>**
is 0 if the removed module was in domain 0, and 1 for a module that was in domain 1.

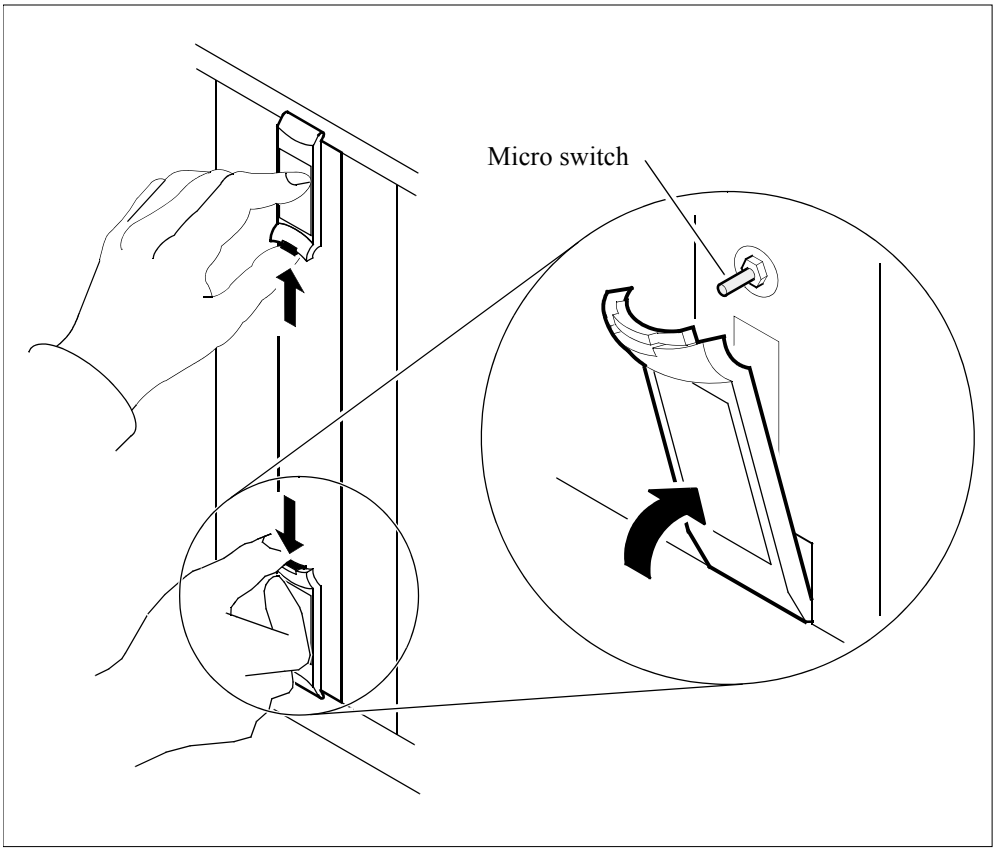
***At the front of the CS 2000 Core Manager***

**25** Insert the replacement module into the CS 2000 Core Manager shelf.

**26** Gently slide the module into the shelf until it is fully inserted.



**27** To seat the module properly, make sure that both the top and bottom micro switches are lined up with the levers. Close the locking levers to secure the module.




**28** Tighten the thumbscrews (if present) on the module. If you are replacing domain 0, proceed to step 29. If you are replacing domain 1, proceed to step 41.

***At the local or remote VT100 console***

**29** Access the maintenance interface:

```
# sdmmtc
```

**30** Access the hardware (Hw) level:

```
> hw
```

**31** Return the DS512 controller module to service:

```
> rts 0 512
```

*Example response*

```
Hardware RTS : Domain 0 Device 512 - Command
initiated.
Please wait...
```

When the RTS command is finished, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then to *complete*.

*Example response*

```
Hardware RTS : Domain 0 Device 512 - Command
complete.
```

***Note:*** At the hardware menu level of the CS 2000 Core Manager maintenance interface, the state of the DS512 controller module changes to a dot (.). This change indicates that the module has returned to service. The in-service LED on the DS512 controller module is on (green).

***At the MAP display***

**32** Access the MS port module level of the MAP display (accessed in step 7). Return to service the DS512 link between MS plane 0 and the DS512 controller module you replaced:

```
> rts 0 link 0
```

*Example response:*

```
Request to RTS MS: 0 shelf: 0 chain:15 link:  0
submitted.
Request to RTS MS: 0 shelf: 0 chain:15 link: 0
passed.
```

***Note:*** The state for the DS512 link changes to a dot (.) if the CS 2000 Core Manager DS512 link is in service. Otherwise, the state for the DS512 link changes to a “P".

**33** Return to service the DS512 link between MS plane 1 and the DS512 controller module you replaced:

```
> rts 1 link 0
```

*Example response:*

```
Request to RTS MS: 1 shelf: 0 chain:15 link:  1
submitted.
Request to RTS MS: 1 shelf: 0 chain:15 link: 1
passed.
```

***Note:*** The state for the DS512 link changes to a dot (.) if the CS 2000 Core Manager DS512 link is in-service. Otherwise, the state for the DS512 link changes to a “P".

**34** You must now replace the second NTRX50GA module with the second NTRX50GX module. Busy the DS512 link between MS plane 0 and the CS 2000 Core Manager DS512 controller module you wish to replace:

```
> bsy 0 link 1
```

*Example response*

```
Request to MAN BUSY MS: 0 shelf: 0 chain:15
link:  0 submitted.
Request to MAN BUSY MS: 0 shelf: 0 chain:15
link: 0 passed.
```

***Note:*** The state for the DS512 link changes to “M" for MS plane 0.

**35** Busy the DS512 link between MS plane 1 and the CS 2000 Core Manager DS512 controller module you wish to replace:

```
> bsy 1 link 1
```

*Example response:*

```
Request to MAN BUSY MS: 1 shelf: 0 chain:15
link:  0 submitted.
Request to MAN BUSY MS: 1 shelf: 0 chain:15
link: 0 passed.
```

***Note:*** The state for the DS512 link changes to “M" for MS plane 1.

***At the local or remote VT100 console***

**36** Busy the DS512 controller module:

```
> bsy 0 512
```

| If you are | Do |
|---|---|
| prompted to confirm the busy command | step 37 |
| not prompted to confirm the busy command | step 39 |

**37** Confirm the busy command:

```
> y
```

### *At the front of the CS 2000 Core Manager*

**38**



**WARNING**
**Static electricity damage**
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge (ESD) grounding wrist strap.

**39** Locate the NTRX50GA card in slot 12.

**40** Replace the NTRX50GA module in slot 12 with the NTRX50GX module. To replace the module in slot 12, use steps 17 to 28, then continue with step 41.

### *At the local or remote VT100 console*

**41** At the hardware level, return the DS512 controller module to service:

```
> rts 1 512
```

*Example response*

```
Hardware RTS : Domain 1 Device 512 - Command
initiated.
Please wait...
```

When the RTS command is finished, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then to *complete*.

*Example response*

```
Hardware RTS : Domain 1 Device 512 - Command
complete.
```

***Note:*** At the hardware level, the state of the DS512 controller module changes to a dot (.). This change indicates that the module has returned to service. The in-service LED on the DS512 controller module is on (green).

### *At the MAP display*

**42** Access the MS port module level of the MAP display (accessed in step 7).

**43** Return to service the DS512 link between MS plane 1 and the DS512 controller module you replaced:

```
> rts 0 link 1
```

*Example response*

```
Request to RTS MS: 0 shelf: 0 chain:15 link:  0
submitted.
Request to RTS MS: 0 shelf: 0 chain:15 link: 0
passed.
```

***Note:*** The state for the DS512 link changes to a dot (.) if the CS 2000 Core Manager DS512 link is in service. Otherwise, the state for DS512 link changes to a “P".

**44** Return to service the DS512 link between MS plane 1 and the DS512 controller module you replaced:

```
> rts 1 link 1
```

*Example response*

```
Request to RTS MS: 1 shelf: 0 chain:15 link:  1
submitted.
Request to RTS MS: 1 shelf: 0 chain:15 link: 1
passed.
```

***Note:*** The state for the DS512 link changes to a dot (.) if the CS 2000 Core Manager DS512 link is in service. Otherwise, the state for DS512 link changes to a “P".

***At the local or remote VT100 console***

**45** Exit the maintenance interface:

```
> quit all
```

**46** Confirm that the new cards are properly installed:

```
> locate
```

The system displays a list of CS 2000 Core Manager hardware. The NTRX50GX module is the hardware in slots 1 and 12.

***Note:*** If the system does not list the NTRX50GX modules, the card(s) may be faulty. Replace the NTRX50GX DS512 controller modules with the original NTRX50GA modules. To replace the modules, return to step 13 of this procedure and reinstall the NTRX50GA DS512 controller modules.

***At the MAP display***

**47** Exit the MAP session:

```
> quit all
```

**48** You have completed this procedure.

# Upgrading DCE

## Purpose

**ATTENTION**

This procedure will upgrade the DCE system files and provide the cell_admin user with sdm_admin sub administrator account access permissions. These permissions allow the cell_admin to default to the sdm_admin user id when prompted elsewhere in SDM upgrade and administration actions. If the cell_admin declines to enter the user id and password in this procedure, the cell_admin user id and password will need to be specified when performing subsequent CS 2000 Core Manager DCE admininstration and upgrade tasks.

Use this procedure to upgrade your Distributed Computing Environment (DCE). For more information about DCE, refer to the following procedures:

- “Creating a DCE user” in *CS 2000 Core Manager Administration and Security*, NN10170-611
- “Configuring an SDM in a DCE cell” in the Configuration Management document
- “Removing an SDM from a DCE cell” in the Configuration Management document
- “Deleting a DCE user” in *CS 2000 Core Manager Administration and Security*, NN10170-611
- “Updating DCE principal names” in *CS 2000 Core Manager Administration and Security*, NN10170-611

# Procedure

## Upgrading DCE

### *At the CS 2000 Core Manager*

**1** Begin the DCE upgrade:

```
# dceupgrade
```

***Note:*** The system displays the status of each step during the DCE upgrade.

*Response*

```
Update mkdce file now...
Stop dce daemons now...
Update rc.dce file and restart the dce daemons
now...
It may take about 3 minutes, please wait...
You are required to login as cell_admin for the
following operations

DCE administrator user ID [cell_admin]:
```

**2** At the prompt, enter the DCE cell_admin user ID.

***Note:*** If you do not have a DCE cell_admin user ID, press the Enter key to accept the default user ID (cell_admin).

*Response*

```
DCE administrator password:
```

**3** At the prompt, enter the password for the DCE cell_admin user ID.

*Response*

```
Update access permission for sdm_admin now...
Dceupgrade command complete
The DCE upgrade is complete.
```

***Note:*** If you did not have a DCE cell_admin user ID and you pressed Enter in the previous step to accept the default DCE user ID, press Enter at the password prompt. The response will indicate that the DCE login failed; however, the DCE upgrade completed correctly and you can continue.

**4** You have completed this procedure.

# Stopping and starting the DDMS proxy

## Application

**ATTENTION**
Use this procedure only if you have been directed here from the Completing the CS 2000 Core Manager upgrade in the Upgrades section. Perform this procedure after a software upgrade.

Use this procedure to stop and start the DDMS proxy on the CS 2000 Management Tools server. The DDMS proxy enables communication between the CS 2000 Management Tools server and the core.

## 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 <IP address>
```

and pressing the Enter key.

where

**IP address**
is the IP address 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 you want to | Do |
|---|---|
| stop the DDMS proxy | step 6 |
| start the DDMS proxy | step 7 |

6 Stop the DDMS proxy by typing

# **/opt/nortel/NTsesm/admin/scripts/ddmsproxy stop**

and pressing the Enter key.

7 Start the DDMS proxy by typing

# **/opt/nortel/NTsesm/admin/scripts/ddmsproxy start**

and pressing the Enter key.

8 You have completed this procedure.

# Stopping and starting the Apache Web Server and Tomcat Servlet Container

## Application

**ATTENTION**
Use this procedure only if you have been directed here from the Completing the CS 2000 Core Manager upgrade in the Upgrades section. Perform this procedure after a software upgrade.

Use this procedure to stop and start the Apache Web Server and Tomcat Servlet Container components 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 <IP address>
```

and pressing the Enter key.

where

**IP address**
is the IP address 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 you want to | Do |
|---|---|
| stop the Apache web server and Tomcat servlet container | step 6 |
| start the Apache web server and Tomcat servlet container | step 7 |

6 Stop the Apache Tomcat component by typing

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

and pressing the Enter key.

7 Start the Apache Tomcat component by typing

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

and pressing the Enter key.

8 You have completed this procedure.

# Completing the IW-SPM IP upgrade

## Post upgrade or downgrade process

Perform this procedure after the entire office upgrade or downgrade is completed. The process consists of:

- dumping an image to disk after completing maintenance shift upgrade or downgrade activities
- deleting the old file names from the PMLOADS table
- deleting the old load and patch files from disk volumes

The Variable Abbreviations table defines the variables used in this procedure.

**Table 1 Variable Abbreviations**

| Abbreviation | Definition |
|---|---|
| load_name | the name of the old load (as it appears in the PMLOADS table) |
| disk_vol | the name of the backup disk volume |
| act_load | the name of the new active load (as it appears in the PMLOADS table) |

### Post upgrade or downgrade process

***At MAP level***

**1** Access the PMLOADS table by typing

```
>TABLE PMLOADS
```

**2** Position on each old load name designated for deletion in the PMLOADS table by typing

```
>POS load_name
```

*Example*

```
>POS GEM19AF
```

**3** Initiate the tuple deletion by typing

```
>DEL
```

**4** At the confirmation prompt, delete the tuple by typing

```
>Y
```

5 Access the disk utility by typing

**>DISKUT**

*Response*

```
Disk utility is now active
```

6 List the active PMLOADS volume by typing

**>LF disk_vol**

*Example*

**>LF F0LPMLOADS**

7 Delete each load file from the active disk volume by typing

**>DDF act_load**

*Example*

**>DDF CEM19CD_010064A1**

8 List the loads on the active volume to ensure that all loads have been deleted by repeating step 6.

Follow step 7 for any files that have not been deleted.

9 Repeat step 1 through step 7 for the backup and patch volumes.

When all active, backup, and patch files have been deleted, continue to step 10.

10 Quit the disk utility by typing

**>QUIT**

11 Store an image of the completed upgrade or downgrade to a disk volume by typing

**DUMP act_file image_vol ACTIVE RETAIN NOSDM**

*Example*

**>DUMP DSP16AF_010005 S00DIMAGE ACTIVE RETAIN NOSDM**

***Note:*** The route action to turn off SDM spooling option (nosdm) reduces CI lockout time. Without specifying a route action, the default value is leave SDM spooling on (usesdm).

12 The process is completed.

# Completing the CS 2000 Management Tools upgrade

The supported upgrade paths to the (I)SN07 release are listed below. Follow the link associated with the release you upgraded from.

- Completing the upgrade from (I)SN05 to (I)SN07 on page 1549
- Completing the upgrade from (I)SN06 to (I)SN07 on page 1551
- Completing the upgrade from (I)SN06.2 to (I)SN07 on page 1553

## Completing the upgrade from (I)SN05 to (I)SN07

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

**(I)SN05 to (I)SN07 Post-upgrade checklist**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Re-configure DCE (Distributed Computing Environment).<br><br>***Note:*** Only perform this activity if DCE is used as an authentication mechanism. | | Perform procedure Unconfiguring DCE on an SSPFS-based server on page 1555. |
| | | | Perform procedure Configuring DCE on an SSPFS-based server on page 1559. |
| 2 | Configure the Apache Server<br><br>***Note:*** Only perform this activity if STORage Management (STORM) units are configured in your network. | | Perform procedure Configuring the Apache Web Server for HTTPS proxy on page 1566. |
| 3 | Set up users with user group access. | | Perform procedure Setting up local user accounts on an SSPFS-based server on page 1569. |

## (I)SN05 to (I)SN07 Post-upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 4 | Configure the NPM for automatic patch file delivery.<br><br>***Note:*** Only perform this activity if you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS). | | Perform procedure Configuring NPM for automatic patch file delivery on page 1580. |
| 5 | Restore NPM data. | | Perform procedure Restoring NPM data on page 1584. |
| 6 | Install the QCA software package on a separate server.<br><br>***Note:*** This activity is optional if you want redundancy. You must have another server that is running the (I)SN07 release of SSPFS. | | Perform procedure Installing the QCA software package on a separate server on page 1589. |
| 7 | Configure the APS SNMP agent. | | Perform procedure Configuring the SNMP agent on page 1591. |
| 8 | Verify the upgrade was successful. | | Perform procedure Verifying the upgrade was successful on page 1597. |
| 9 | Back up the (I)SN07 CS 2000 Management Tools server. | | Perform procedure Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater on page 265. |
| | | | Perform procedure Performing a full backup of file systems - (I)SN06.2 or greater on page 271. |
| | | | Perform procedure Performing a backup of APS audio files to tape - Sun t1400 on page 289 or Performing a backup of APS audio files to CD/DVD - Sun Netra 240 on page 291. |
| 10 | Upgrade the next component in the end-to-end upgrade. | | Refer back to End-to-end upgrade overview on page 1. |

# Completing the upgrade from (I)SN06 to (I)SN07

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

### (I)SN06 to (I)SN07 Post-upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Re-configure DCE (Distributed Computing Environment).<br><br>***Note:*** Only perform this activity if DCE is used as an authentication mechanism. | | Perform procedure Unconfiguring DCE on an SSPFS-based server on page 1555. |
| | | | Perform procedure Configuring DCE on an SSPFS-based server on page 1559. |
| 2 | Configure the Apache Server<br><br>***Note:*** Only perform this activity if STORage Management (STORM) units are configured in your network. | | Perform procedure Configuring the Apache Web Server for HTTPS proxy on page 1566. |
| 3 | Set up users with user group access.<br><br>***Note:*** Only perform this activity if you are adding new users. Existing users are maintained over the upgrade. | | Perform procedure Setting up local user accounts on an SSPFS-based server on page 1569. |
| 4 | Configure the NPM for automatic patch file delivery.<br><br>***Note:*** Only perform this activity if you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS). | | Perform procedure Configuring NPM for automatic patch file delivery on page 1580. |
| 5 | Restore NPM data. | | Perform procedure Restoring NPM data on page 1584. |

## (I)SN06 to (I)SN07 Post-upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 6 | Intall the QCA software package on a separate server.<br><br>***Note:*** This activity is optional if you want redundancy. You must have another server that is running the (I)SN07 release of SSPFS. | | Perform procedure Installing the QCA software package on a separate server on page 1589. |
| 7 | Configure the APS SNMP agent. | | Perform procedure Configuring the SNMP agent on page 1591. |
| 8 | Verify the upgrade was successful. | | Perform procedure Verifying the upgrade was successful on page 1597. |
| 9 | Back up the (I)SN07 CS 2000 Management Tools server. | | Perform procedure Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater on page 265. |
| | | | Perform procedure Performing a full backup of file systems - (I)SN06.2 or greater on page 271. |
| | | | Perform procedure Performing a backup of APS audio files to tape - Sun t1400 on page 289 or Performing a backup of APS audio files to CD/DVD - Sun Netra 240 on page 291. |
| 10 | Upgrade the next component in the end-to-end upgrade. | | Refer back to End-to-end upgrade overview on page 1. |

# Completing the upgrade from (I)SN06.2 to (I)SN07

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist , and place a check (√) in the √column as you complete each procedure.

***Note:*** The activities that follow apply to Sun Netra t1400, Sun Netra 240 one-server, and Sun Netra 240 two-server configurations except where indicated.

### (I)SN06.2 to (I)SN07 Post-upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Re-configure DCE (Distributed Computing Environment).<br><br>***Note:*** Only perform this activity if DCE is used as an authentication mechanism. | | Perform procedure Unconfiguring DCE on an SSPFS-based server on page 1555. |
| | | | Perform procedure Configuring DCE on an SSPFS-based server on page 1559. |
| 2 | Configure the Apache Server<br><br>***Note:*** Only perform this activity if STORage Management (STORM) units are configured in your network. | | Perform procedure Configuring the Apache Web Server for HTTPS proxy on page 1566. |
| 3 | Set up users with user group access.<br><br>***Note:*** Only perform this activity if you are adding new users. Existing users are maintained over the upgrade. | | Perform procedure Setting up local user accounts on an SSPFS-based server on page 1569. |
| 4 | Configure the NPM for automatic patch file delivery.<br><br>***Note:*** Only perform this activity if you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS). | | Perform procedure Configuring NPM for automatic patch file delivery on page 1580. |

## (I)SN06.2 to (I)SN07 Post-upgrade checklist

| | Activities | √ | Procedures |
|---|---|---|---|
| 5 | Restore NPM data. | | Perform procedure Restoring NPM data on page 1584. |
| 6 | Intall the QCA software package on a separate server.<br><br>***Note:*** This activity is optional if you want redundancy. You must have another server that is running the (I)SN07 release of SSPFS. | | Perform procedure Installing the QCA software package on a separate server on page 1589 |
| 7 | Configure the APS SNMP agent. | | Perform procedure Configuring the SNMP agent on page 1591. |
| 8 | Verify the upgrade was successful. | | Perform procedure Verifying the upgrade was successful on page 1597. |
| 9 | Back up the (I)SN07 CS 2000 Management Tools server.<br><br>***Note:*** It is not necessary to perform this activity in a two-server configuration. | | Perform procedure Performing a data backup on an SSPFS-based server: (I)SN06.2 or greater on page 265. |
| | | | Perform procedure Performing a full backup of file systems - (I)SN06.2 or greater on page 271. |
| | | | Perform procedure Performing a backup of APS audio files to tape - Sun t1400 on page 289 or Performing a backup of APS audio files to CD/DVD - Sun Netra 240 on page 291. |
| 10 | Upgrade the next component in the end-to-end upgrade. | | Refer back to End-to-end upgrade overview on page 1. |

# Unconfiguring DCE on an SSPFS-based server

## Application

Use this procedure to unconfigure the Distributed Computing Environment (DCE) on a Succession Server Platform Foundation Software (SSPFS)-based server following an SSPFS software upgrade. Only perform this procedure if DCE is used as an authentication mechanism. As of (I)SN05, DCE is not required for all systems, therefore, if your system does not have DCE, you do not need to perform this procedure.

## Prerequisites

You need the DCE cell administrator password.

## 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 that uses DCE as an authentication method

**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 “DCE Configuration” option in the menu.

*Example response*

```
DCE Configuration
 1 - dce_conf <Configure the DCE Client>
 2 - dce_unconf <Unconfigure the DCE Client>

 X - exit

select -
```

**8** Enter the number next to the “dce-unconf” option in the menu.

*Example response*

```
=== Executing "dce_unconf"
Gathering current configuration information...
Enter password for principal cell_admin:
```

**9** Enter the cell administrator password and press the Enter key.

*Example response*

```
Start of DCE Host, znc0s0jy, will now begin.
RPC is already running.
The Security client is already running.
The Directory client is already running.


Unconfiguration of DCE Host, znc0s0jy, will now
begin.
Unconfiguring the DTS client...
Stopping the DTS client...
The DTS client was stopped successfully.
The DTS client will be completely unconfigured
when RPC is unconfigured.
Unconfiguration of this component has been
successful so far.
Unconfiguring the Directory client...
Stopping the Directory client...
The Directory client was stopped successfully.
```

```
The Directory client was unconfigured
successfully.

Unconfiguring the Security client...

Stopping the Security client...

The Security client was stopped successfully.

The Security client was unconfigured
successfully.

Unconfiguring RPC...

Stopping RPC...

RPC was stopped successfully.

RPC was unconfigured successfully.

Gathering component state information...


      Component Summary for Host: znc0s0jy
 Component   Configuration State   Running State

No DCE components are configured.

Unconfiguration of DCE Host, znc0s0jy, was
successful.

Unconfiguration completed successfully.

done unconfiguring DCE

=== "dce_unconf" completed successfully
```

**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.

# Configuring DCE on an SSPFS-based server

## Application

Use this procedure to configure the Distributed Computing Environment (DCE) on a Succession Server Platform Foundation Software (SSPFS)-based server following an SSPFS upgrade. Only perform this procedure if DCE is used as an authentication mechanism.

As of (I)SN05, DCE is not required for all systems, therefore, if your system does not have DCE, you do not need to perform this procedure.

## Prerequisites

This procedure has the following prerequisites:

- unconfigure DCE if DCE was configured prior to upgrading the SSPFS - refer to procedure Unconfiguring DCE on an SSPFS-based server on page 1555 in this document, if required
- obtain the following information
  - the DCE cell name for your customer-provided DCE cell

    ***Note:*** This should be the same DCE cell that contains the core manager.

  - the host name or IP address of the DCE Master Security Server (MSS)
  - the host name or IP address of the DCE Cell Directory Server (CDS)
  - the DCE cell administrator password.
  - the host name or IP address of the DCE Time Server (DTS)

## 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 that uses DCE as an authentication method

**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 “DCE Configuration” option in the menu.

*Example response*

```
DCE Configuration
 1 - dce_conf <Configure the DCE Client>
 2 - dce_unconf <Unconfigure the DCE Client>


 X - exit

select -
```

**8** Enter the number next to the “dce-conf” option in the menu.

*Example response*

```
DCE Cell Name(default:)
```

**9** Enter the DCE Cell Name.

*Example response*

```
Master Security Server Name(default:)
```

**10** Enter the host name or IP address of the MSS.

*Example response*

```
Time Server Name(default:)
```

**11** Enter the host name or IP address of the DTS.

*Example response*

```
CDS Server Name(default:)
```

**12** Enter the host name or IP address of the CDS

*Example response*

```
You have selected to configure your DCE
environment as the following:
Host Name                          : znc0s0jx
DCE Cell Name                      :
rtpptm.sdm.nortel.com
Time Server Name                   : wnc0s0j8
Master Security Server Host Name : wnc0s0j8
CDS Server Host Name               : wnc0s0j8
Continue with configuration?(default:Y[Y/N]
```

**13** Continue the configuration by typing

**y**

and pressing the Enter key.

*Example response*

```
Synchronizing time with wnc0s0j8......

Tue Apr 16 15:00:47 2002

done synchronizing time with wnc0s0j8(0)

Configuring DCE.............................

Default DCE configuration timeout value
successfully changed.

Gathering current configuration information...

Enter password for principal cell_admin:
```

**14** Enter the cell administrator password and press the Enter key.

*Example response*

```
Configuration of DCE Host, znc0s0jx, will now
begin.

Configuring RPC...

Starting RPC...

RPC was started successfully.

RPC configuration is complete.

Configuring the Security client...

Information from the /etc/krb5.conf.backup file
may need to be manually merged into the
/etc/krb5.conf file.

Starting the Security client...

The Security client was started successfully.

Security client configuration is complete.

Configuring the Directory client...

Starting the Directory client...

Waiting up to 10 minutes for the directory
server.

Contacted the directory server.

The Directory client was started successfully.
```

```
Waiting up to 10 minutes for DCED registration
to be functional.
Directory client configuration is complete.
Configuring the DTS client...
Starting the DTS client...
The DTS client was started successfully.
DTS client configuration is complete.
Gathering component state information...

Component Summary for Host: znc0s0jx
Component    Configuration State   Running State
Security client      Configured         Running
RPC                 Configured         Running
Directory client     Configured         Running
DTS client           Configured         Running

The component summary is complete.
Configuration of DCE Host, znc0s0jx, was
successful.
Configuration completed successfully.
done configuring DCE
Gathering current configuration information...
Configuration of DCE Host, znc0s0jx, will now
begin.
There are no components in the request that need
to be configured.
Gathering component state information...

Component Summary for Host: znc0s0jx
Component    Configuration State   Running State
Security client      Configured         Running
RPC                 Configured         Running
Directory client     Configured         Running
```

```
DTS client          Configured          Running


The component summary is complete.

Configuration of DCE Host, znc0s0jx, was
successful.

Configuration completed successfully.

=== "dce_conf" completed successfully
```

**15** 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.

**16** You have completed this procedure.

# Configuring the Apache Web Server for HTTPS proxy

## Application

Use this procedure to configure the Apache Web Server for HTTPS proxy.

***Note:*** You can provision a maximum of 6 IP addresses for use in HTTPS proxy.

**ATTENTION**
Only perform this procedure if STORage Management (STORM) units are configured in your network. If Session Server units are configured in your network, refer to the Session Server Security and Administration document, NN10346-611 for a detailed procedure on configuring a web proxy.

## Prerequisites

None

## 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 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 -
```

**3** 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 -
```

**4** Enter the number next to the “Apache Proxy Configuration” option in the menu.

*Example response*

```
Apache Proxy Configuration
 1 - add_proxy_conf (Add an IP to the Apache
     Proxy Module configuration)
 2 - del_proxy_conf (Delete an IP from the
     Apache Proxy Module configuration)
 3 - list_proxy_conf (List the Apache Proxy
     Module configuration)

 X - exit

select -
```

5 Enter the number next to the “add_proxy_conf” option in the menu.

6 When prompted, enter the proxy IP address.

7 When prompted, enter the hostname associated with the IP address you just entered

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.

# 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 1569).

**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 1569 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 on page 1571
- Carrier provisioning operations on page 1573
- Audit operations on page 1573
- Alarm operations on page 1574
- Internet transparency operations on page 1574
- Trunk provisioning operations on page 1574
- Trunk maintenance operations on page 1575
- ADSL provisioning operations on page 1575
- Line provisioning operations on page 1576
- Line maintenance operations on page 1576
- V5.2 provisioning operations on page 1577
- Patching operations on page 1577


### 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 1569) 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.

# Configuring NPM for automatic patch file delivery

## Application

Use this procedure to configure the Network Patch Manager (NPM) for automatic patch file delivery, which consists of enabling the Patch File Receipt System (PFRS). When the PFRS is enabled, patches are automatically delivered to the NPM database and retrieved for processing on a daily basis.

Options are provided to disable the PFRS, retrieve patches and generate reports on demand, and view the settings of the PFRS when it is already enabled.

## Prerequisites

To enable the PFRS, you need the following information:

- the CLLI ID of the Communication Server 2000 associated with the office - You can obtain the CLLI ID from table OFCENG on the Communication Server 2000. Use the POS (position) command to locate the OFFICE_CLLI_NAME tuple. The value of this tuple, is the CLLI ID.
- the hostname or IP address of the patch file drop-off server
- the user ID and password to connect to the patch file drop-off server

## 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 the NPM software resides

**2** When prompted, enter your user ID and password.

**3** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

**4** When prompted, enter the root password.

**5** Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

*Example response*

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

 X - exit

select -
```

**6** Enter the number next to the “Configuration” option in the menu.

*Example response*

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit

Select -
```

**7** Enter the number next to the “Succession Element Configuration” option in the menu.

*Example response:*

```
Succession Element Configuration
 1 - NPM Application Configuration
 2 - SESM Application Configuration
 3 - SAM21EM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH Application Configuration


 X - exit

select -
```

**8** Enter the number next to the “NPM Application Configuration” option in the menu.

*Example response:*

```
NPM Application Configuration
  1 - PFRS (Patch File Receipt System
      Configuration (PFRS))
  2 - CreateDB (Initialize or re-initialize the
      NPM database)
  3 - ConfigureNpm (Configure the Network Patch
      Manager)

  X - exit

select -
```

**9** Enter the number next to the “PFRS” option in the menu.

*Example response:*

```
===Executing “PFRS”

PFRS Configuration
1 - View
2 - Enable/Reconfigure
3 - Disable
4 - Patch retrieval (Now)
5 - Generate Report (Now)
```

**10** Enter the number next to the “Enable/Reconfigure” option in the menu.

**11** When prompted, enter the CLLI ID of the Communication Server 2000 associated with the office (see Prerequisites on page 1580 at the beginning of this procedure).

**12** When prompted, enter the host name or IP address of the drop-off server where patch files are to be delivered.

**13** When prompted, enter the user ID that will be used to connect to the drop-off server.

***Note:*** The user ID must have read, write, and overwrite privileges in the FTP user's default directory on this server.

**14** When prompted, enter the password associated with the user ID that will be used to connect to the drop-off server.

**15** When prompted, enter the time at which patch files are to be retrieved from the drop-off server.

***Note:*** You can retrieve patches at any time using option 4, "Patch retrieval (Now)", in the PFRS Configuration menu.

**16** When prompted, enter the time at which you would like reports to be generated and put on the drop-off server.

***Note:*** You can generate reports at any time using option 5, "Generate Report (Now)", in the PFRS Configuration menu.

PFRS is now enabled. You can view the settings of PFRS at any time using option 1, "View", in the PFRS Configuration menu.

**17** 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.

**18** You have completed this procedure.

# Restoring NPM data

## Application

Use this procedure to restore any user-defined Network Patch Manager (NPM) data such as set definitions, report definitions, alarm definitions, plan definitions or SystemPlan modifications made in the release you upgraded from, that are to be carried over to the new release. This data should have been captured prior to the upgrade using procedure Saving user-defined NPM data using the NPM on page 274.

***Note:*** NPM patch files saved to a location on disk are preserved over an upgrade. However, if for some reason you need to restore those patch files, contact your next level of support. If you saved the NPM patch files on tape (Sun Netra t1400) or CD/DVD (Sun Netra 240), refer to procedure Restoring NPM patch files on page 1586 in this document.

## Prerequisites

The SSPFS and CS2M software upgrades are complete.

## 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 hostname 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.

***At the NPM CLUI or GUI***

**5** With the information you collected prior to the upgrade using procedure Saving user-defined NPM data using the NPM on page 274, restore user-defined data from the previous release as follows:

**a** Restore all user-defined set definitions using procedure Defining sets using the NPM on page 1729 in this document, for each set you recorded.

**b** Restore all user-defined report definitions using procedure Defining reports using the NPM on page 1745 in this document, for each report you recorded.

**c** Restore all user-defined alarm definitions using procedure “Defining alarms with the NPM” in the ATM/IP Solution-level Fault Management document, NN10408-900 for each alarm you recorded.

**d** Restore all user-defined patch definitions using procedure Saving a task using the NPM on page 1735 in this document, for each patch you recorded.

**e** Restore any modifications you made to the SystemPlan using procedure Defining a plan using the NPM on page 1752 in this document.

**6** You have completed this procedure.

# Restoring NPM patch files

## Application

Use this procedure to restore NPM patch files on the server. This procedure provides the following instructions:

- Restoring NPM patch files from tape (Sun Netra t1400 only) on page 1586
- Restoring NPM patch files from CD/DVD (Sun Netra 240 only) on page 1588

***Note:*** NPM patch files saved to a location on disk are preserved over an upgrade. However, if for some reason you need to restore those patch files, contact your next level of support.

## Prerequisites

This procedure has the following prerequisites:

- you need the NPM patch file archive tape (Sun Netra t1400 only)
- you need the NPM patch file archive CD/DVD (Sun Netra 240 only)

## Action

Perform the steps using one of the following methods to complete this procedure:

- Restoring NPM patch files from tape (Sun Netra t1400 only)
- Restoring NPM patch files from CD/DVD (Sun Netra 240 only)

### Restoring NPM patch files from tape (Sun Netra t1400 only)

***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 hostname 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 Stop the NPM server application if it is running. Refer to procedure Stopping the NPM server application on page 1881 in this document, if required.

6 Re-initialize the NPM database. Refer to procedure “Initializing the NPM database” in the ATM/IP Security and Administration document, NN10402-600, if required.

7 Insert the NPM patch file archive tape into the drive.

8 Rewind the tape by typing

```
# mt rewind
```

and pressing the Enter key.

9 Access the NPM patch file directory by typing

```
# cd /data/npm/Au
```

10 Restore the NPM patch files to the /data/npm/Au directory by typing

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

and pressing the Enter key.

11 Rewind and eject the tape by typing

```
# mt offline
```

and pressing the Enter key.

12 Remove the tape from the drive.

13 Start the NPM server application. Refer to procedure Starting the NPM server application on page 1883 in this document, if required.

14 You have completed this procedure.

## Restoring NPM patch files from CD/DVD (Sun Netra 240 only)

***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 hostname 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 Stop the NPM server application if it is running. Refer to procedure Stopping the NPM server application on page 1881 in this document, if required.

6 Re-initialize the NPM database. Refer to procedure “Initializing the NPM database” in the ATM/IP Security and Administration document, NN10402-600, if required.

7 Insert the NPM patch file archive CD/DVD into the drive.

8 Copy the NPM patch files to the /data/npm/Au directory by typing

```
# cp /cdrom/patches/*.ptch* /data/npm/Au/
```

and pressing the Enter key.

9 Eject the CD/DVD by typing

```
# eject cdrom
```

10 Remove the CD/DVD from the drive.

11 Start the NPM server application. Refer to procedure Starting the NPM server application on page 1883 in this document, if required.

12 You have completed this procedure.

# Installing the QCA software package on a separate server

## Application

Use this procedure if you want to install the QCA software package on a separate server. In doing so, you will be able to perform in-service upgrades with no loss of records.

***Note 1:*** Adding another QCA instance in the network requires that the GWC be associated with that QCA. Refer to the GWC Configuration Management document, NN10205-511, for instructions on how to associate a QoS collector to a GWC.

***Note 2:*** QCA is not applicable to AAL2 solutions.

## Prerequisites

The server must be running the latest release of the Succession Server Platform Foundation Software (SSPFS).

## Action

Perform the following steps to complete this procedure.

***At your workstation***

1 Log in to the CS2000 Management Tools server where the first instance of QCA is running.

2 FTP the NTQCA.pkg onto the other server running SSPFS.

3 Telnet to that server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**
is the IP address or hostname of the second server running SSPFS

4 When prompted, enter your user ID and password.

5 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

6 When prompted, enter the root password.

7 Install the QCA software package by typing

```
# pkgadd -d NTQCA.pkg
```

and pressing the Enter key.

8 You have completed this procedure.

To configure QCA, refer to procedure “Modifying the QoS Collector Application” in ATM/IP Solution-level Configuration Management document, NN10409-500.

# Configuring the SNMP agent

Alarms are managed, sorted, and viewed on the Universal Audio Server Manager. The alarms are delivered to the Universal Audio Server Manager by system software known as the “Simple Network Management Protocol (SNMP) agent.” The Universal Audio Server Manager server IP address that the SNMP agent delivers alarms to is established immediately after installation of the APS system by performing the procedure below. This procedure is also used if the IP address of the Universal Audio Server Manager changes later on.

## Configuring the SNMP agent

### *At the command line*

**1** Perform the following procedure:

**a** telnet to the CS 2000 Management Tools server

**b** log in using the “maint” login and password

**c** become the “root” user by entering:

```
su - root
```

**2** Type the following command to stop the SNMP agent:

**APSagentctl stop**

***Note:*** If this command is not found, enter the full path for the command, /opt/uas/SnmpAgent/bin/APSagentctl stop

**3** After the system response, “APS Agent terminated” displays, type the following command:

**configure_agent**

***Note:*** If this command is not found, enter the full path for the command, /opt/uas/SnmpAgent/bin/configure_agent

4 In response to the prompt, “Enter your selection,” enter either 1 or 2

where:

**1**
specifies that new configuration data is to be entered

**2**
specifies that previous configuration data is to be restored

| If | Do |
|---|---|
| you entered 1 | step 5 |
| you entered 2 | step 18 |

5 In response to the prompt, “What is the element manager’s IP address?” enter either 1 or 2

where:

**1**
specifies the default IP address

**2**
specifies that another IP address is to be entered

| If | Do |
|---|---|
| you entered 1 | step 7 |
| you entered 2 | step 6 |

6 In response to the prompt, “Enter the correct IP address” enter the IP address.

7 In response to the prompt, “What port does the element manager use to receive traps or alarms/logs?” enter either 1 or 2

where:

**1**
specifies the default port number, 162

**2**
specifies that another port number is to be entered

| If | Do |
|---|---|
| you entered 1 | step 9 |
| you entered 2 | step 8 |

8 In response to the prompt, “Enter the element manager’s port for receiving traps,” enter the port number.

**9** In response to the prompt, “Should the agent forward alarms/logs to syslog?” enter either 1 or 2

where:

**1**
specifies “yes”

***Note 1:*** APS system logs are available for viewing only in the var/log/ptmlog file.

***Note 2:*** Forwarding alarms/logs to the syslog ensures backup access to this information.

**2**
specifies “no”

| If | Do |
|---|---|
| you entered 1 | step 10 |
| you entered 2 | step 11 |

**10** In response to the prompt, “What is the logging level?” enter either 1, 2, or 3

where:

**1**
specifies “error messages”

**2**
specifies “error and warning messages”

**3**
specifies the default logging level, “error, warning, and information messages”

**11** In response to the prompt, “What port does the agent use to receive SNMP messages from the element manager?” enter either 1 or 2

where:

**1**
specifies the default port number, 5161

**2**
specifies that another port number is to be entered

***Note:*** If error messages display indicating that the port you have selected is already in use and cannot be used unless you specify it when you are logged in as the “root” user, either:

- log in again, restart the configure_agent program (see step 3), select 2 when you perform this step, and enter a different port number

or

- log in as the “root” user, restart the configure_agent program, and select 1 again when you perform this step

Note that the port number you select must also then be set in the Universal Audio Server Manager station when the APS is added to the network topology.

| If | Do |
|---|---|
| you entered 1 | step 13 |
| you entered 2 | step 12 |

**12** In response to the prompt, “Enter the agent’s port for receiving SNMP messages,” enter the port number.

**13** In response to the prompt, “What Read community string should the agent use to authenticate SNMP GET messages?” enter either 1 or 2

where:

**1**
specifies the default, “public”

**2**
specifies that another Read community string is to be entered

***Note:*** You can enter 2 if you do not want a public SNMP read community string.

| If | Do |
|---|---|
| you entered 1 | step 15 |
| you entered 2 | step 14 |

**14** In response to the prompt, “Enter the new Read community string,” enter the Read community string.

**15** In response to the prompt, “What Write community string should the agent use to authenticate SNMP SET messages?” enter either 1 or 2

where:

**1**
specifies the default, “admin”

**2**
specifies that another Write community string is to be entered

***Note 1:*** You can enter 2 if you do not want an admin SNMP Write community string.

***Note 2:*** Make sure that you specify the same Write community string when you add an APS to the network topology through the Universal Audio Server Manager.

| If | Do |
|---|---|
| you entered 1 | step 17 |
| you entered 2 | step 16 |

**16** In response to the prompt, “Enter the new Write community string,” enter the Write community string.

17 In response to the prompt, “What SNMP version should the agent use in sending SNMP messages? (enter either 1, for v1, or 2, for v2 (default))

18 After the system response, “Saving information to ApsAgent.conf” and “Saving information to ApsSnmpAgent.sh” displays, a UNIX shell prompt will display. Enter, then, the following command to start the SNMP agent:

**/opt/uas/SnmpAgent/bin/APSagentctl start**

***Note:*** This step manually restarts the SNMP agent. If the command is not used, the SNMP agent is automatically restarted when the system is rebooted.

19 Verify that the agent has started by entering the following command:

**more /opt/uas/aps/scripts/SnmpAgent.pid**

If the agent has started, a process id (pid) displays.

20 Verify that the process is running by entering:

**ps -ef | grep *nnnn***

where *nnnn* is the process id that was displayed in step 19.

21 You have completed this procedure.

# Verifying the upgrade was successful

## Application

Use this procedure to verify the upgrade was successful.

## Prerequisites

The CS2M software has been upgraded.

## Action

Perform the following steps to complete this procedure.

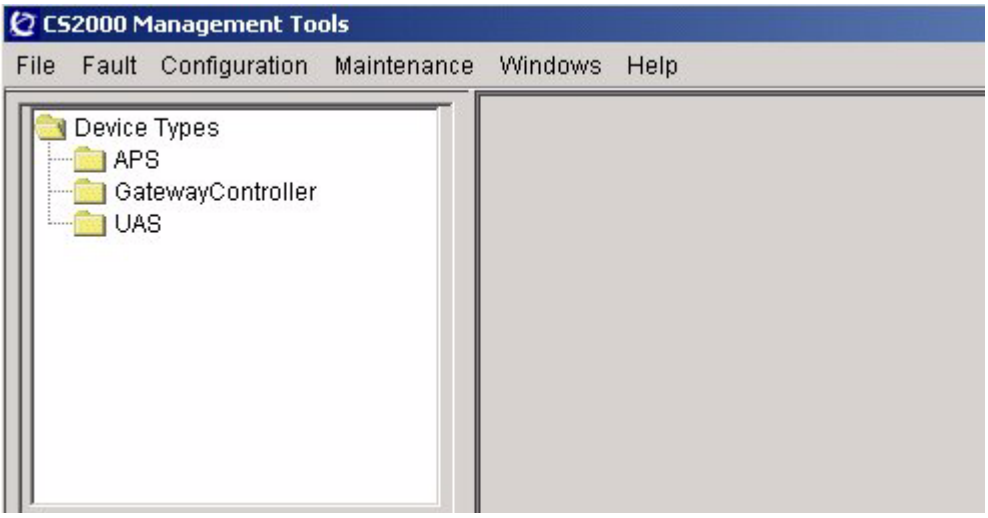
**ATTENTION**

If you encounter a problem during any one of the steps in this procedure, contact your next level of support. If required, refer to section Downgrading the CS 2000 Management Tools software on page 1842 in this document.

***At your workstation***

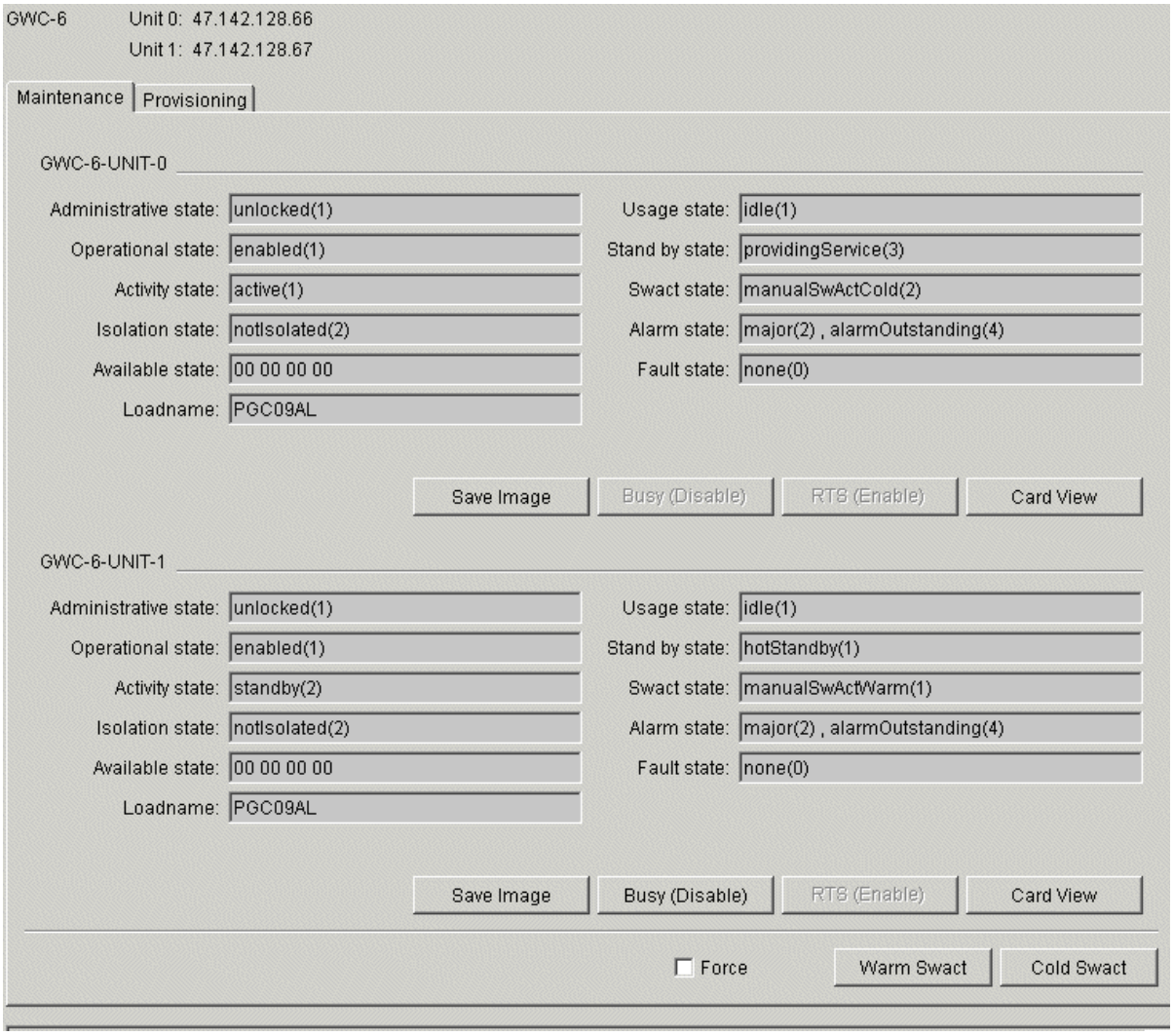
1 Launch the CS2000 Management Tools application GUI and ensure the topology is displayed correctly as shown in the figure below. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

This verifies correct restoration of the database.



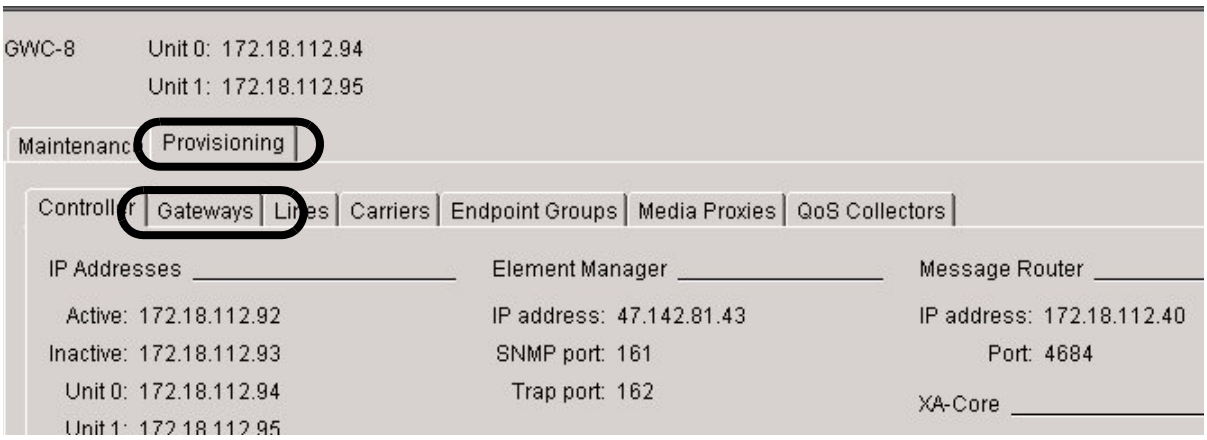
2 Click on **GatewayController**, then select a GWC from the list, and ensure correct maintenance states are displayed for the active and inactive units as shown in the figure below.

This verifies GWC SNMP communication.

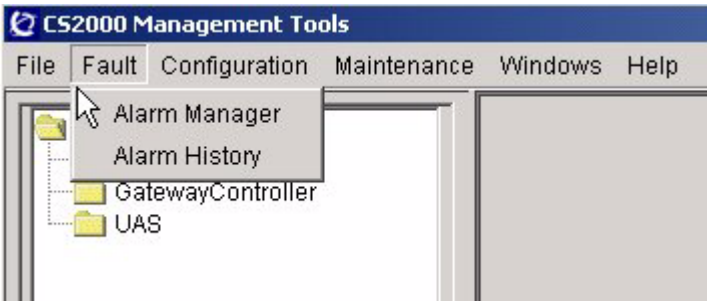


3 Click the **Provisioning** tab, then the **Gateways** tab as shown in the figure below, and then click **Retrieve All** to retrieve all subtending gateways.

This verifies correct restoration of the database.




4 On the **Fault** menu, click **Alarm Manager** as shown in the figure below, and verify alarms show up when a maintenance attempt is performed on a GWC unit.




5 Click the **Maintenance** tab, then click **Card View** to launch the CS 2000 SAM21 Manager card view.

This verifies correct operation of the CS 2000 SAM21 Manager application GUI.

6 Connect to OSSGate. Refer to the associated procedure in the ATM/IP Security and Administration document, NN10402-600, if required. Query a provisioned line (line solutions) or trunk (trunk solutions). Refer to the associated procedures in the OSSGate user guide, if required.

This verifies the SDM OSS APS, DDMS, and core communication path.

7 For line solutions, launch the line maintenance manager (LMM) application GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document if required. Post, busy, and return a line to service. Refer to associated procedures in the ATM/IP Solution-level Fault Management document, NN10408-900, if required.

   This verifies the SDM - DMA, BMI, and core communication path.

8 For trunk solutions, launch the trunk maintenance manager (TMM) application GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document if required. Post, busy, and return a trunk to service. Refer to associated procedures in the ATM/IP Solution-level Fault Management document, NN10408-900, if required.

   This verifies the SDM - DMA, BMI, and core communication path.

9 If you did not start the Network Patch Manager (NPM) GUI in any of the previous procedures, start it now to verify it is functional. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

10 You have completed this procedure.

# Completing the UAS upgrade

This procedure enables you to remove existing UAS06 or UAS07 application software.

***Note:*** During this procedure, existing UAS configuration parameters are automatically saved before the configuration files containing these parameters are removed. Thus, these configuration parameters can then be restored during the installation process.



**CAUTION**

No remote access sessions (telnet, ftp) should be in progress on a unit from which application software is being removed.

### Procedure 1 UAS06/UAS07 application software removal

***At your console***

**1** Select the fabric type of your system, either IP or ATM.

| If | Do |
|---|---|
| the UAS bearer fabric type is IP | step 5 |
| the UAS bearer fabric type is ATM | step 2 |

**2** Select the appropriate ATM bearer fabric type and UAS release.

| If | Do |
|---|---|
| the UAS bearer fabric type is ATM-AAL1 and the release is UAS06 | step 3 |
| the UAS bearer fabric type is ATM-AAL1 and the release is UAS07 | step 3 |
| the UAS bearer fabric type is ATM-AAL2 and the release is UAS06 | step 4 |
| the UAS bearer fabric type is ATM-AAL2 and the release is UAS07 | step 3 |

**3** For AAL1 UAS06 or UAS07 systems or AAL2 UAS07 systems, perform the following steps:

**a** Right-click My Computer and select “Properties.”

**b** In the System Properties window, click the Hardware tab and then select “Device Manager.”

**c** In the Device Manager window, click the plus (+) sign located at the left of “TDM/ATM bridge 2”.

**d** Right-click PA200 base board WDM and then select “Properties”.

**e** In the PA200 Base Board WDM Properties window that displays, select the Driver tab.

**f** In the Driver tab screen that displays, click Uninstall.

**g** In the Confirm Device Removal window that displays, click OK.

**h** In the “Systems Settings Change” pop-up window that displays, the system asks whether to restart the computer. Select “NO”.

**i** In the “Systems Settings Change” pop-up window that displays, the system indicates that the hardware settings have been changed and asks whether to restart the computer. Select “NO”.

**j** Close the Device Manager window (click X, located in the upper right-hand corner of the window).

**k** Close the System Properties window (click OK).

**l** Go to step 5.

**4** For AAL2 UAS06 systems, perform the following steps:

**a** Remove the bindings by performing the following steps:

**i** Right-click My Computer and select “Properties.”

**ii** In the System Properties window, click the Hardware tab and then select “Device Manager.”

**iii** In the Device Manager window, double-click Network Adapters. Right-click ArTeMux s00x Adapter - Win2K and then select “Uninstall.”

**iv** In the Confirm Device Removal window, verify that the device being removed is “ArTeMux s00x Adapter - Win2K” and then click OK.

The Device Manager window will refresh and the ArTeMux adapter will then be absent from the window.

**v** Close the Device Manager window (click X, located in the upper right-hand corner of the window).

**vi** Close the System Properties window (click OK).

**b** Verify that the fourth Local Area Connection has been removed by performing the following steps:

**i** Right-click My Network Places and select “Properties.”

In the Network and Dial-up Connections window, the fourth Local Area Connection should now be absent.

**ii** Close the Network and Dial-up Connections window (click X, located in the upper right-hand corner of the window).

**5** Perform the following steps:

**a** select **Start -> Settings** -> Control Panel

**b** In the Control Panel window, double-click Add/Remove Programs.

**c** Determine whether you are removing patches in addition to the UAS software.

| If | Do |
|---|---|
| you are removing patches in addition to the UAS software | step d |
| you are only removing the UAS software | step h |

**d** In the Add/Remove Program Properties window, scroll down the list of software programs and select “Universal Audio Server patch to be removed”.

**e** Click Add/Remove.

**f** In all succeeding confirmation and status screens, click OK (or any equivalent positive response displayed).

**g** Perform steps d through f until all patches that display are removed.

***Note:*** If you are prompted for a re-boot, respond “NO”.

**h** In the Add/Remove Program Properties window, scroll down the list of software programs and select “Universal Audio Server”.

**i** Click Change/Remove.

The “Welcome Modify, Repair, or Remove the Program” window of the InstallShield Wizard for UAS displays.

j Click Next.

***Note:*** The Remove button is the only functional option in this window and is selected by default.

The Confirm File Deletion screen displays and asks whether you wish to remove completely the selected application and all of its components.

**6** Click OK.

The following InstallShield message windows display:

- Stopping pmgrdaemon service
- Stopping SNMP services
- Removing SNMP subagents
- Stopping time service NTP Client
- Please wait while InstallShield removes and restores files

An InstallShield Wizard screen displays, indicating that maintenance is complete.

***Note:*** If at any time a pop-up window displays that prompts for the removal of “read-only” files, select YES.

**7** Ensure that the “Yes, I want to restart my computer now” option on the screen has been selected, and then click Finish.

The system performs a restart.

***Note:*** If the system reboots when the UAS software is not yet installed and when telephony cards (CG6000, AG4000, S007, PA200) are installed in the chassis, the “Found New Hardware Wizard” window will display. Press the Escape key to dismiss each instance of the display of this window.

**8** You have completed this procedure.

# Limiting access to the “regedit.exe” and “regedt32.exe” utilities

The utilities, “regedit.exe” and “regedt32.exe” cannot be removed from the system. Therefore, the following optional procedure enables you to restrict access to the utilities. After you have completed this procedure, any attempt to the access either of the utilities will result in the pop-up message display, “Access to the specified device, path, or file is denied.”

## Limiting access to the “regedit.exe” and “regedt32.exe” utilities

***At the system console (Windows desktop interface)***

1 Access Windows Explorer by performing the following steps:

```
select Start -> Programs -> Accessories ->
Windows Explorer
```

2 Select and open “My Computer”.

3 Select and open “GS_SYSTEM”. (This is the “C:” drive.)

4 Select “WINNT”, and then right-click Search.

5 Perform Steps 5 through 10 for each utility. In the Search Results pop-up that displays, enter either **regedit.exe** or **regedt32.exe**.

6 Click Search Now.

7 In the results panel that displays, right-click the “regedit.exe” file and select “Properties”.

8 In the Properties pop-up that displays, select the “Security” tab.

9 For each user listed in the resulting display:

- **a** Click on the user.
- **b** Ensure that “Allow inheritable permissions from parent to propagate to this object” has not been selected.

  ***Note:*** When you de-select this option, a security pop-up window displays. In the pop-up window, select “copy”.
- **c** In the Permissions box, for every permission that is marked “Allow”, select the equivalent “Deny” and then click the Apply button.

  ***Note:*** This may not reset the “Allow” setting.

10 After you have completed updating the permissions for all users, click OK. If a Security pop-up displays the message, “Caution! Deny takes priority over Allow entries, which can cause unintended effects due to group memberships. Do you want to continue?”, click Yes.

**11** After you have performed steps 5 through 10 for each of the two utilities, you have completed this procedure.

# Limiting access to shared network folders

This procedure enables you to disable sharing of any network folder. The affected shared folders include “C:” (which is also known as “GS_SYSTEM”), “D:” (which is also known as “New Volume”), and “C: \WINNT”.

### Limiting access to shared network folders

***At the system console (Windows desktop interface)***

1 Access Windows Explorer by performing the following steps:

**`select Start -> Programs -> Accessories -> Windows Explorer`**

2 Select and open “My Computer”.

3 Perform steps 3 and 4 for each of the folders in the resulting display. Right-click the folder and select “Sharing”.

***Note:*** “C: \WINNT” is contained on the C: folder/drive.

4 In the resulting Properties pop-up, ensure that “Do not share this folder” has been selected, and then click OK.

5 After you have performed steps 3 and 4 for each of the shared folders, you have completed this procedure.

# Limiting access to the “hh.exe”, “winhelp.exe”, and “winhlp32.exe” utilities

The utilities, “hh.exe”, “winhelp.exe”, and “winhlp32.exe” cannot be removed from the system. Therefore, the following procedure enables you to restrict access to the utilities. After you have completed this procedure, any attempt to the access any of these utilities will result in the pop-up message display, “Access to the specified device, path, or file is denied.”

***Note:*** The three utilities are located in C: \WINNT.

### Limiting access to the “hh.exe”, “winhelp.exe”, and “winhlp32.exe” utilities

***At the system console (Windows desktop interface)***

1 Access Windows Explorer by performing the following steps:

**`select Start -> Programs -> Accessories -> Windows Explorer`**

2 Select and open “My Computer”.

3 Select and open “GS_SYSTEM”. (This is the “C:” drive.)

4 Select “WINNT”, and then right-click Search.

5 Perform Steps 5 through 10 for each utility. In the Search Results pop-up that displays, enter either **hh.exe**, **winhelp.exe**, or **winhlp32.exe**.

6 Click Search Now.

7 In the results panel that displays, right-click the “hh.exe”, “winhelp.exe” or “winhlp32.exe” file and select “Properties”.

8 In the Properties pop-up that displays, select the “Security” tab.

9 For each user listed in the resulting display:

- **a** Click on the user.
- **b** Ensure that “Allow inheritable permissions from parent to propagate to this object” has not been selected.
- **c** In the Permissions box, for every permission that is marked, “Allow”, select the equivalent, “Deny”.

***Note:*** This may not reset the “Allow” setting.

10 After you have completed updating the permissions for all users, click OK. If a Security pop-up displays the message, “Caution! Deny takes priority over Allow entries, which can cause

unintended effects due to group memberships. Do you want to continue?", click Yes.

**11** After you have performed steps 5 through 10 for each of the three utilities, you have completed this procedure.

# Configuring IPSec and IKE

The following procedure provides the steps required to configure IPSec and IKE. Additional information and instructions for configuring IPSec and IKE can be found at the Microsoft web site: http://www.microsoft.com/windows2000/en/server/help/ipsec_sec_pol_create.htm

***Note:*** This procedure should be performed during non-peak hours to prevent loss of network communication.



**CAUTION**
**Possible communication disruption**
Failure to match UAS IPSec configuration values with those of the Gateway Controller may result in loss of communication capabilities between the Gateway Controller and the UAS.

## Configuring IPSec and IKE

***At your Windows desktop interface:***

1 select **`Start -> Run`**

2 Enter the following command:

**`secpol.msc`**

3 In the file tree of the Local Security Settings window that displays, select “IP Security Policies on Local Machine.”

4 In the pull-down menu under Action (located in the tool bar at the top of the window), select “Create IP Security Policy.”

5 In the next window that displays, click Next.

6 In the IP Security Policy Wizard “IP Security Policy Name” window that displays, enter a policy name and description, and then click Next.

***Note:*** Entering a policy name and description is optional.

7 In the next window that displays, ensure that the “Activate the default response rule” option is deselected, and then click Next.

8 In the next window that displays, ensure that the “Edit properties” option is selected, and then click Finish.

9 In the “Security rules for communicating with other computers” window that displays, click Add.

10 In the next window that displays, click Next.

11 In the Security Rule Wizard “Tunnel Endpoint” window that displays, ensure that the “This rule does not specify a tunnel” option is selected, and then click Next.

12 In the Security Rule Wizard “Network Type” window that displays, ensure that the “All network connections” option is selected, and then click Next.

13 In the IP Security Policy Wizard “Authentication Method” window that displays, select the “Use this string to protect the key exchange (preshared key)” option, and then enter the preshared key in the accompanying box. Click Next.

***Note:*** The preshared key entered must match exactly the preshared key on the Gateway Controller.

14 In the Security Rule Wizard “IP Filter List” window that displays, click Add.

15 In the IP Filter List window that displays, select a name and description for the IP filter list. Click Add to enter the source, destination, and protocol information for your IP filter. Click Next in the next window that displays.

16 In the Filter Wizard “IP Traffic Source” window that displays, select a source address from the pull-down menu, and then click Next.

***Note:*** Ensure that you set the Source address to “My IP Address.”

17 In the Filter Wizard “IP Traffic Destination” window that displays, select “A specific IP address” from the pulldown menu for the “Destination address” field. In the “IP Address” field, enter the IP address of the Gateway Controller, and then click Next.

18 In the Filter Wizard “IP Protocol Type” window that displays, select a protocol type from the pull-down menu for the “Select a protocol type” field. Click Next, and in the next window that displays, click Finish. Click Close in the next window that displays.

***Note:*** It is recommended that you set the protocol type to “Any.”

19 In the Security Rule Wizard “IP Filter List” window, click the circle located next to the newly-created filter, and then click Next.

20 In the Filter Action window, click Add. Click Next in the next window that displays.

**21** In the Filter Action “Filter Action Name” window that displays, select a name and description for the filter action. Click Next.

***Note:*** A sample entry is: “ESP: MD5 / 300s SA lifetime,” which means that ESP is being used with MD5 authentication and a security association lifetime of 300 seconds. The security values that you enter, however, must be compatible with those being used on the Gateway Controller.

**22** In the Filter Action “Filter Action General Options” window that displays, set your policy behavior from the following options:

- The “Permit” (bypass) option allows all IP traffic from the Gateway Controller to pass through the IPSec filter.
- The “Block” option prevents all IP traffic from the Gateway Controller from passing through the IPSec filter.
- The “Negotiate Security” option allows the UAS and the Gateway Controller to negotiate security settings. If negotiation fails, all traffic to and from the Gateway Controller is prevented.

| If | Perform |
|---|---|
| you set your policy behavior to “Permit” | click Next, and then click Finish in the next window that displays. Go to step 29 |
| you set your policy behavior to “Block” | click Next, and then click Finish in the next window that displays. Go to step 29 |
| you set your policy behavior to “Negotiate Security” | click Next and then go to step 23 |

**23** In the Filter Action Wizard “Communicating with computers that do not support IPSec” window that displays, ensure that you set the security option to “Do not communicate with computers that do not support IPSec” and then click Next.

**24** In the Security Method Wizard “IP Traffic Security” window that displays, select the “Custom” option and then click Settings.

**25** In the Custom Security Method Settings window that displays, select the “Data integrity and encryption (ESP)” option. Make the appropriate selections in the pull down window for the “Integrity algorithm” field and in the pull-down window for the “Encryption algorithm” field. In the “Session key settings” panel, select “Generate a new key every” and enter the value of the Gateway Controller IPSec SA lifetime. Click OK.

**26** In the IP Traffic Security window that displays, click Next.

**27** In the Filter Action Wizard window that displays, ensure that "Edit properties" option is selected and then click Finish.

**28** In the New Filter Action Properties window that displays, deselect "Accept unsecured communication, but always respond using IPSec option." The "Session key Perfect Forward Secrecy" option must be selected. Click Apply and then OK in the next screen that displays.

**29** In the Security Rule Wizard "Filter Action" window that displays, click the circle next to the new filter action that you have created and then click Next. Click Finish in the next window that displays.

**30** In the *<security policy>* Properties window that displays, select the "General" tab and then click Advanced.

**31** In the Key Exchange Settings window that displays, enable "Master key Perfect Forward Secrecy." Then enter a key negotiation time value that is compatible with the Gateway Controller's internet key exchange (IKE) SA lifetime, in the "Protect identities with these security methods" field. Click Methods.

***Note:*** If you don't know the minute values that are compatible, use the same value used with the Gateway Controller. Ensure that you enter the value in minutes equivalent to the Gateway Controller's value, which is expressed in seconds.

**32** In the Key Exchange Security Methods window that displays, you can alter the security method preference order or the encryption and authentication settings used, for the internet key exchange (IKE).

***Note:*** Since the "Master key Perfect Forward Secrecy" option was enabled in step 31, the Gateway Controller must have both the IKE and IPSec Diffie-Hellman groups that match the

Diffie-Hellman group set in the IKE Security Algorithms window.

| If | Perform |
|---|---|
| IKE settings for the Gateway Controller are known | move the matching preference to the top of the list in the Key Exchange Security Methods window. Click OK in the Key Exchange Security Methods window. Click OK in the Key Exchange Settings window. |
| you do not find a matching preference | click Add**.** In the IKE Security Algorithms window that displays, select the necessary IKE from the pull-down menus, click OK, and then move this preference to the top of the list in the Key Exchange Security Methods window. Click OK in the Key Exchange Security Methods window. Click OK in the Key Exchange Settings window. |

**33** Click Close in the next window that displays.

**34** To activate the newly-created IP Security policy, select the policy name from the list under the “Name” column in the Local Security Settings window and select “Assign” from the pull-down “Action” menu located in the tool bar.

***Note 1:*** An IP Security policy can be un-assigned by selecting a policy from the list and selecting Unassign from the pull-down “Action” menu.

***Note 2:*** The security policies for the Gateway Controller and for the UAS must be assigned, or unassigned, at the same time, in order to prevent communication disruption.

**35** You have completed this procedure.

# Nortel Networks Global Server 3.3 installation

The following procedure enables you to install the Nortel Networks Global Server 3.3 software on the UAS.

In UAS nodes equipped with the CPV5350SCSI configuration, the SCSI controller does not reside on the same board as the host processor. In UAS nodes equipped with the CPV5370 SCSI configuration, the SCSI controller resides on the same board as the host processor. Although the procedure below appears to only address installation of the Nortel Networks Global Server 3.3 software on a chassis equipped with the CPV5370 SCSI configuration, it is still applicable if your system is equipped with a CPV5350 SCSI configuration.

The following table lists the procedures performed during the Global Server 3.3 installation on the SAM16-based UAS application server, showing the method used for the installation, the CD-ROM, if any, used during the installation, and the approximate amount of time required for performing the procedure.

**Global Server 3.3 Installation Procedures**

| Procedure | Script, application, interface used during installation | CD-ROM | Minimum duration (minutes) |
|---|---|---|---|
| Installing operating system software on a Win2K | boot from CD-ROM | Win2K: Win2K OS and System Software for CPV5350, GS v3.3 or Win2K: Win2K OS and System Software for CPV5370, GS v3.3 | 30 |
| Installing HAE software on a Win2K AS | none | none | 15 |
| Installing platform software on a Win2K AS | none | none | 15 |

This procedure provides the required order in which the Global Server installation procedures are performed for a ground-up installation.



**CAUTION**

You must perform the steps in the Win2K application server software installation procedures exactly as instructed. Errors cannot be undone during the installation. If a procedure or step is skipped, if incorrect information is entered, or if there is any change in the hardware configuration, all data may be lost and the entire Win2K application server software installation process must be performed again.

### Installing Nortel Networks Global Server 3.3 base software on the UAS

***At your console:***

1. Perform the procedure, Installing OS and system software on a Win2K AS on page 969
2. Perform the procedure, Installing HAE software on a Win2K AS on page 1617
3. Perform the procedure, Configuring Global Server base platform software on a Win2K AS on page 1620
4. If you want to change the system password, perform the procedure, Setting the system password on page 1622
5. You have completed this procedure.

# Installing HAE software on a Win2K AS

This procedure enables you to install HAE software on a single Win2K application server.

Before you start performing this procedure, it is important that the following information is available to you for the application server that is being installed:

- hostname
- IP address
- subnet mask
- default gateway address
- domain name (optional)
- Domain Name Server (DNS) IP addresses search order (optional)
- Domain Suffix addresses search order (optional)

### Installing HAE software on a Win2K AS

***At your console:***

**1** Double-click the green network card icon located in the right-hand corner of the task bar.

*The system displays the Intel (R) ProSet II window.*

**2** In the left pane of the Intel (R) ProSet II window, right-click on the top network adapter.

**3** Select **Add to Team -> Create New Team** from the drop-down menu.

*The Teaming Wizard window displays.*

**4** Ensure that “Adapter Fault Tolerance” mode is selected, and then click Next.

**5** Select both adapters, then click Next.

**6** Observe the team configuration and click Finish.

*The Intel (R) ProSet II window displays.*

**7** In the Intel (R) ProSet II window, right-click the first adapter, then click Preferred Primary.

**8** In the Intel (R) ProSet II window, right-click the second adapter, then click Preferred Secondary.

**9** Click OK.

**10** On the host processor desktop, right-click the “My Network Places” icon and select Properties from the drop-down menu.

*The Network and Dial-up Connections window displays.*

**11** In the Network and Dial-up Connections window, right-click Local Area Connection 3 and select Properties from the drop-down menu.

*The Local Area Connection 3 Properties window displays.*

**12** In the Local Area Connection 3 Properties window, scroll to Internet Protocol and double-click Internet Protocol (TCP/IP).

*The Internet Protocol TCP/IP Properties window displays.*

**13** In the Internet Protocol TCP/IP Properties window, select “Use the following IP addresses” and fill in all fields with the addresses previously obtained from the system administrator, including:

- IP address
- subnet mask
- default gateway address
- Domain Name Server (DNS) IP addresses search order (optional)
- Domain Suffix addresses search order (optional)

***Note:*** You may need to click Advanced to set some optional settings.

**a** Click OK.

**14** In the Local Area Connection 3 Properties window, click OK.

**15** You may see the prompt, “This connection has empty primary WINS address - do you want to continue?” If this prompt displays, click Yes.

**16** Close the Network and Dial-up Connection window.

**17** Right-click the “My Computer” icon, and then select Properties from the drop-down menu.

*The System Properties box displays.*

**18** Select the Network Identification tab, and then click Properties.

*The Identification Changes window displays.*

**19** Enter the hostname of the host processor in the Computer Name field, then click More.

***Note:*** Ensure that “Caps lock” on your PC is not “on.”

*The DNS Suffix and NetBIOS Computer Name window displays.*

**20** In the DNS Suffix and NetBIOS Computer Name window, enter the Primary DNS suffix and click OK.

*The Identification Changes window displays.*

**21** In the Identification Changes window, click OK.

*The Network Identification information dialog window displays.*

**22** In the Network Identification information dialog window, click OK.

**23** In the System Properties box, click OK.

**24** Click NO in the System Settings Change pop-up to reboot the computer with the new name and IP address.

**25** You have completed this procedure.

### Configuring Global Server base platform software on a Win2K AS

***At your console:***

**1** Determine whether you are installing platform software on the "B" domain (right side) or on the "A" domain (left side).

| If | Start with |
|---|---|
| you are configuring platform software on the B domain | step a |
| you are configuring platform software on the A domain | step b |

**a** Using the Notepad tool, edit file "EventSrv.cfg" to contain EMS sub-system datafill by performing the following steps:

**i** `select` **`Start -> Run`**

**ii** Enter the following on a single line:

```
Notepad
c:\GlobalServer\config\EventSrv.cfg
```

**iii** Change the data value for the EMSServerName key by entering the following:

```
EMSServerName mate_sc
```

***Note:*** Enter only a tab (using the tab key) between "EMSServerName" and "mate_sc."

**iv** Save the file and close the Notepad window.

**v** Go to step b.

**b** Using the Notepad tool, edit the host file and add the IP address and host name (if any) associated with the peer and local domains by performing the following steps:

**i** `select` **`Start -> Run`**

**ii** Enter the following on a single line:

```
Notepad
c:\winnt\system32\drivers\etc\hosts
```

**iii** Add the following two lines in the format shown:

```
<IP address> <hostname> mate_sc
```

where <IP address> is the IP address of the peer domain (opposite of your domain) and <hostname> is the hostname of the peer domain

```
<IP address> <hostname> local_sc
```

where <IP address> is the IP address of your local domain and <hostname> is the hostname of your local domain

**iv** Save the file and close the Notepad window.

**2** Re-boot the system by performing the following steps:

**a** select **Start -> Shutdown**

**b** Select “restart” in the Shutdown Windows screen.

***Note 1:*** If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

***Note 2:*** If the system reboots when the UAS software is not yet installed and when telephony cards (CG6000, AG4000, PA200) are installed in the chassis, the “Found New Hardware Wizard” window will display. Press the Escape key to dismiss each instance of the display of this window.

**3** You have completed this procedure.

# Setting the system password

This optional procedure enables you to change the system password to ensure system security.

### Setting the system password

***At your console:***

1. Select **Start -> Programs -> Administrative Tools -> Computer Management**
2. In the left pane of the Computer Management screen that displays, expand “Local Users and Groups.”
3. Select Users.
4. In the right pane of the “Users” screen, right-click Administrator.
5. Select “Set Password.”
6. In the Set Password window that displays, enter the new password and confirm your entry, and then click OK.
7. In the Local Users and Groups box that displays, click OK.
8. Close the Computer Management screen.
9. Perform the following steps to set the system password:
   a. `select` **`Start -> Run`**
   b. Enter the following:

      **`Services.msc`**

      *The Services window displays.*
10. In the Services window, right-click pmgrDaemon and select Properties.

    *The PMGRdaemon Properties (Local Computer) window displays.*
11. In the PMGRdaemon Properties (Local Computer) window, select the Log On tab.
    a. Select “This account.”
    b. In the “account name” field, verify the entry or enter:

       **`.\Administrator`**
    c. In the “password” and “confirm password” fields, enter the new password.
    d. Click OK.

*The Microsoft Management Console dialog box displays.*

**12** To effect the change to the system password that you have made, log off by performing the following step:

`select` **`Start -> Shutdown -> Log off`**

**13** Log back in.

**14** You have completed this procedure.

# Disabling web browsers (UAS06)

This procedure enables you to disable the Windows Explorer and Netscape Navigator web browsers in order to enhance system operation. The procedure must be performed separately for each browser.

***Note:*** The steps presented in this procedure assume that you are operating using a right-hand mouse.

## Disabling web browsers

***At the system console (Windows desktop interface)***

1. Using Windows Explorer (select **Start -> Programs -> Accessories -> Windows Explorer**).
2. In the Tools menu, select “Folder Options.”
3. Select the View tab and ensure that “Hide files extension for known file types” is not checked, and then click OK.
4. Locate either the “c:\Program Files\Internet Explorer\lexplore.exe” file to disable Internet Explorer, or the “c:\Program Files\Netscape Communicator\Program\netscape.exe” file to disable Netscape Communicator.
5. After you have located the file, click on the file to select it and then right-click. In the pop-up window that displays, scroll the cursor down to “Properties” and then left-click “Properties”.
6. In the Properties pop-up window that displays, select the Security tab.
7. In the Permissions box in the Security panel, deny access for the groups, Administrators, Power Users, and Users by selecting each group, one at a time, and then selecting “Deny for Full Control”. After the selection has been made for all groups, click Apply.
8. When the Security change acknowledgment pop-up window displays, click Yes.
9. Click OK to close the Properties window.
10. Remove the desktop shortcuts to the web browser by performing the following steps:
    a. Exit all applications to the Windows desktop.
    b. On the Windows desktop, right-click on the shortcut for the browser (Internet Explorer or Netscape Communicator).

**c** In the pop-up window that displays, click Delete.

**d** In the deletion confirmation window that displays, click Yes.

**11** If you have performed this procedure for both browsers, go on to step 12. If you have not performed this procedure for both browsers, perform steps 1 through 10 for the other browser.

**12** You have completed this procedure.

# Handling a “ConfigMgr failed” error

The following procedure is performed in response to the display of the message, “ConfigMgr failed. See C:\WINNT\Temp\restoreLog.txt file for details” in a pop-up window, when the UAS07 software is being installed.

### Handling a “ConfigMgr failed” error

***At the system console (Windows desktop interface)***

**1** Using the Notepad tool, view file “restoreLog.txt” file by performing the following steps:

**a** select **`Start -> Run`**

**b** Enter the following on a single line:

```
Notepad c:\WINNT\Temp\restoreLog.txt
```

**c** Look in the file display for a message similar to the following: “Warning: number of cards in old config file (2) is not the same as the number of cards in the system (0).”

| If | Do |
|---|---|
| you see such a message | step d |
| you don’t see this kind of message | step e |

**d** Close the Notepad window and then go to step 2.

**e** Log the message and report the problem to your Nortel Networks service representative. Click Finish in the InstallShield Wizard Complete screen and abandon the UAS06 software installation until the problem can be corrected.

**2** Open a command line interface at the UAS:

**a** select **Start -> Run**

**b** type **cmd** in the window that displays

**c** press Enter

**d** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

**e** press Enter

**3** Perform the procedure, Checking the status of AG4000 and CG6000 device drivers on page 1632.

| If | Do |
|---|---|
| entries for cards are missing from the list of NMS Telecomm Devices, indicating a possible problem with the Hot Swap Controller card | step 4 |
| there are entries for all cards in the list of NMS Telecomm Devices, but problems are indicated with one or more devices | step 14 |

**4** Shut down the system:

select **Start -> Shut Down**

**a** On the Shut Down Windows screen, select “Shut down this computer.” When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do not turn off power to the computer.

**5** Locate the Hot Swap Controller card. The Hot Swap Controller cards reside in the domain of the chassis opposite from the domain that they control. Thus, the Hot Swap Controller for the left domain resides in slot 10; the Hot Swap Controller for the right domain resides in slot 8.

**a** Using a Phillips head screwdriver, loosen the screws that secure the card in the slot, and then unlock the lock latches.

***Note:*** There is no rear transition module for this card.

**b** Slide the card out in the slot approximately one inch and then reseat the card in the slot. Lock the lock latches and then, using a Phillips head screwdriver, tighten the screws that secure the card in the slot. The node will reboot automatically upon insertion of the new card.

**6** After the system finishes rebooting, open a command line interface at the UAS:

**a** select **Start -> Run**

**b** type **cmd** in the window that displays

**c** press Enter

**d** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

**e** press Enter

**7** Perform the procedure, Checking the status of AG4000 and CG6000 device drivers on page 1632.

| If | Do |
|---|---|
| entries for cards are missing from the list of NMS Telecomm Devices, indicating a possible problem with the Hot Swap Controller card | step 8 |
| there are entries for all cards in the list of NMS Telecomm Devices, but problems are indicated with one or more devices | step 14 |
| the problem seems to have been corrected | step 17 |

**8** Stop any applications that may be 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.

**9** Shut down the system:

select **Start -> Shut Down**

**a** On the Shut Down Windows screen, select “Shut down this computer.” When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do not turn off power to the computer.

**10** Locate the Hot Swap Controller card. The Hot Swap Controller cards reside in the domain of the chassis opposite from the domain that they control. Thus, the Hot Swap Controller for the left domain resides in slot 10; the Hot Swap Controller for the right domain resides in slot 8.

**a** Remove the Hot Swap Controller card. (The screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed.)

***Note:*** There is no rear transition module for this card.

**b** Insert the new Hot Swap Controller card. (After the new card has been inserted into the card slot, lock the lock latches, and tighten the screws that secure the card in the shelf.) The node will reboot automatically upon insertion of the new card.

**11** After the system finishes rebooting, open a command line interface at the UAS:

**a** select **Start -> Run**

**b** type **cmd** in the window that displays

**c** press Enter

**d** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

**e** press Enter

**12** Perform the procedure, Checking the status of AG4000 and CG6000 device drivers on page 1632.

| If | Do |
|---|---|
| entries for cards are missing from the list of NMS Telecomm Devices, indicating a possible problem with the Hot Swap Controller card | step 13 |
| there are entries for all cards in the list of NMS Telecomm Devices, but problems are indicated with one or more devices | step 14 |
| the problem seems to have been corrected | step 17 |

**13** Contact your Nortel Networks service representative and abandon the installation until the problem is corrected.

**14** Perform the procedure, Reinstalling an AG4000 or CG6000 device driver on page 1633.

**15** After the system finishes rebooting, open a command line interface at the UAS:

**a** select **Start -> Run**

**b** type **cmd** in the window that displays

**c** press Enter

**d** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

**e** press Enter

**16** Perform the procedure, Checking the status of AG4000 and CG6000 device drivers on page 1632.

| If | Do |
|---|---|
| entries for cards are missing from the list of NMS Telecomm Devices, indicating a possible problem with the Hot Swap Controller card | Contact your Nortel Networks service representative and abandon the installation until the problem has been corrected. |
| there are entries for all cards in the list of NMS Telecomm Devices, but problems are indicated with one or more devices | Contact your Nortel Networks service representative and abandon the installation until the problem has been corrected. |
| the problem seems to have been corrected | step 18 |

**17** Re-boot the system by performing the following steps:

**a** select **Start -> Shutdown**

**b** Select “restart” in the Shutdown Windows screen.

**18** Stop any applications that may be 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.

**19** Open a command line interface at the UAS:

**a** select **Start -> Run**

**b** type **cmd** in the window that displays

**c** press Enter

**d** type **configmgr -restore -v** in the window that displays

**e** press Enter

| If | Do |
|---|---|
| the configmgr tool reports a “successful” completion status, and does not display a warning message | step 20 |
| the configmgr tool does not report a “successful” completion message | Contact your Nortel Networks service representative and abandon the installation until the problem has been corrected. |

**20** You have completed this procedure. Return to the step in the procedure that you were performing when you were referred to this procedure.

# Checking the status of AG4000 and CG6000 device drivers

This procedure enables you to determine the status of the AG4000 or CG6000 device drivers.

## Checking the status of the AG4000 or CG6000 device drivers

### *At the system console (Windows desktop interface)*

1. Right-click “My Computer” and then select “Properties”.
2. In the System Properties pop-up window that displays, select the Hardware tab.
3. Click the “Device Manager” button.

   *The Device Manager window opens.*
4. Expand the “NMS Telecomm Devices” entry. In the expanded entry, you should see one NMS cPCI CG6000 entry for each CG6000 card provisioned in the system, and one NMS cPCI AG4000 entry for each AG4000 card provisioned in the system.
5. Examine the status of each card in the list, one at a time, by double-clicking the icon for a card.

   *An NMS cPCI <AG4000 or CG6000> Properties window displays.*

   If the device is operating normally, you will see in the Device Status panel the message, “This device is working properly.”
6. You have completed this procedure.

# Reinstalling an AG4000 or CG6000 device driver

This procedure enables you to reinstall AG4000 or CG6000 device drivers.

### Reinstalling an AG4000 or CG6000 device driver

***At the system console (Windows desktop interface)***

1. Right-click “My Computer” and then select “Properties”.
2. In the System Properties pop-up window that displays, select the Hardware tab.
3. Click the “Device Manager” button.

   *The Device Manager window opens.*
4. Expand the “NMS Telecomm Devices” entry. In the expanded entry, you will see one NMS cPCI CG6000 entry for each CG6000 card provisioned in the system, and one NMS cPCI AG4000 entry for each AG4000 card provisioned in the system.
5. Double-click the icon associated with the card driver to be reinstalled.

   *An NMS cPCI <AG4000 or CG6000> Properties window displays.*
6. Click the Driver tab and then click the “Update Driver” button.
7. In the Welcome screen that displays, click Next.
8. In the Install Hardware Device Drivers screen that displays, select “Search for a suitable driver for my device (recommended).”
9. In the Locate Driver Files screen that displays, click Next.
10. In the popup window that displays, click OK to select the default folder name, “C:\NMS\CG\Sys” for CG6000 cards, and “C:\NMS\AG\Sys” for AG4000 cards.
11. In the Driver Files Search Results window that displays, select “Install one of the other drivers” and then click Next.
12. In the Driver Files Found window that displays, the NMS cPCI CG6000 entry or the NMS cPCI AG4000 entry will already be selected. Click Next.
13. When the Completing the Upgrade Device Driver Wizard window displays, indicating that the driver has been installed, click Finish.

**14** Either perform steps 5 through 13 for another driver, or proceed to step 15.

**15** Re-boot the system by performing the following steps:

**a** select **Start -> Shutdown**

**b** Select “restart” in the Shutdown Windows screen.

**16** You have completed this procedure.



Copyright © 2005, Nortel Networks


# Additional procedures

This section contains additional prodedures that may be necessary after a Succession upgrade.

# Succession patching

## Overview

Software enhancements or corrections are provided either through patches or maintenance releases. A patch is a temporary enhancement or correction to the functionality included in the software of a particular release. Patches allow for a number of small changes to be made to the software until the next release of the software is available. In general, a new software release incorporates all the changes made in the preceding patches. A maintenance release is a new software version of a particular release that contains corrective content.

This section discusses patching for the following Succession components that support the patching capability:

- core manager
- Succession Server Platform Foundation Software (SSPFS)
- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 Management Tools components
  - CS 2000 SAM21 Manager
  - Succession Element and Sub-network Manager (SESM)
  - QoS Collector Applicaton (QCA)
- Network Patch Manager (NPM)
- Preside Multi-service Data Manager (MDM)
- Media Gateway (MG) 9000 Manager
- Passport 15000
- Gateway Controller (GWC)
- Multi-service Gateway (MG) 4000
- Media Gateway (MG) 9000
- Inter-Working Spectrum Peripheral Module (IW SPM)
- Dynamic Packet Trunking Spectrum Peripheral Module (DPT SPM)
- Legacy peripherals (for example, LIU7, DTC, SPM)
- Communication Server 2000 (CS 2000)

## Delivery

Patches can be delivered at the same time a new software release is delivered (upgrade with patching), or between software releases (maintenance patching).

For software upgrades, a CD with the software load and a CD with any patches released to date are delivered. Any patches released after the patch CD was created can be delivered through Electronic Software Delivery if the site is set up for ESD, or downloaded from a secure Nortel Networks web page.

### Electronic Software Distribution

Patch files are pushed from Nortel Networks to an external drop box location. The drop box can exist on Nortel Networks' Customer Access Network (CAN), or the customer's wide area network (WAN).

***Note:*** For information on how to deploy ESD, contact your Nortel Networks representative.

### Web distribution

Patches are pulled through the Internet from a secure Nortel Networks web page and stored on a customer-provided server.

Web distribution is done through www.nortelnetworks.com. Patches are located under "Support > Software Downloads > Succession > Succession Communication Server 2000 > Software".

***Note:*** Use the filter criteria to only display a selected set of patches.

Also, to facilitate patch management, the Patch Audit tool is available under "Support > Software Downloads > Succession > Succession Communication Server 2000 > Tools > Patch Audit for Inform Lists". The Patch Audit tool enables customers to perform a site-specific audit and determine any missing patches as well as patches that may require customer action. The Patch Audit User Guide in the same location, provides more details.

## Tools and utilities

The following table lists the tools and utilities used to patch the components that support the patching capability in a Succession network.

| Tool/utility | Description |
|---|---|
| PRSM | The Post-Release Software Manager (PRSM) is a command line interface (CLI) utility on the CS 2000. The PRSM is used for patching activities on the following components:<br>• CS 2000<br>• MG 4000<br>• IW SPM<br>• DPT SPM<br>• Legacy peripherals, for example, the Spectrum Peripheral Module (SPM)<br><br>***Note:*** Patches are also referred to as Post-Release Software Updates (PRSUs). |
| NPM | The Network Patch Manager (NPM) is a patching tool with both a command line user interface (CLUI) and a webstart-based graphical user interface (GUI). The NPM is used for patching activities on the following components:<br>• GWC<br>• CS 2000 SAM21 Manager<br>• MG 9000<br>• MG 9000 Manager<br>• PSE<br>• NPM<br>• SESM<br>• QCA<br>• SSPFS<br>• Integrated EMS<br>• Integrated EMS security component<br><br>***Note:*** You can obtain help information on the NPM through the Help menu of the GUI or by typing “help” in the CLUI. |

| Tool/utility | Description |
|---|---|
| Preside MDM | The Preside MDM when configured as a software distribution site (SDS), manages, stores, and provides access to patch files. The Preside MDM is used for patching activities on the following components:<br>• Preside MDM<br>• Passport 15000 |
| SWIM | The Software Inventory Manager (SWIM) is a utility integrated in the maintenance interface of the CS 2000 core manager, and is used to apply patch files, also referred to as fix filesets, on the CS 2000 core manager. |
| patchctrl | The patchctrl tool is used to apply one or more patches to the Core Billing Manager (CBM). The patchctrl tool can be invoked from any directory on the CBM. |

## Patching order

When patches are available with the new software version for a component, apply the patches immediately following the software upgrade.

When patches are available between upgrades (maintenance patching), patch the components in the following order:

***Note:*** Only the components that support the patching capability, are listed.

- Core manager
- Succession Server Platform Foundation Software
- Integrated Element Management System
- Integrated EMS security component
- Patching Server Element
- CS 2000 Management Tools components
  - CS 2000 SAM21 Manager
  - SESM
  - QCA
- Media Gateway 9000 Manager

- Network Patch Manager
- Preside Multi-service Data Manager
- Passport 15000
- Gateway Controller
- Multi-service Gateway 4000
- Media Gateway 9000
- Interworking Spectrum Peripheral Module
- Dynamic Packet Trunking Spectrum Peripheral Module
- Legacy Peripheral Modules
- Communication Server 2000

## Patching procedures

The sections that follow provide patching information for the individual components that support the patching capability, including references to the documents or the procedures that contain the detailed steps.

### Core manager

For the CS 2000 Core Manager, refer to procedure “Upgrading the CS 2000 Core Manager with software fixes” in the CS 2000 Core Manager Upgrade document, NN10060-461. For the CBM 850, refer to “Setting up automatic patching on a CBM 850 cluster and removing previously configured schedules”, and to “Manually applying patches to the CBM 850” in the Core and Billing Manager 850 Upgrades document, NN10347-461.

### Succession Server Platform Foundation Software

The table below lists the procedures you must perform to patch the Succession Server Platform Foundation Software (SSPFS). The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (√) in the √column as you complete each procedure.

**Table 1 Patching procedures checklist for the SSPFS**

| Activities | √ | Procedures |
|---|---|---|
| Retrieve the patch files from CD or electronically, and copy into the NPM database. | | Perform procedure Transferring patches to the NPM database manually on page 1664 in this document. |
| Apply the patches to the SSPFS. | | Perform procedure Applying patches using the NPM on page 1674 in this document. |

### Integrated Element Management System

The table below lists the procedures you must perform to patch the Integrated Element Management System (EMS). The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (√) in the √column as you complete each procedure.

**Table 2 Patching procedures checklist for the Integrated EMS**

| Activities | √ | Procedures |
|---|---|---|
| Retrieve the patch files from CD or electronically, and copy into the NPM database. | | Perform procedure Transferring patches to the NPM database manually on page 1664 in this document. |
| Apply the patches to the Integrated EMS. | | Perform procedure Applying patches using the NPM on page 1674 in this document. |
| Restart the Integrated EMS to enable the applied patches. | | Perform procedure Restarting a device using the NPM on page 1721 in this document. |

### Integrated EMS security component

The table below lists the procedures you must perform to patch the Integrated Element Management System (EMS) security component. The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (√) in the √column as you complete each procedure.

**Table 3 Patching procedures checklist for the Integrated EMS security component**

| Activities | √ | Procedures |
|---|---|---|
| Retrieve the patch files from CD or electronically, and copy into the NPM database. | | Perform procedure Transferring patches to the NPM database manually on page 1664 in this document. |
| Apply the patches to the Integrated EMS security component. | | Perform procedure Applying patches using the NPM on page 1674 in this document. |
| Restart the Integrated EMS security component to enable the applied patches. | | Perform procedure Restarting a device using the NPM on page 1721 in this document. |

### Patching Server Element

The table below lists the procedures you must perform to patch the Patching Server Element (PSE). The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (√) in the √column as you complete each procedure.

**Table 4 Patching procedures checklist for the PSE**

| Activities | √ | Procedures |
|---|---|---|
| Retrieve the patch files from CD or electronically, and copy into the NPM database. | | Perform procedure Transferring patches to the NPM database manually on page 1664 in this document. |
| Apply the patches to the Patching Server Element (PSE). | | Perform procedure Applying patches using the NPM on page 1674 in this document. |
| Restart the PSE to enable the applied patches. | | Perform procedure Restarting a device using the NPM on page 1721 in this document. |

### CS 2000 Management Tools components

The table below lists the procedures you must perform to patch the CS 2000 Management Tools components (CS 2000 SAM21 Manager, SESM, and QCA). The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (√) in the √column as you complete each procedure.

**Table 5 Patching procedures checklist for the CS 2000 Management Tools components**

| Activities | √ | Procedures |
|---|---|---|
| Audit the devices for existing patch activity. | | Perform procedure Performing a device audit using the NPM on page 1669in this document. |
| Retrieve the patch files from CD or electronically, and copy into the NPM database. | | Perform procedure Transferring patches to the NPM database manually on page 1664 in this document. |
| Apply the patches to the CS 2000 SAM21 Manager. | | Perform procedure Applying patches using the NPM on page 1674 in this document. |
| Restart the CS 2000 SAM21 Manager to enable the applied patches. | | Perform procedure Restarting a device using the NPM on page 1721 in this document. |
| Apply the patches to the Succession Element and Sub-network Manager (SESM). | | Perform procedure Applying patches using the NPM on page 1674 in this document. |
| Restart the SESM to enable the applied patches. | | Perform procedure Restarting a device using the NPM on page 1721 in this document. |
| Apply the patches to the QoS Collector Application (QCA). | | Perform procedure Applying patches using the NPM on page 1674 in this document. |
| Restart the QCA to enable the applied patches. | | Perform procedure Restarting a device using the NPM on page 1721 in this document. |

### Media Gateway 9000 Manager

The table below lists the procedures you must perform to patch the Media Gateway (MG) 9000 Manager. The procedures must be performed in the order they are listed.

**ATTENTION**

Before you apply disruptive dcc patches, you must ensure the node is not aps switched by displaying the master shelf for the dcc pair you are patching. If the node is aps switched, an “S” appears on the inactive dcc card. Refer to procedure “Recovery from APS split-mode” in the MG9000 Fault Management document, NN10074-911, to correct the condition. Only apply dcc disruptive patches when the node is not aps switched. In addition, ensure no alarms are present on the dcc card you are patching, through the Alarms menu. Refer to the MG9000 Fault Management document, NN10074-911, for instructions on how to post and clear alarms. Only apply dcc disruptive patches when the dcc card is alarm free.

Use this table as a checklist during the patching process. Place a check (√) in the √column as you complete each procedure.

**Table 6 Patching procedures checklist for the MG 9000 Manager**

| Activities | √ | Procedures |
|---|---|---|
| Retrieve the patch files from CD or electronically, and copy into the NPM database. | | Perform procedure Transferring patches to the NPM database manually on page 1664 in this document. |
| Apply the patches to the MG 9000 Manager components as follows:<br>• mg9kemserver<br>• mg9kemmidtier<br>• mg9kemomcollector | | Perform procedure Applying patches using the NPM on page 1674 in this document. |
| Restart the MG 9000 Manager components to enable the applied patches. | | Perform procedure Restarting a device using the NPM on page 1721 in this document. |

### Network Patch Manager

The table below lists the procedures you must perform to patch the Network Patch Manager (NPM). The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (√) in the √column as you complete each procedure.

**Table 7 Patching procedures checklist for the NPM**

| Activities | √ | Procedures |
|---|---|---|
| Retrieve the patch files from CD or electronically, and copy into the NPM database. | | Perform procedure Transferring patches to the NPM database manually on page 1664 in this document. |
| Apply the patches to the Network Patch Manager (NPM). | | Perform procedure Applying patches using the NPM on page 1674 in this document. |
| Restart the NPM to enable the applied patches. | | Perform procedure Restarting a device using the NPM on page 1721 in this document. |

### Preside Multi-service Data Manager

Refer to section “Downloading the Preside MDM software and patches” in the Preside MDM in Succession Network Upgrade Guide, NN10085-461.

### Passport 15000

Refer to section “Installing and downloading Passport 15000 software and patches” in the Passport 15000 in Succession Network Upgrade Guide, NN10070-461.

### Gateway Controller

Patching activities occur when new patches become available and need to be installed and activated. They also occur when an older patch becomes obsolete and must be deactivated and removed.

The table below lists the procedures you must perform to patch the GWC. The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (√) in the √column as you complete each procedure.

***Note:*** Apply all patches to the Gateway Controller (GWC), including the ACT category patches that apply to your site. Contact Nortel customer support to determine which ACT category patches are to be activated in your site. Do not activate any other GWC ACT

category patches unless advised to do so by Nortel customer support.

**Table 8 Patching procedures checklist for the GWC**

| Activities | √ | Procedures |
|---|---|---|
| Audit the GWC unit for existing patch activity. | | Perform procedure Performing a device audit using the NPM on page 1669in this document. |
| Retrieve the patch files from CD or electronically, and copy into the NPM database. | | Perform procedure Transferring patches to the NPM database manually on page 1664 in this document. |
| Apply the patches to the standby GWC unit. | | Perform procedure Applying patches using the NPM on page 1674 in this document. |
| Activate the applicable patches. | | Perform procedure Activating patches using the NPM on page 1690in this document. |
| Take an image of the standby GWC unit. | | Refer to document Upgrading the GWC, NN10196-461. |

### Multi-service Gateway 4000

If you are performing an upgrade with patching, refer to the upgrade procedure in this document. If you are performing maintenance patching, refer to the Post-Release Software Manager (PRSM) Reference Guide, 297-8991-540.

### Media Gateway 9000

The table below provides the procedures you must perform to patch the Media Gateway 9000 (MG 9000). The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (√) in the √column as you complete each procedure.

**Table 9 Patching procedures checklist for the MG 9000**

| Activities | √ | Procedures |
|---|---|---|
| Audit the devices for existing patch activity. | | Perform procedure Performing a device audit using the NPM on page 1669in this document. |
| Retrieve the patch files from CD or electronically, and copy into the NPM database. | | Perform procedure Transferring patches to the NPM database manually on page 1664 in this document. |
| Apply the patches to the MG 9000. | | Perform procedure Applying patches using the NPM on page 1674 in this document. |

***Note:*** As of the SN07 release, you have the capability to perform an image on an MG 9000 device, which allows you to upgrade the remaining MG 9000 devices in the office with the newly imaged load. You also have the capability to schedule imaging so that it occurs automatically. Refer to section Patch management on page 1648 in this document for more details.

**Interworking Spectrum Peripheral Module**

If you are performing an upgrade with patching, refer to the upgrade procedure in this document. If you are performing maintenance patching, refer to the Post-Release Software Manager (PRSM) Reference Guide, 297-8991-540.

**Dynamic Packet Trunking Spectrum Peripheral Module**

If you are performing an upgrade with patching, refer to the upgrade procedure in this document. If you are performing maintenance patching, refer to the Post-Release Software Manager (PRSM) Reference Guide, 297-8991-540.

**Legacy Peripheral Modules**

Refer to the Post-Release Software Manager (PRSM) Reference Guide, 297-8991-540.

**Communication Server 2000**

Refer to the Post-Release Software Manager (PRSM) Reference Guide, 297-8991-540.

## Patch management

The procedures available to manage your patching activities using the Network Patch Manager (NPM), are listed in the table that follows.

**Table 10 Patch management procedures**

| Procedure | Page |
|---|---|
| Defining sets using the NPM | 1729 |
| Saving a task using the NPM | 1735 |
| Setting field values using the NPM | 1740 |
| Defining reports using the NPM | 1745 |
| Defining a plan using the NPM | 1752 |
| Modifying a plan using the NPM | 1759 |
| Deleting a plan using the NPM | 1770 |
| Prioritizing a patching maintenance request using the NPM | 1773 |
| Performing a device image using the NPM | 1683 |

To automate a task, perform procedure Saving a task using the NPM on page 1735 to define the task, for example autoimaging, then perform procedure Modifying a plan using the NPM on page 1759 to include the task you saved, for example autoimaging, in the plan.

# 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 1651 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 1569 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.

# 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 1649 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 1653. You must use this method when launching an application for the first time.
- Launching applications from the JWS Application Manager on page 1656.

  ***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 1659.

  ***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 1662.

***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.

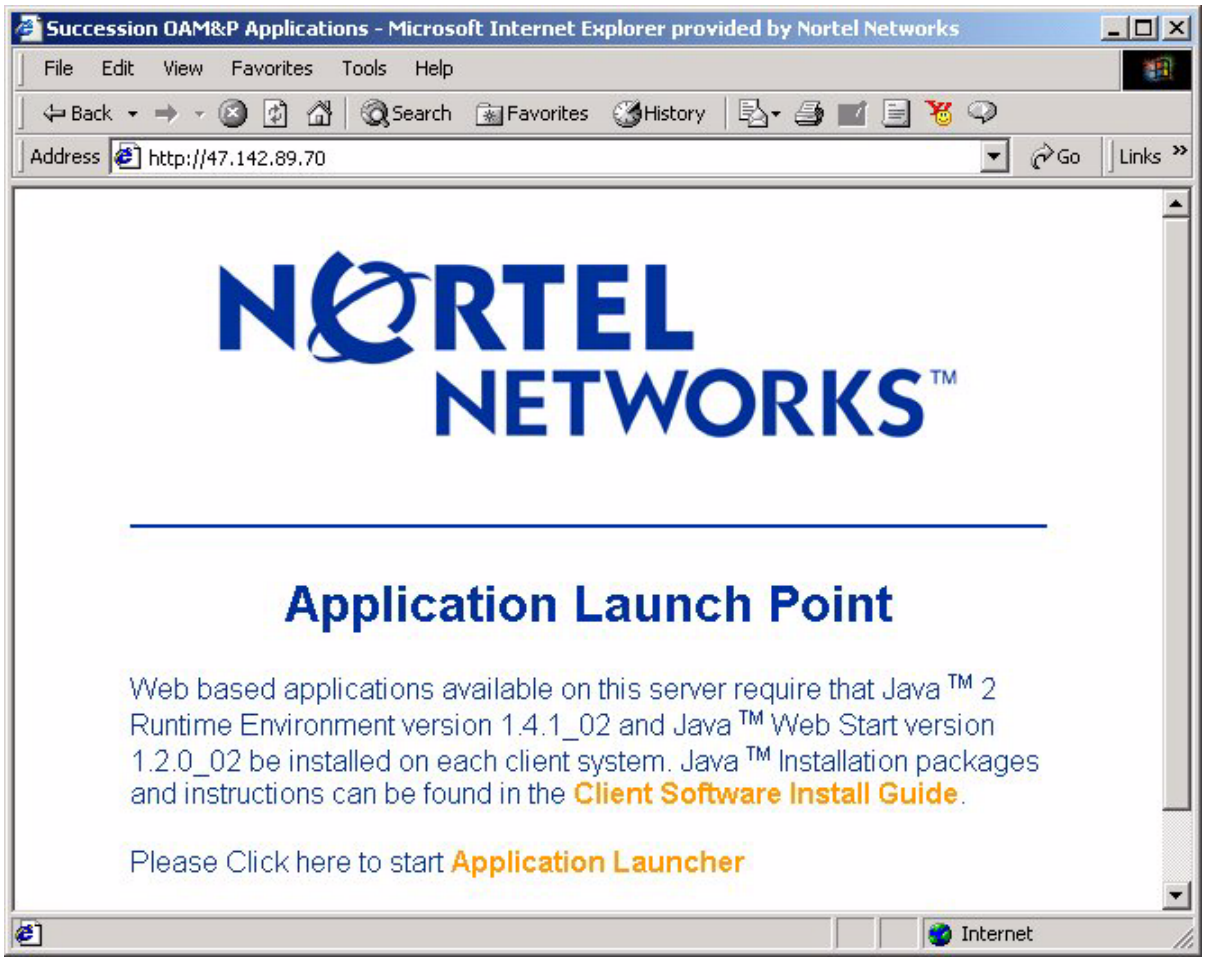
**2** Access the CS 2000 Management Tools server by typing

**>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.

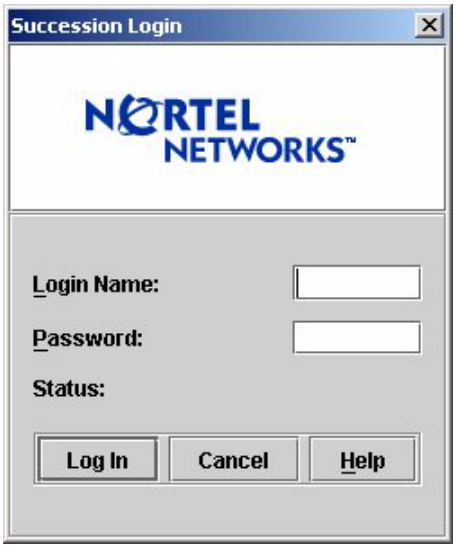
7 Click **Java 2 Runtime Environment Software Download** under “Microsoft Windows” or “Sun Solaris” to download and install the software.

***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”.

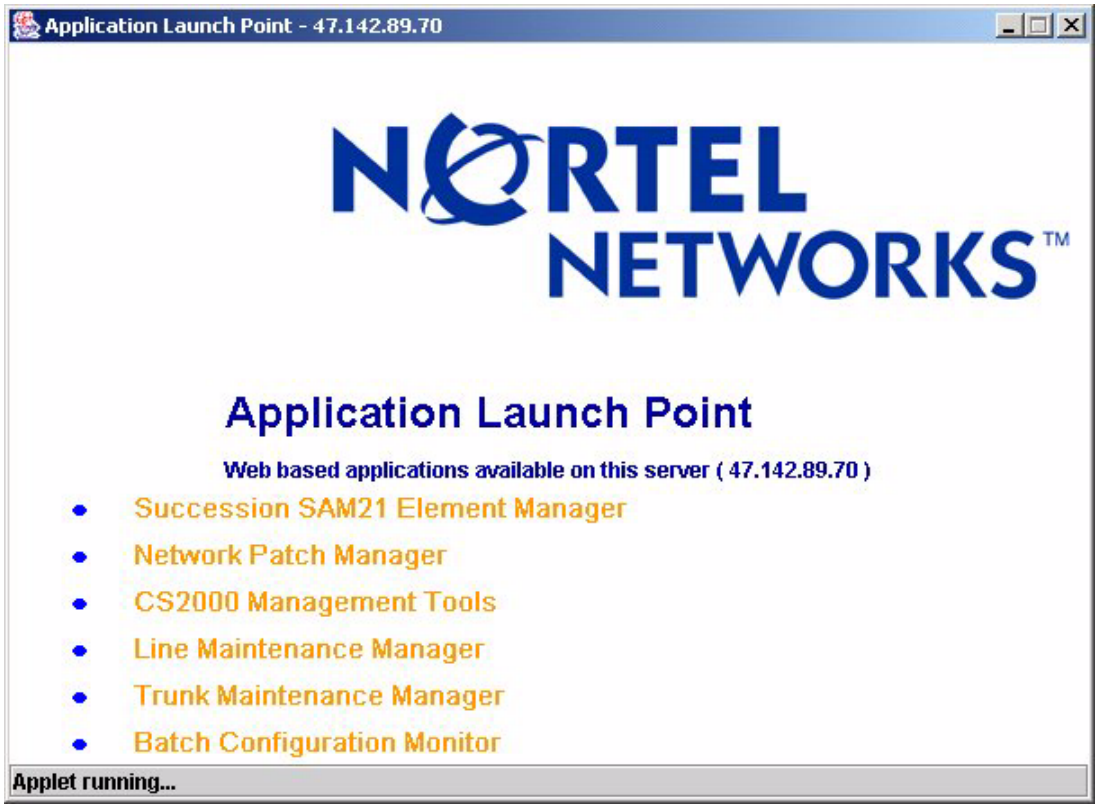
**9** Click **Application Launcher**.

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.

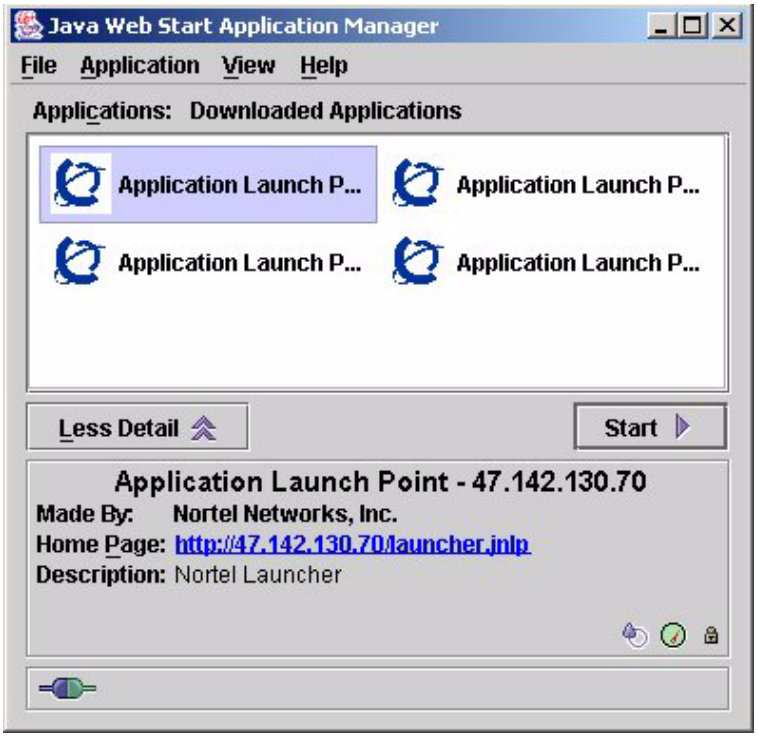
**12** You have completed this procedure.

### 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.

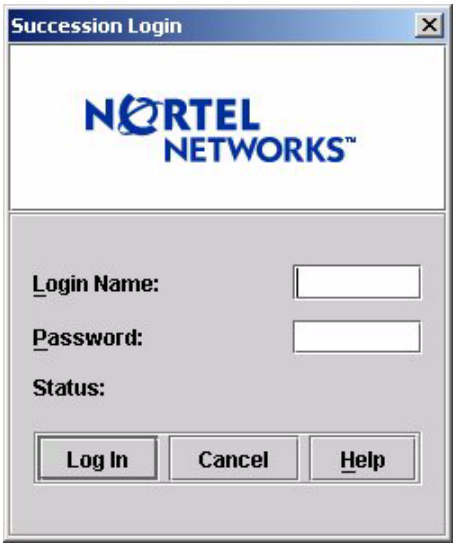



***Note:*** If you do not see the downloaded applications as shown in the example above, on the **View** menu, click **Downloaded Applications**.

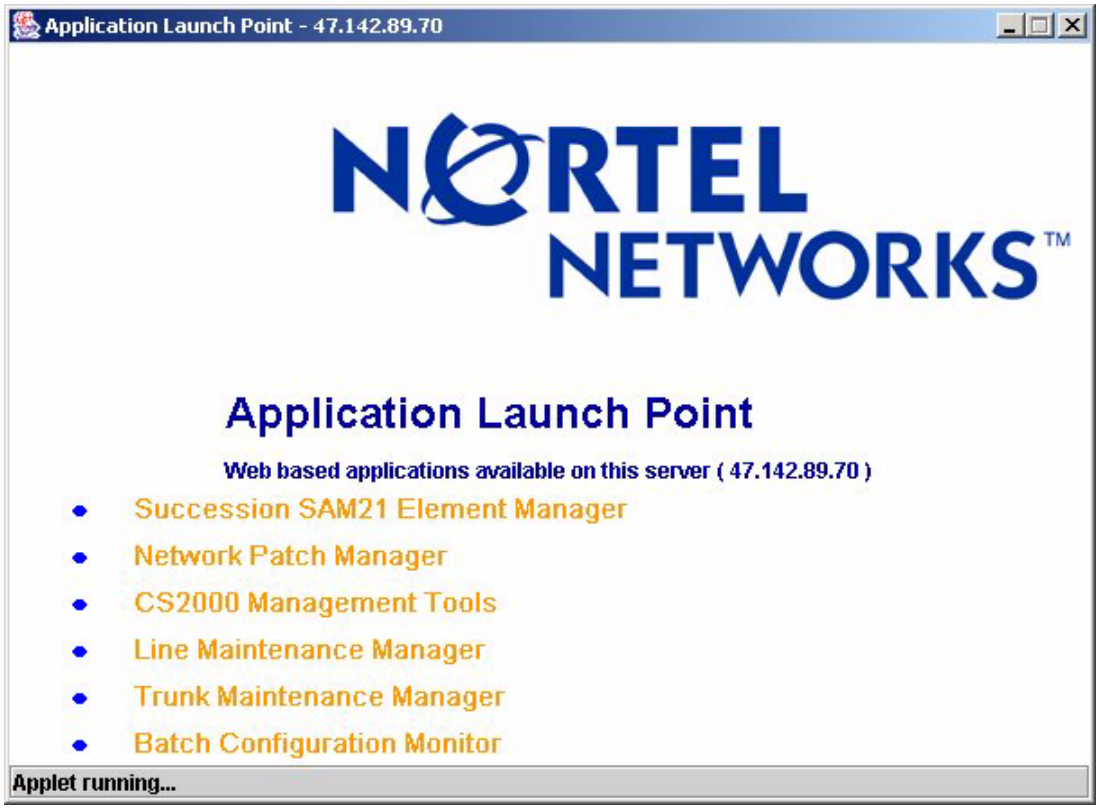
2 Double click on the Application Launch Point you want to access, or select the Application Launch Point and click **Start**.

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)

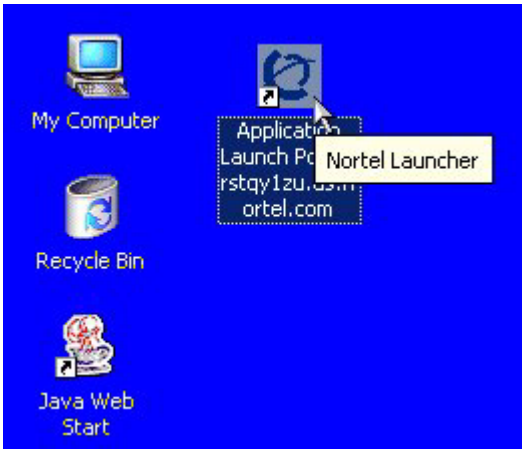
**ATTENTION**
You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

### *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.

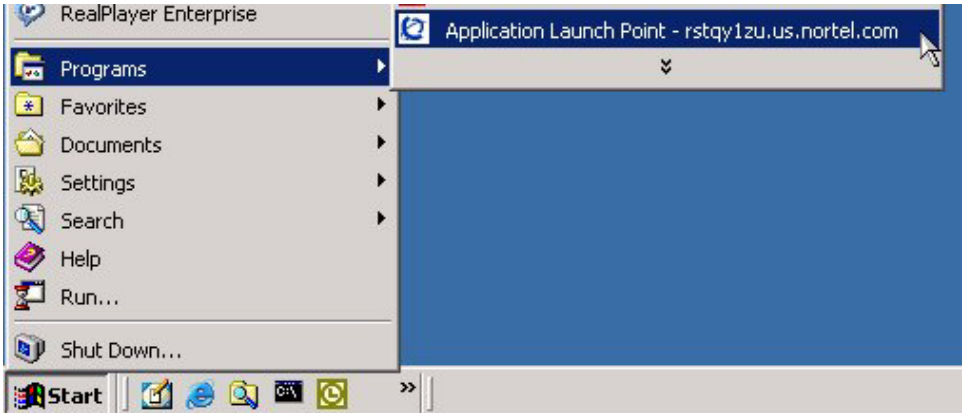



The Login window appears.

Proceed to step 2.

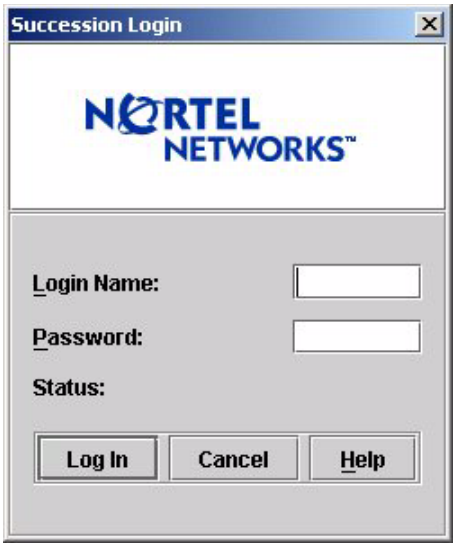
OR

**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.

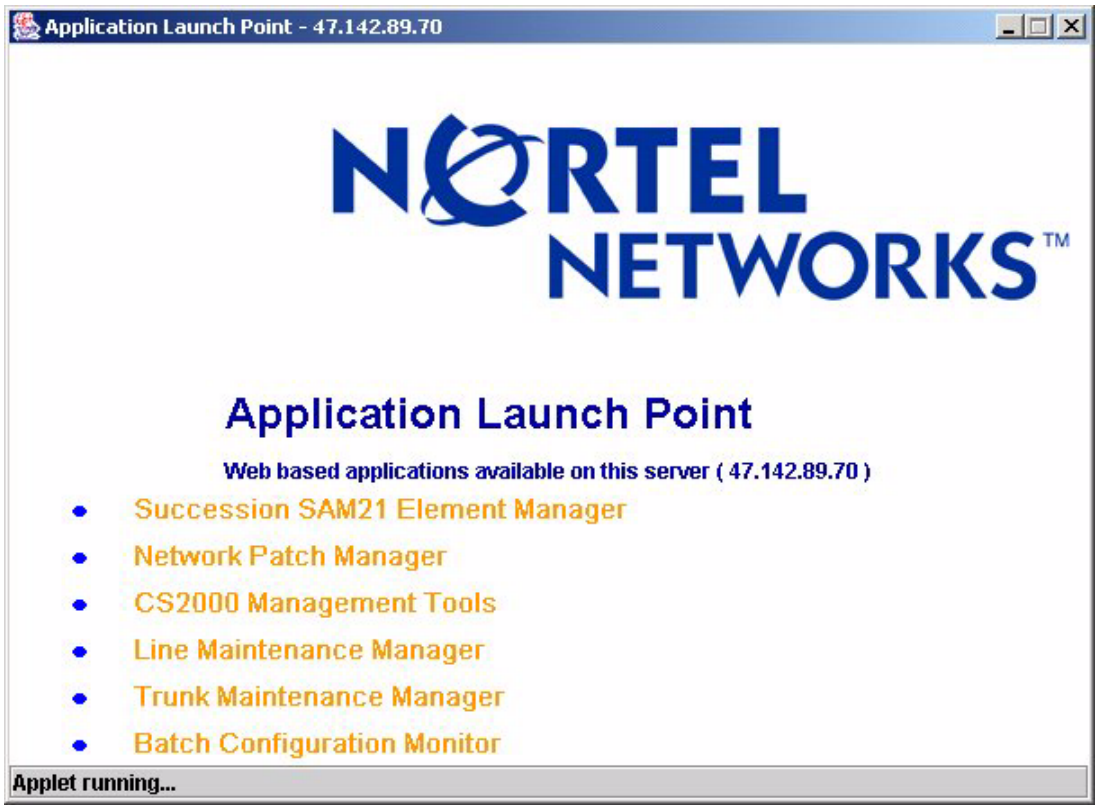



The Login window appears.

**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 1653.

### *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:

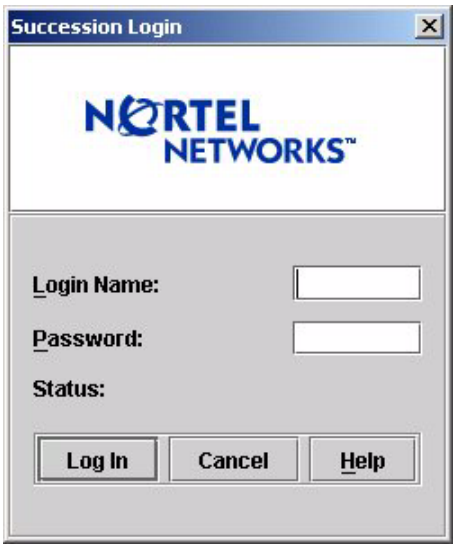
| Application | URL |
|---|---|
| CS2000 Management Tools | http://<host>/:8080/launch/servlet/Launch?app=sesm |
| Line Maintenance Manager | http://<host>/:8080/launch/servlet/Launch?app=lmm |
| Trunk Maintenance Manager | http://<host>/sesm/tmm.html |
| Batch Configuration Monitor | http://<host>/sesm/bpt.html |
| 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.

# Transferring patches to the NPM database manually

## Application

Use this procedure to manually transfer patches to the Network Patch Manager (NPM) database and retrieve them for processing. Patches can be delivered either on a CD or electronically.

***Note:*** You can enable automatic patch file delivery to the NPM database, including patch retrieval for processing, by enabling the Patch File Receipt System (PFRS). Refer to procedure “Configuring NPM for automatic patch file delivery” in the ATM/IP Solution-level Configuration Management document, NN10409-500, to enable PFRS or determine if it is already enabled.

Also use this procedure when you are attempting to audit or apply patches that have a blank patch category or patch status field.

## Prerequisites

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 1569 in this document.

## Action

**ATTENTION**
In a two-server configuration, perform this procedure on the Active server.

***At the Sun server***

1 Use the following table to determine how to proceed.

| If patches were delivered | Do |
|---|---|
| on CD | step 2 |
| electronically | step 3 |

2 Insert the CD that contains the patches into the CD drive of the Sun server where NPM resides.

***At your workstation***

**3** 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

**4** When prompted, enter your user ID and password.

**5** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

**6** When prompted, enter the root password.

**7** Use the following table to determine your next step.

| If patches were delivered | Do |
|---|---|
| on CD | step 8 |
| electronically | step 13 |

**8** Make a temporary directory for the patchlist file by typing

```
# mkdir /data/npm/tmp
```

and pressing the Enter key.

**9** Change the permissions on the temporary directory by typing

```
# chmod 777 /data/npm/tmp
```

and pressing the Enter key.

**10** Create the ".patchlist" file for all the patches that are on the CD, in the temporary directory by typing

```
# find /cdrom -name "*.patch" >
/data/npm/tmp/current.patchlist
```

and pressing the Enter key.

**11** Access the directory you just created by typing

```
# cd /data/npm/tmp
```

and pressing the Enter key.

**12** Proceed to step 23.

13 Make a directory for the patch files you want to install by typing

```
# mkdir /data/npm/patch_upgrade
```

and pressing the Enter key.

14 Change the permissions on the newly created directory by typing

```
# chmod 777 /data/npm/patch_upgrade
```

and pressing the Enter key.

15 Access the newly created directory by typing

```
# cd /data/npm/patch_upgrade
```

and pressing the Enter key.

16 FTP to the ESD server by typing

```
# ftp <ESD_server>
```

and pressing the Enter key.

where

**ESD_server**
is the IP address of the ESD server

17 When prompted, enter your user ID and password for the ESD server.

18 Set the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

19 Transfer all the patches from the ESD server to the NPM by typing

```
ftp> mget *.patch
```

and pressing the Enter key.

***Note:*** To transfer individual patch files, enter the following command:

`ftp>` get <patch_filename>

20 Exit FTP by typing

```
ftp> quit
```

and pressing the Enter key.

**21** Verify the patches are in the temporary directory on the Sun server by typing

```
# ls
```

and pressing the Enter key.

**22** Change permissions for the patch files in the directory by typing

```
# chmod 777 *
```

and pressing the Enter key.

**23** Verify the NPM server application is running by typing

```
# servquery -status -group NPM
```

and pressing the Enter key.

| If the NPM server application is | Do |
|---|---|
| not running | step 24 |
| running | step 25 |

**24** Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

**25** Access the NPM command line user interface (CLUI) by typing

```
# npm
```

and pressing the Enter key.

**26** When prompted, enter your user ID and password.

***Note:*** Do not change directory.

**27** Retrieve the patch files for the NPM to process as follows

| If | Type |
|---|---|
| You want to retrieve the patch files copied from the CD | npm> **getpatch current.patchlist** |
| You want to retrieve the patch files copied from the electronic service delivery system (ESD) | npm> **getpatch <patch_filename>** |

and press the Enter key.

where

**patch_filename**
is either the name of the file that contains names of the patch files to retrieve (must end with ".patchlist"), or an actual patch file

**28** Exit the NPM CLUI by typing

npm> **quit**

and pressing the Enter key.

**29** Change directory by typing

# **cd**

and pressing the Enter key.

***Note:*** You must change directory from the cdrom directory using the "cd" command for the "eject cdrom" command to execute successfully.

**30** Eject the CD from the drive by typing

# **eject cdrom**

and pressing the Enter key.

| If you have | Do |
|---|---|
| other patch CDs | insert the next CD and go to step 10 |
| no other patch CDs | close the cdrom tray |

**31** You have completed this procedure.

# Performing a device audit using the NPM

## Application

Use this procedure to perform a device audit using the Network Patch Manager (NPM). You can perform a device audit using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1669
- Using the NPM GUI on page 1670

It is recommended that you perform an audit on devices prior to patching.

An audit determines whether the NPM database has accurate device patch information. If the patch category or patch status fields are blank for any patches, complete procedure Transferring patches to the NPM database manually on page 1664 if required.

## Prerequisites

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 1569 if required.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 if required.

### *At the NPM CLUI*

**2** Audit the device by typing

`npm> auditd <devices>`

and pressing the Enter key.

where

**devices**
is a list of one or more device IDs for which you want to run the audit - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

**Example**
`npm> auditd` GWC-8-UNIT-1

**3** You have completed this procedure.

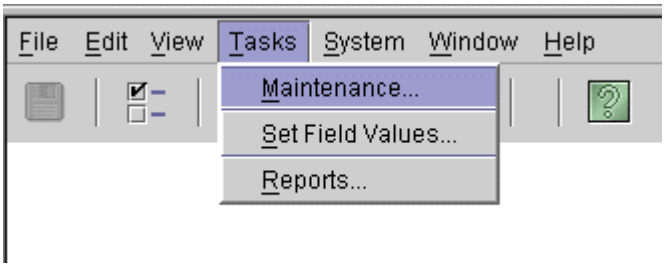
## Using the NPM GUI

### *At your workstation*

**1** Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 if required.

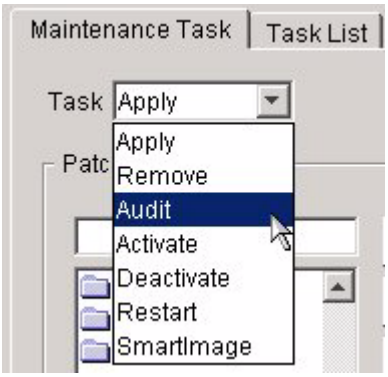
### *At the NPM GUI*

**2** On the **Tasks** menu, click **Maintenance...**.

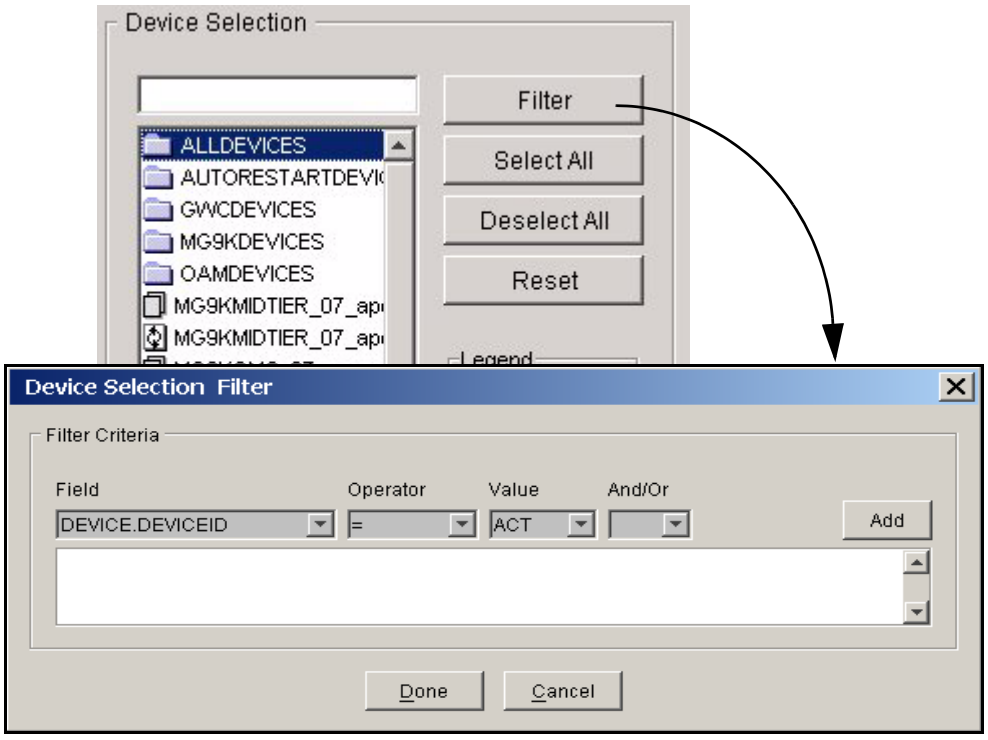



The Maintenance window is displayed.

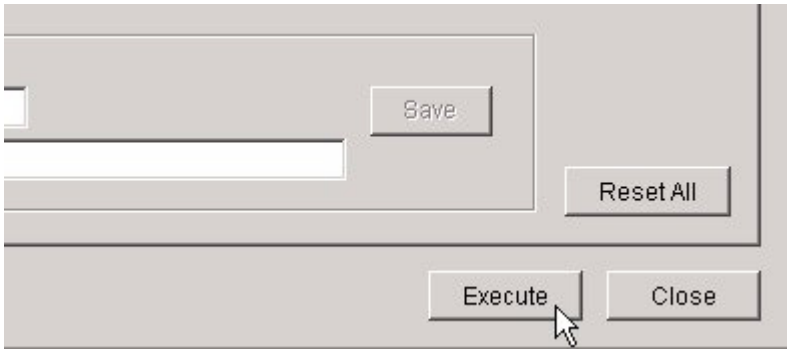
3 In the **Task** list, click **Audit**.



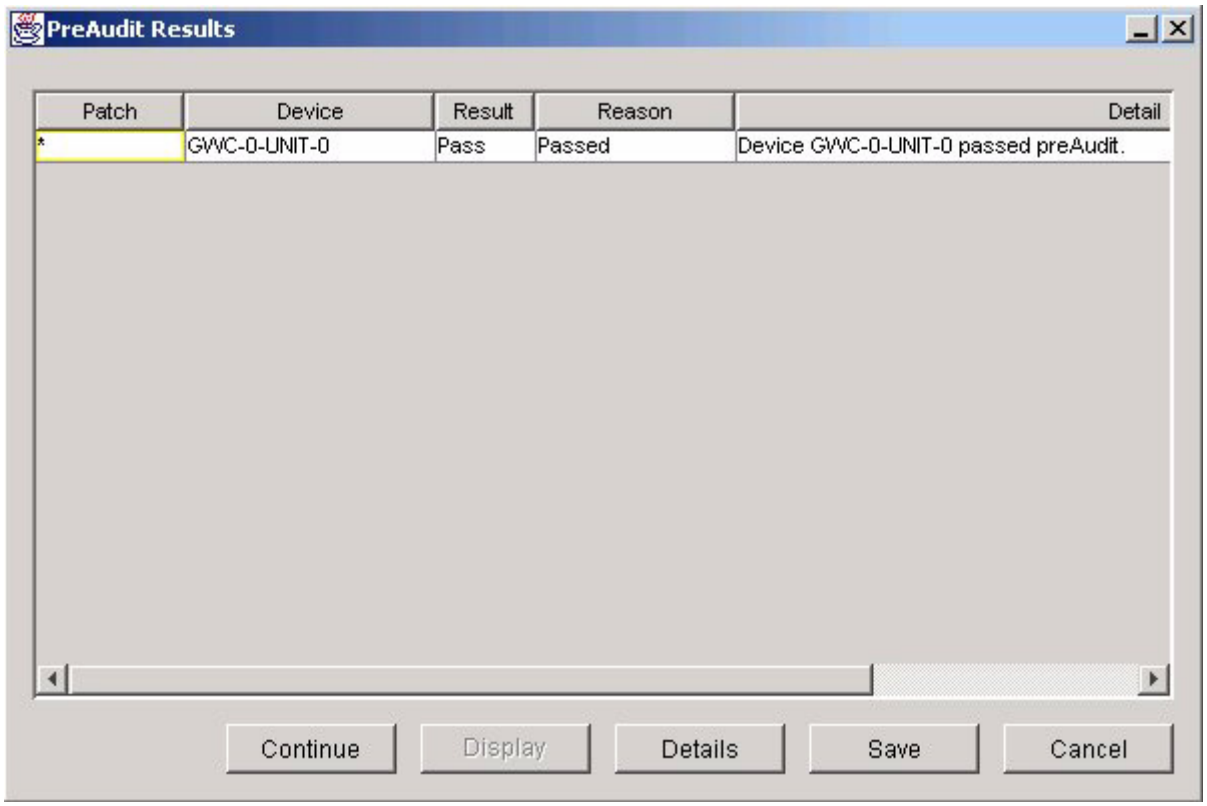

4 In the **Device Selection** list, select the devices or device sets you want to audit, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.



5 Click the **Execute** button to begin the audit process.



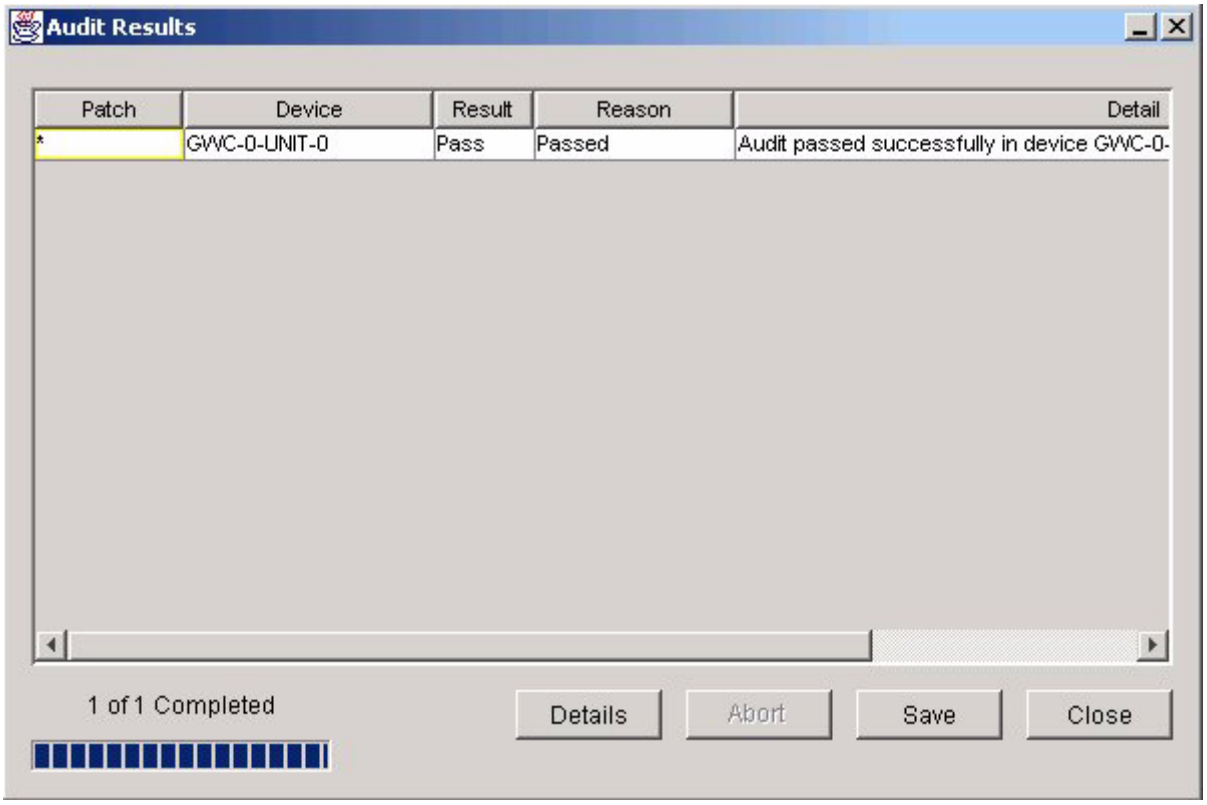

The results of the PreAudit phase are displayed.




6 Review the PreAudit Results, then click **Continue** to proceed.

***Note:*** The Patch field in the Results Table will indicate an asterisk (*) for each operation since only the device is related to the operation.

The Audit Results window is displayed with results added as each action is completed. Failures from the PreAudit phase are also included in the results.




7 Click **Save** to save the results to a file, or click **Close**.

***Note:*** If the audit does not successfully complete, abort the audit procedure and contact your next level of support.

8 You have completed this procedure.

# Applying patches using the NPM

## Application

Use this procedure to apply patches using the Network Patch Manager (NPM). You can apply patches using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

## Prerequisites

The patches must have already been transferred to the NPM database. Contact your network administrator to determine if this has already been done. If required, refer to procedure Transferring patches to the NPM database manually on page 1664 to transfer the patches to the NPM database.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the ATM/IP Administration and Security document, NN10402-600.

It is recommended that you perform an audit on the devices prior to patching. Refer to procedure Performing a device audit using the NPM on page 1669 if required.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 if required.

***At the NPM CLUI***

**2** Apply one or more patches to one or more devices by typing

```
npm> apply <patches> [in <devices>]
```

and pressing the Enter key.

where

**patches**
is a list of one or more patch IDs you want to apply - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

**devices**
is a list of one or more device IDs to which you want to apply the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and applies them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

***Note:*** Enclose the <deviceid> for GWC devices in single quotes (‘).

**Example**
`npm> apply` ACT02GAX in ‘gwc3 Unit 1 47.142.108.39’

**3** When prompted, press the Enter key.

**4** Generate a device query report to verify the patches are applied by typing

```
npm> q device
```

**5** Enter the device name in the format **‘<deviceid>’** that you input in step 2.

***Note:*** The GWC <device id> must be enclosed in single quotes (‘) only when the GWC device id has spaces, dashes or periods as part of its name.

A device report of known patch activity for the particular device associated with the <device id> is returned.

6 Verify from the report that the desired patches are applied (status =A).

***Note:*** If the patches do not successfully apply, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

If you applied patches to any of the following devices, you need to restart the device in order to enable the patches on the device:

- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager (NPM)

To restart a device, refer to procedure Restarting a device using the NPM on page 1721 if required.

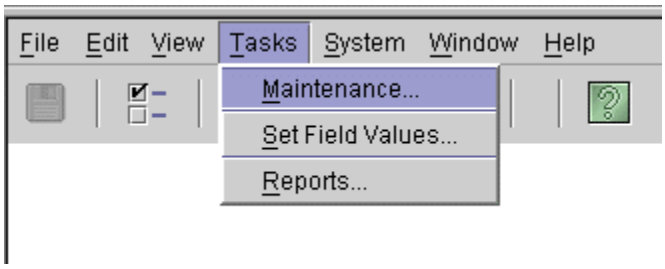
## Using the NPM GUI

### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 if required.

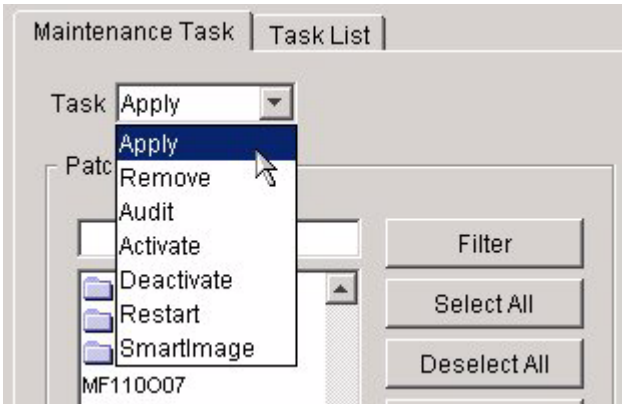
### *At the NPM GUI*

2 On the **Tasks** menu, click **Maintenance...**.

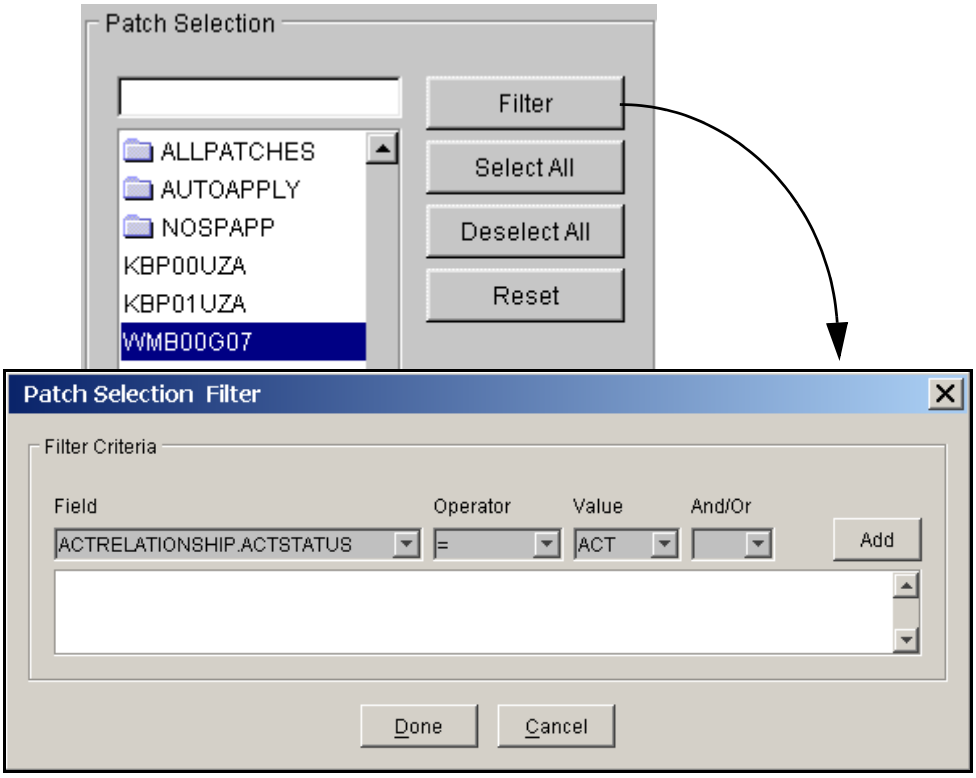



The Maintenance window is displayed.

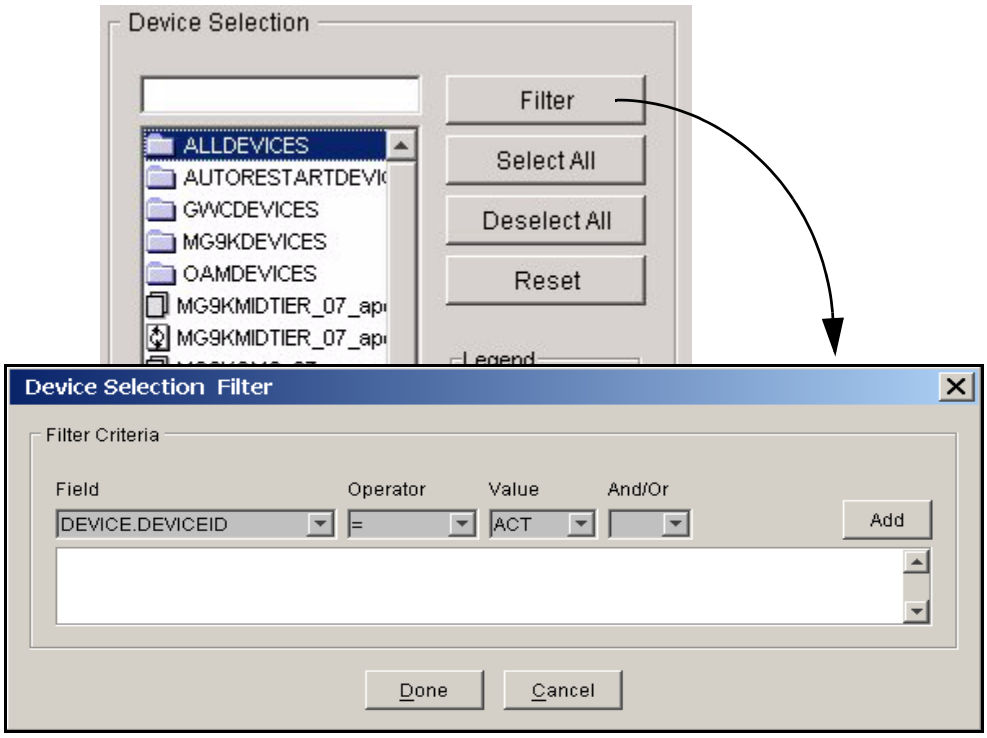
3 In the **Task** list, click **Apply**.



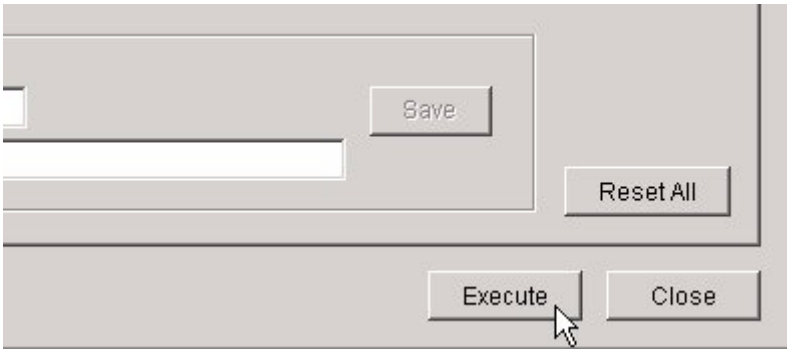
4 In the **Patch Selection** list, select the patch files or patch sets you want to apply, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box.



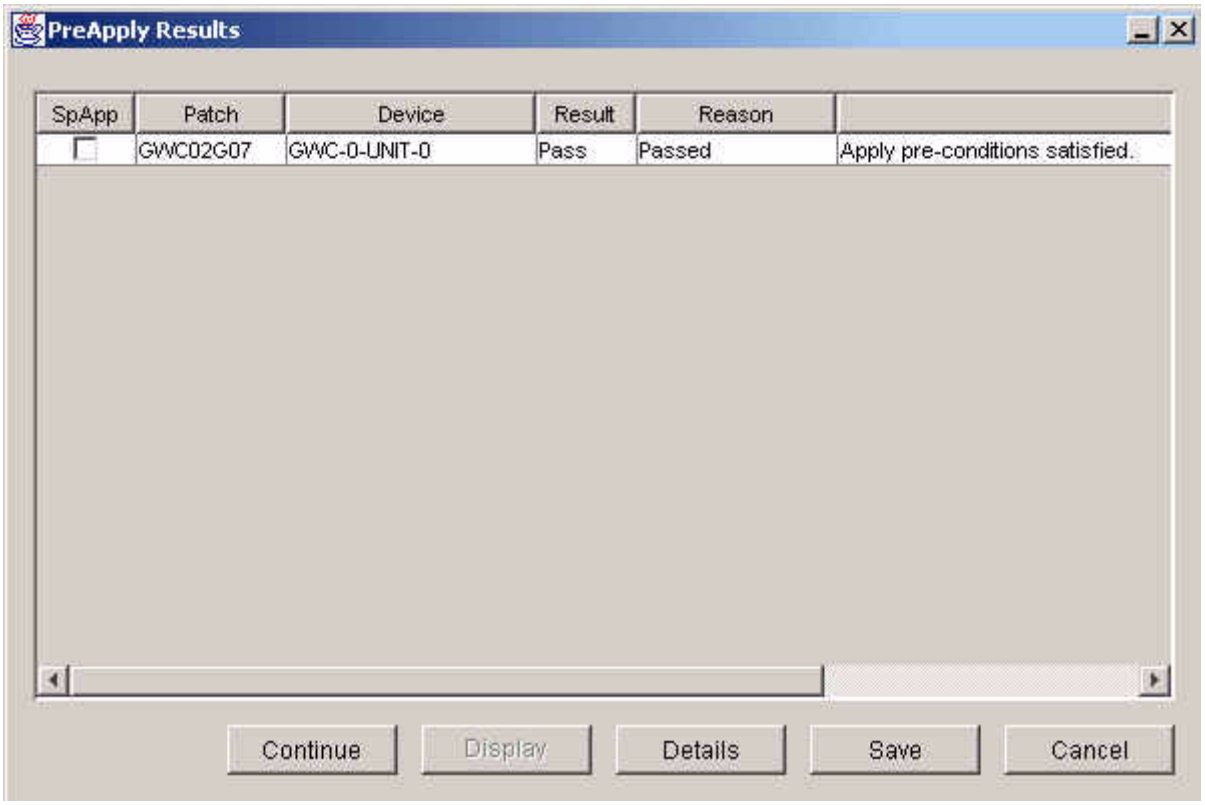
5 In the **Device Selection** list, select the devices or device sets to which you want to apply the patches, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.



6 Click **Execute** to begin the patching process.



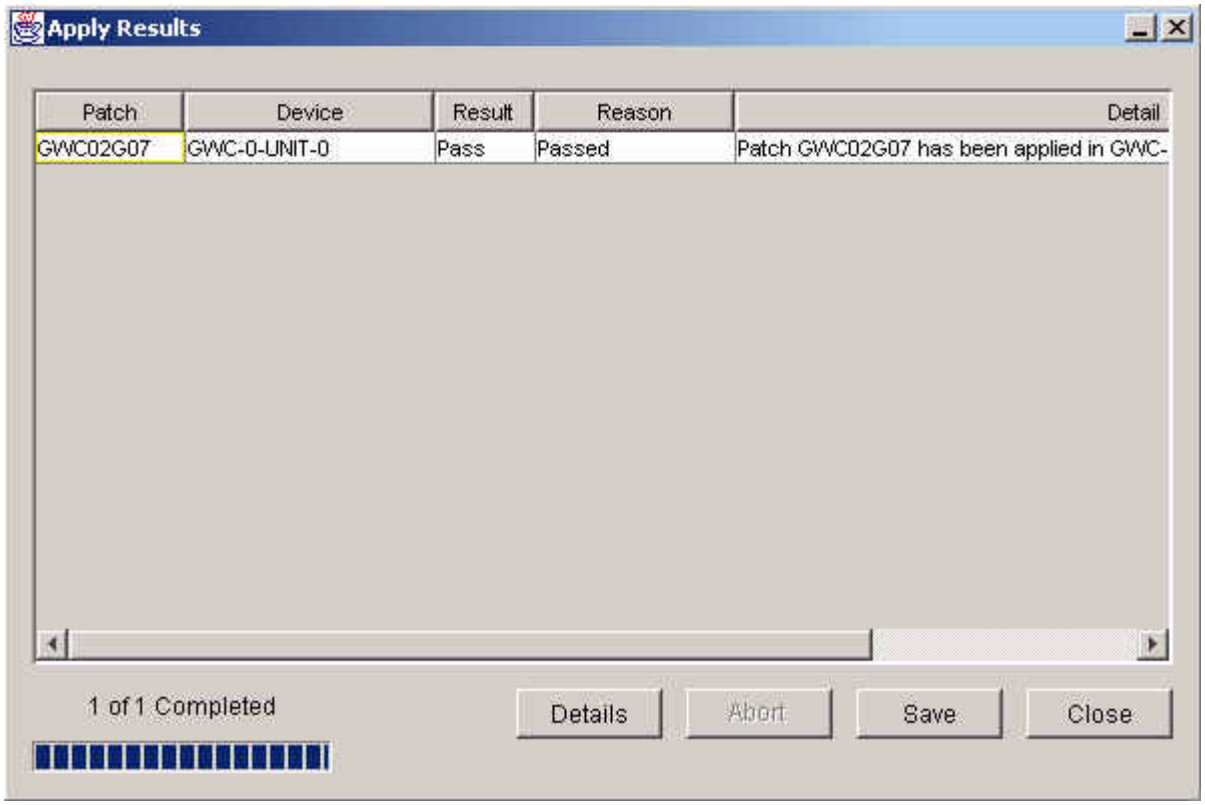

The results of the PreApply phase are displayed.



7 Review the PreApply Results, then click **Continue** to proceed.

***Note:*** If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Apply Results window is displayed with results added as each action is completed. Failures from the PreApply phase are also included in the results.




8 Click **Save** to save the results to a file, or click **Close**.

***Note:*** If the patches do not successfully apply, abort the patching procedure and contact your next level of support.

**9** You have completed this procedure.

If you applied patches to any of the following devices, you need to restart the device in order to enable the patches on the device:

- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager (NPM)

To restart a device, refer to procedure Restarting a device using the NPM on page 1721 if required.

# Performing a device image using the NPM

## Application

Use this procedure to perform a device image using the Network Patch Manager (NPM). You can perform a device image using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1684
- Using the NPM GUI on page 1685

***Note:*** Performing a device image using the SmartImage command, is only supported for MG 9000 devices at this time.

Performing an image on an MG 9000 device allows you to upgrade the remaining MG 9000 devices in the office with the newly imaged load.

**ATTENTION**
The SmartImage command, used to perform a device image, should be used in offices where all MG 9000 devices of the same type are patched with the same patches. It is not intended for use in offices where the MG 9000 devices of the same type use a different set of patches.

For imaging to occur automatically, you can save the SmartImage command as a task (refer to procedure Saving a task using the NPM on page 1735 in this document if required), and schedule that task as part of the NPM System Plan (refer to procedure Modifying a plan using the NPM on page 1759 in this document if required).

## Prerequisites

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

**1** Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

**2** Perform a device image by typing

```
npm> smartimage <devices>
```

and pressing the Enter key.

where

**devices**
is a list of one or more device IDs you want to image - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Example

```
npm> smartimage UD16_16_62_OC3_0_2_10
```

***Note:*** It is highly recommended that you use the predefined device set MG9KDEVICES to ensure the image taken is from a the device that contains the highest patch content.

For example

```
npm> smartimage SET MG9KDEVICES
```

*Response*

```
WARNING: You are about to perform a smartimage
on the specified devices. Note that if all
devices for a particular load are not chosen for
imaging, a device may be chosen that does not
contain the highest patch content.
If you wish to continue with this maintenance
request enter Yes (Y or y). Otherwise, just
enter return.
```

3 When prompted, confirm you want to continue with the maintenance request by typing

**y**

and pressing the Enter key.

*Example response:*

```
Patch: *
Device: UD16_16_62_OC3_0_2_10
Result: true
Reason: Passed
Details: SmartImage pre-conditions satisfied.
If you wish to continue with this maintenance
request, enter Yes (Y or y). Otherwise, just
enter return.
```

4 When prompted, confirm you want to continue with the maintenance request by typing

**y**

and pressing the Enter key.

*Example response:*

```
npm>
Patch: *
Device: UD16_16_62_OC3_0_2_10
Reason: Passed
Detail: Device UD16_16_62_OC3_0_2_10 has been
successfully imaged.
```

5 You have completed this procedure.

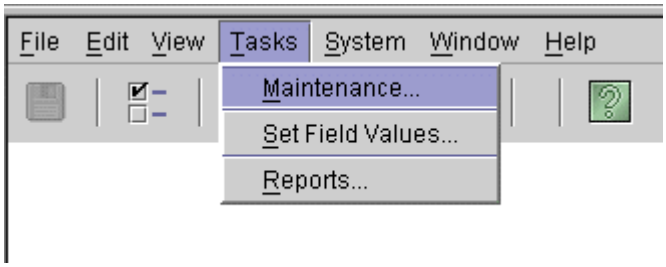
### Using the NPM GUI

#### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

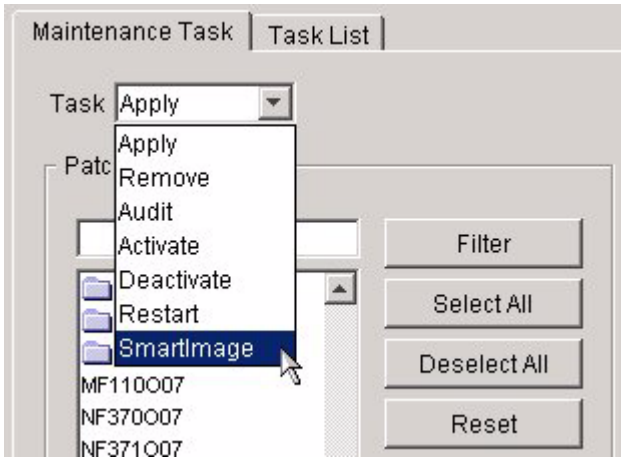
***At the NPM GUI***

**2** On the **Tasks** menu, click **Maintenance...**.

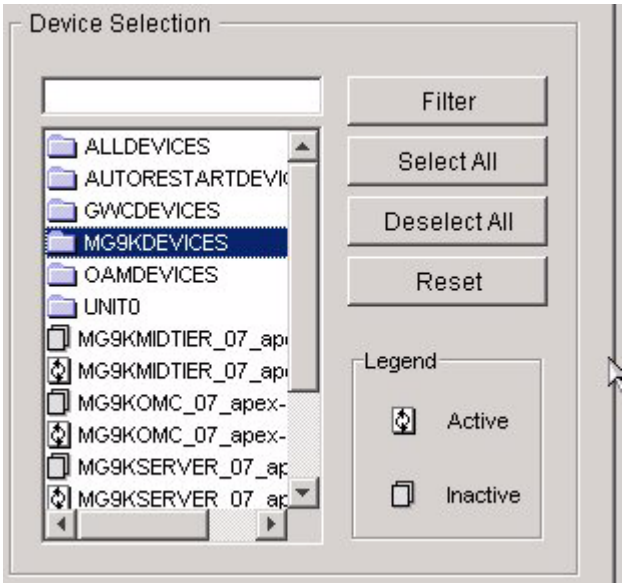



The Maintenance window is displayed.

**3** In the **Task** list, click **SmartImage**.

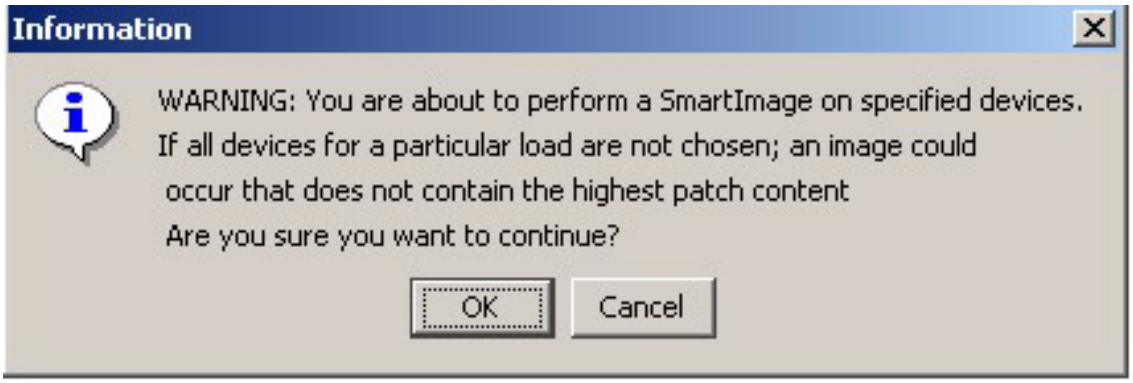


4 In the **Device Selection** list, select the device, device list, or device set that you want to image.



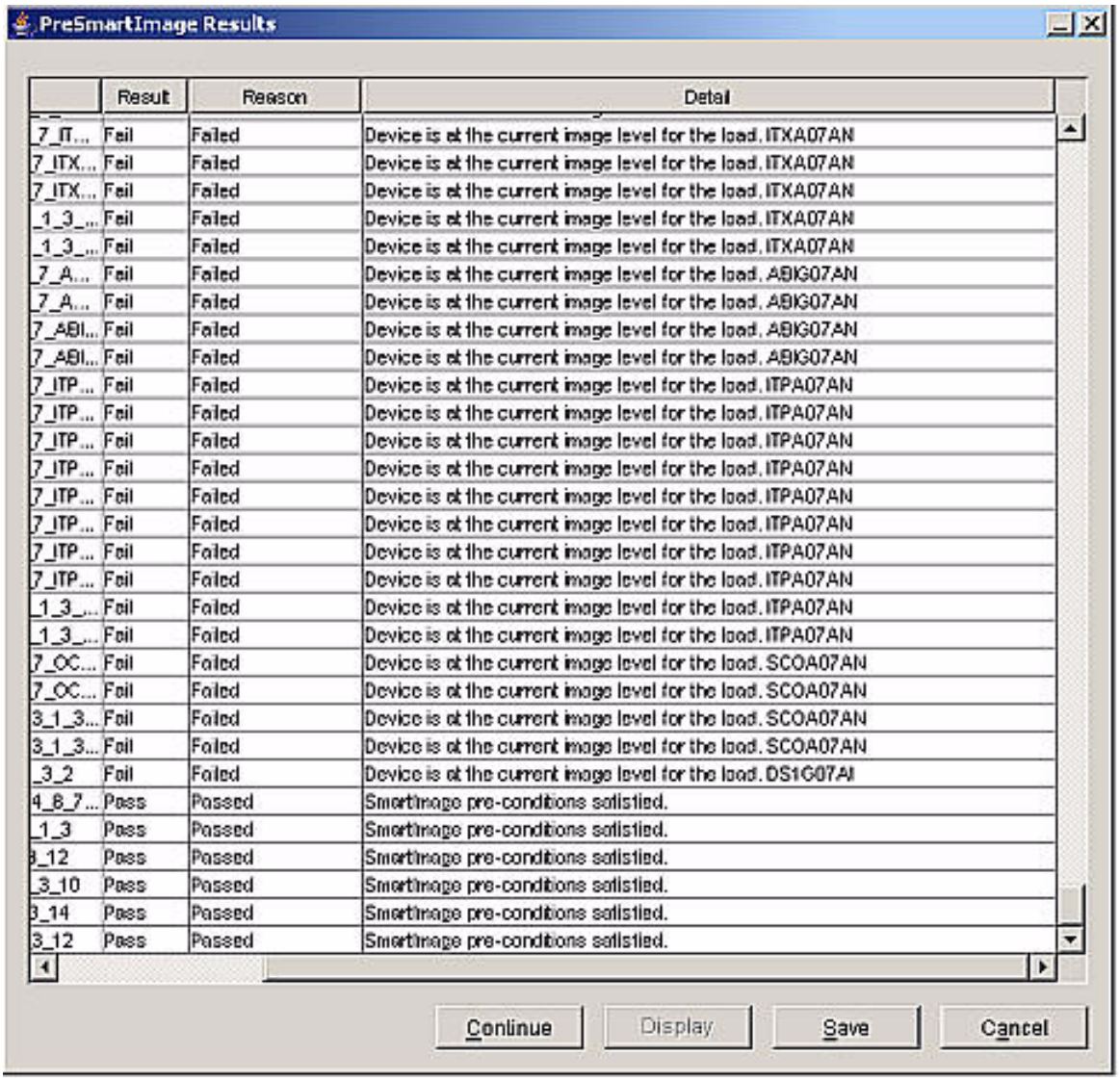

5 Click **Execute** to begin the restart.

The system returns the following warning.



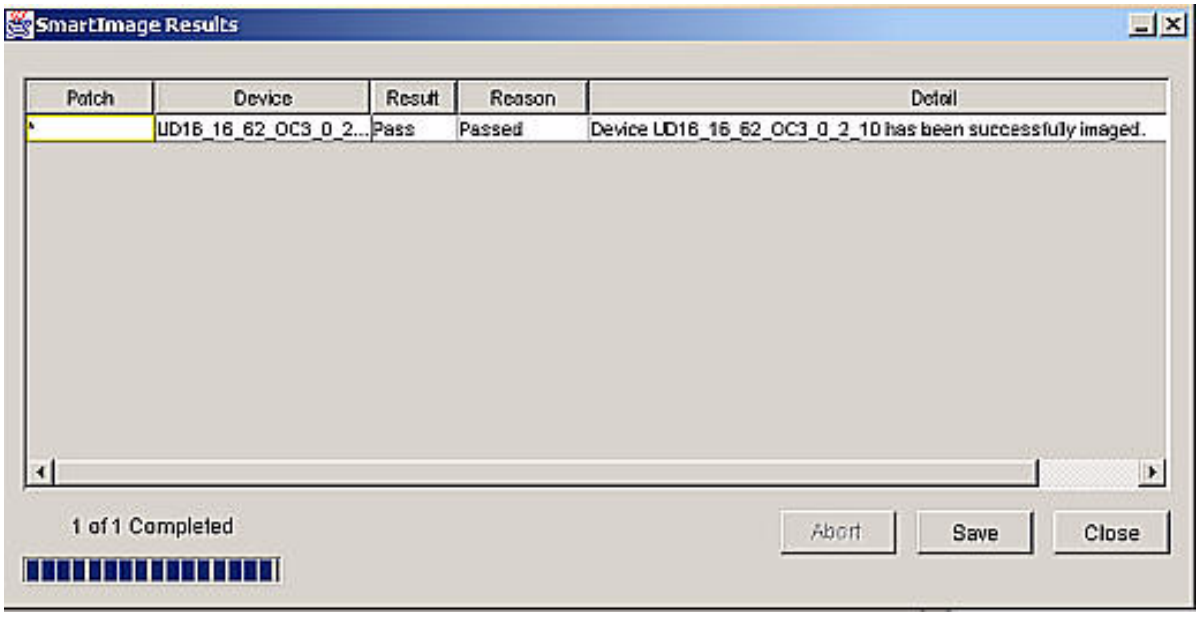
6 If you agree that the devices chosen are the ones you want evaluated, click **OK** to begin imaging.

The results of the PreSmartImage phase are displayed.




7 Review the PreSmartImage Results, then click **Continue** to proceed.

The SmartImage Results window is displayed with results added as each action is completed. Failures from the PreSmartImage phase are also included in the results.




**8** You have completed this procedure.

# Activating patches using the NPM

## Application

Use this procedure to activate patches, which are deemed activatable by the ACT category, using the Network Patch Manager (NPM). You can activate patches using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1691
- Using the NPM GUI on page 1692

***Note:*** Currently, only GWC can have ACT category patches.

**ATTENTION**

Certain GWC patches may be ACT category patches that may require activation. It is important to note that not all ACT category patches require activating. The patches to be activated would depend on the requirements for the GWC load. Prior to activating the ACT category patches, it is important that you read and understand the administration section of the patch and make sure the ACT patch enables the functionality you require. If you are unsure about the impact of activating an ACT patch in your office, contact your next level of support to determine if the patches can be activated.

## Prerequisites

You can activate a patch if all of the following criteria have been fulfilled:

- the patch has been identified by your support team and Nortel as being applicable and necessary for your site
- the patch is not on hold
- the patch has a category of ACT
- the patch has been applied



**CAUTION**

Do not activate patches for your components that have not been identified as needing activation without first consulting with your network administrator and your Nortel customer support representative. Failure to do so can result in partial loss of service.

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

**1** Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

**2** Query the NPM for a list of patches that can be activated by typing

```
npm> q actlist
```

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime. If no patches are in the actlist, then the NPM responds with the message “Empty Results”.

**3** Activate one or more patches for one or more devices by typing

```
npm> activate <patches> [in <devices>]
```

and pressing the Enter key.

where

**patches**
is a list of one or more patch IDs you want to activate - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

**devices**
is a list of one or more device IDs for which you want to activate the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and activates them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

**Example**
`npm> activate` ACT02GAX in GWC-8-UNIT-1

4 When prompted, press the Enter key.

5 Query the NPM to verify the patches are activated by typing

`npm>` **`q actlist`**

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime.

6 Verify from the list that the desired patches are activated.

***Note:*** If the patches do not successfully activate, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

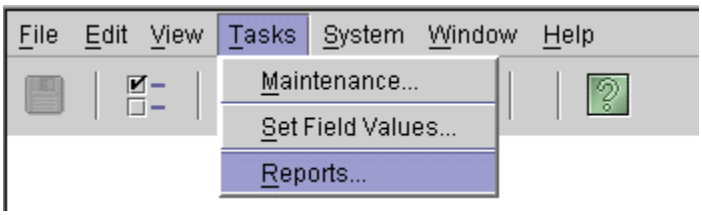
### Using the NPM GUI

#### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

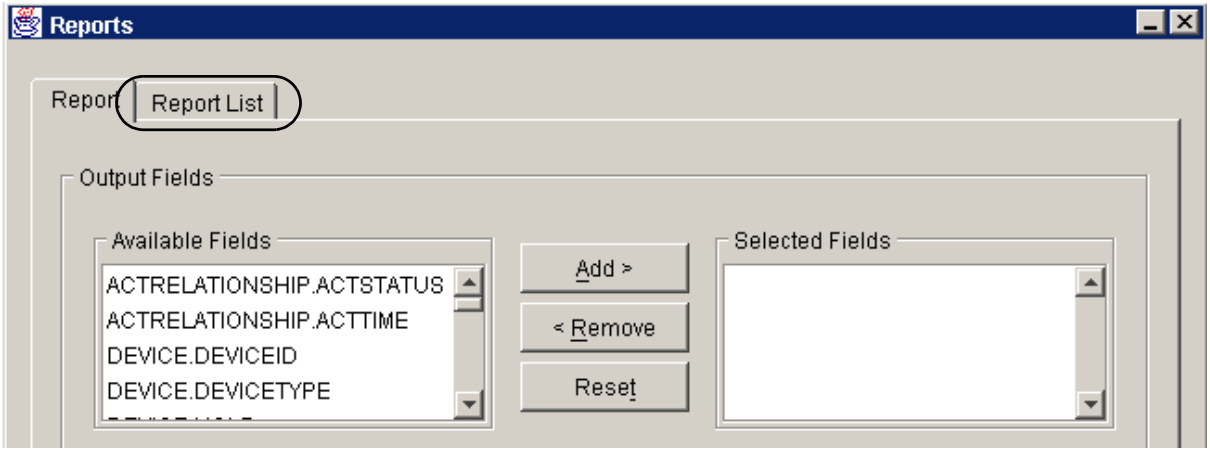
***At the NPM GUI***

**2** On the **Tasks** menu, click **Reports...**.

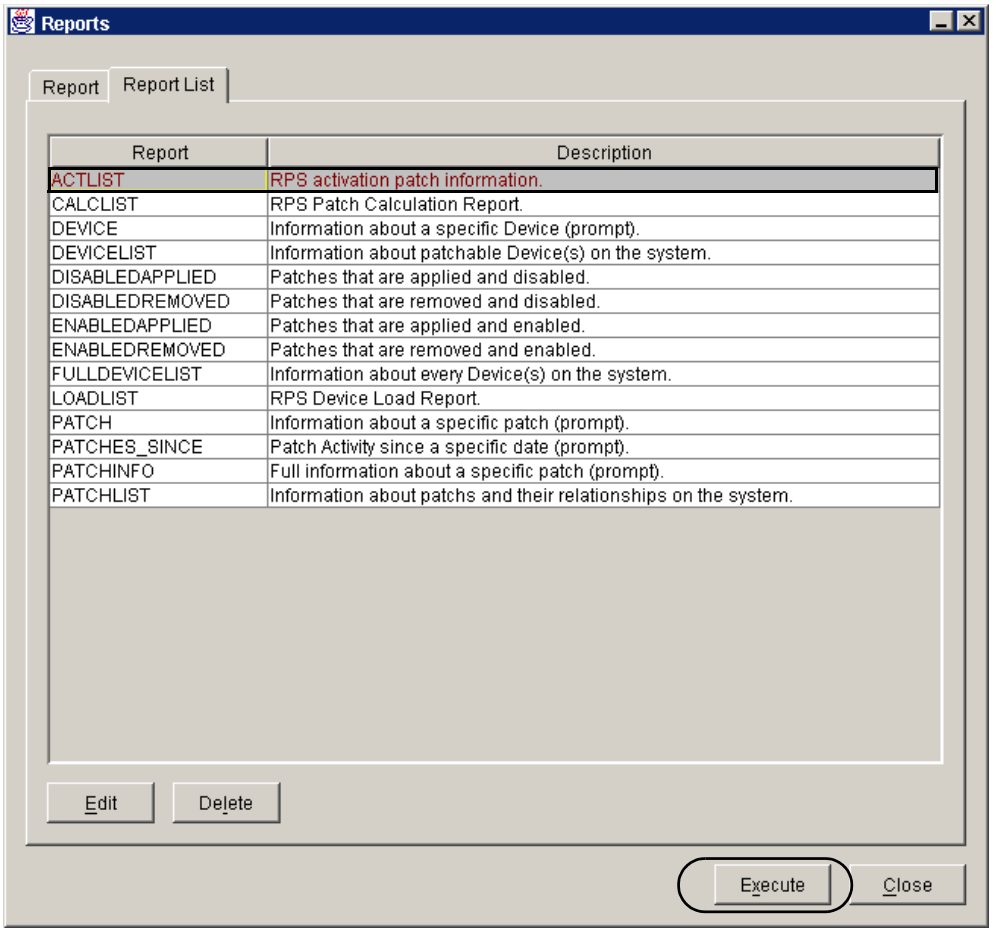



The **Reports** window is displayed.

**3** Click the **Report List** tab.

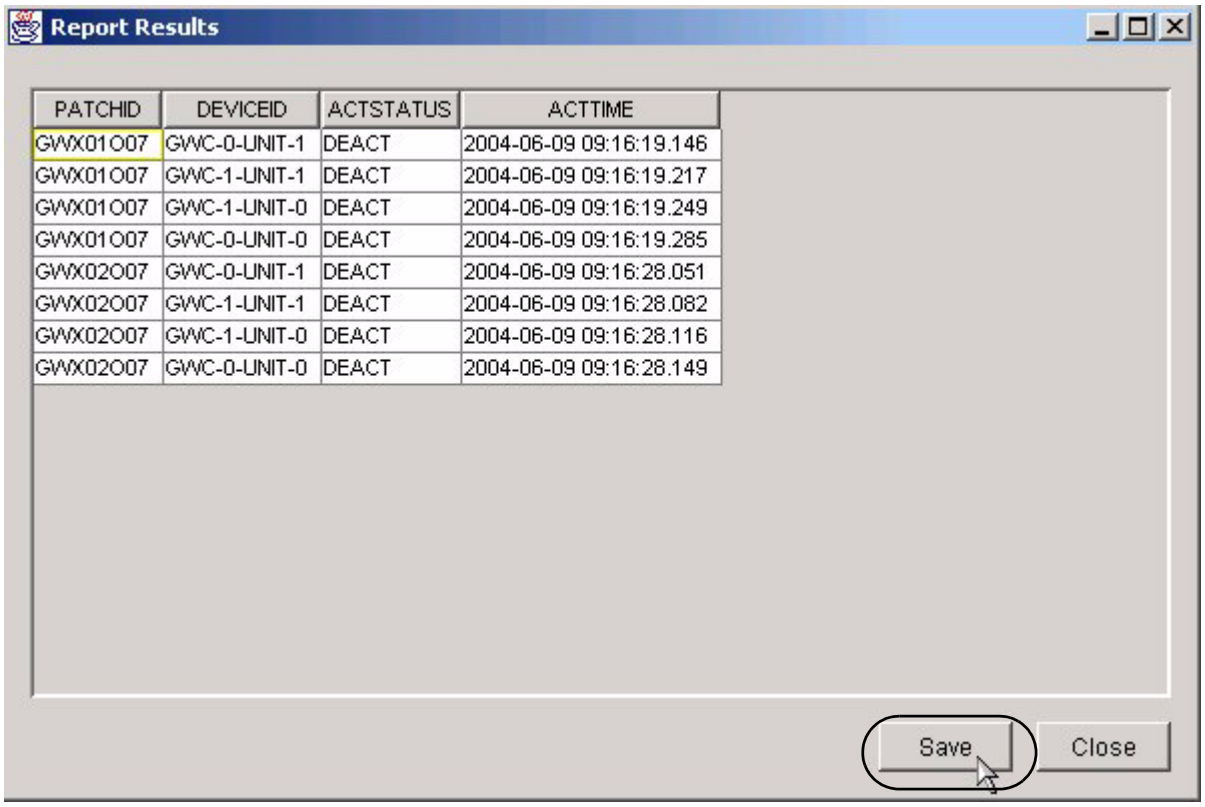


4 Click the **ACTLIST** entry in the **Report** field, then click **Execute**.



5 Review the list of patches displayed, and note which are activated and which are deactivated. Consult with your Nortel customer support representative to determine which patch files are applicable to your site configuration and should be activated.

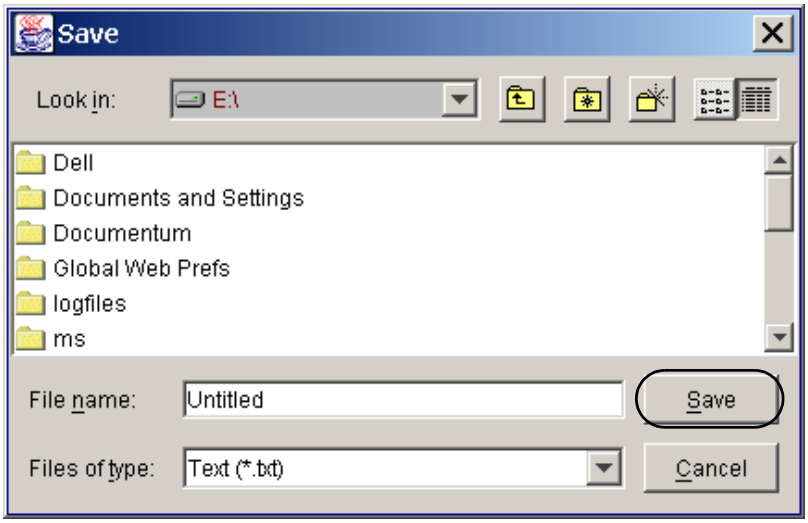
***Note:*** If there are no patches to activate, the system returns a dialog box indicating that the report has “empty results”.



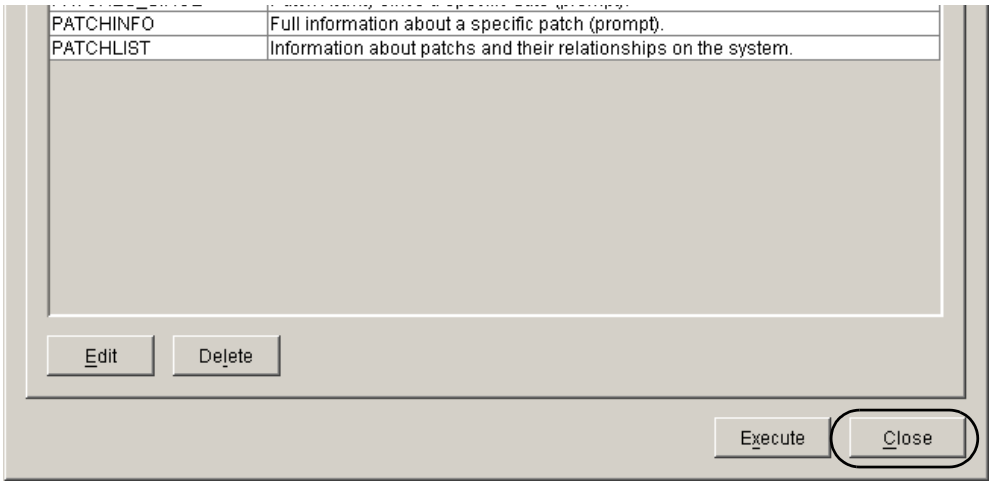

6 If necessary, save a copy of the report to a text file as follows:

**a** Click **Save**.

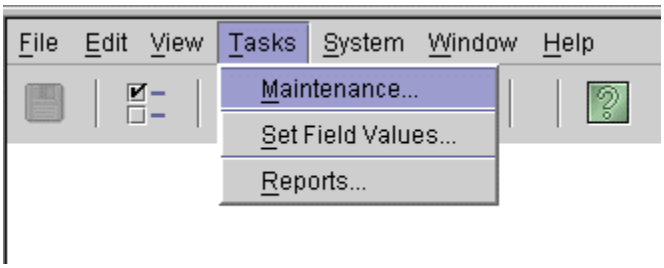
**b** Type a file name in the **File name:** box, and click **Save**.




**7** Click **Close** to close the Reports window.

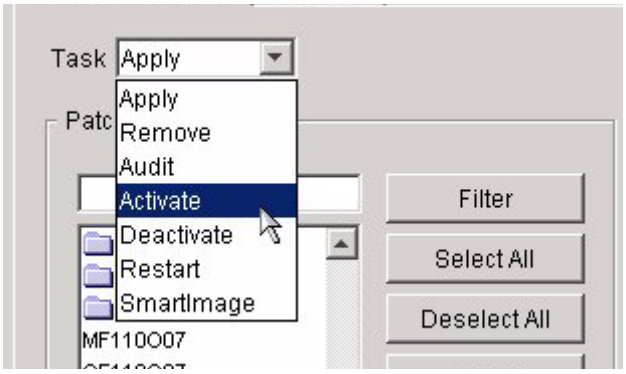



**8** On the **Tasks** menu, click **Maintenance...**.



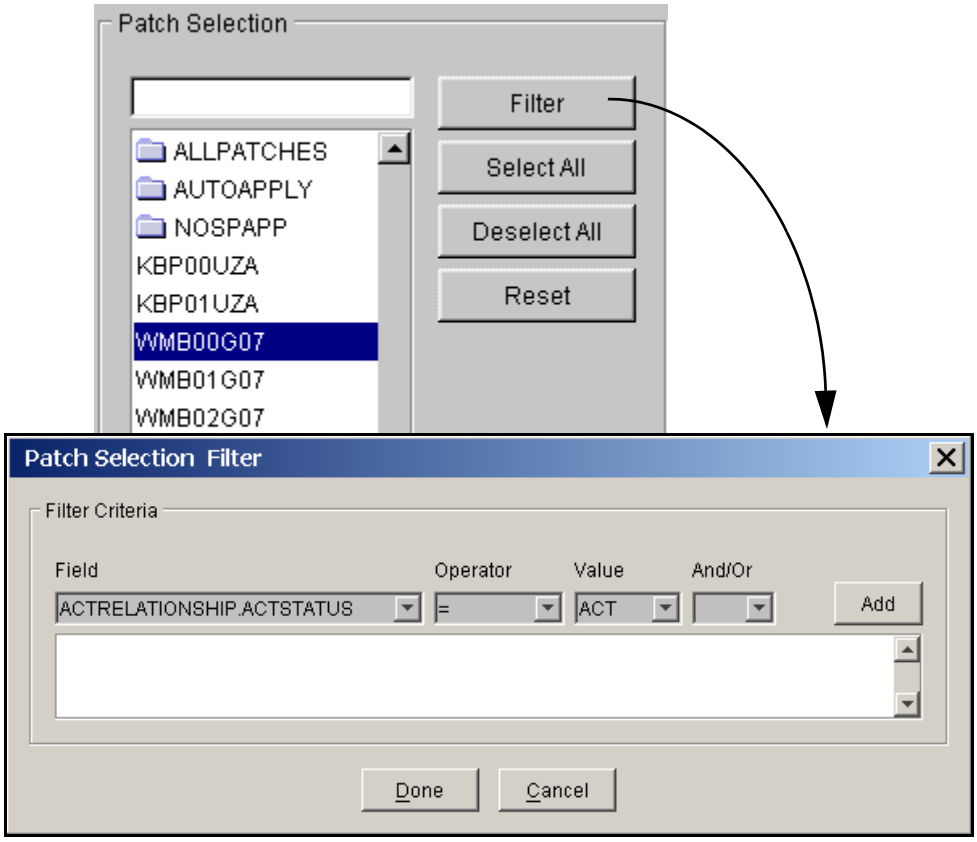

The Maintenance window is displayed.

9 In the **Task** list, click **Activate**.

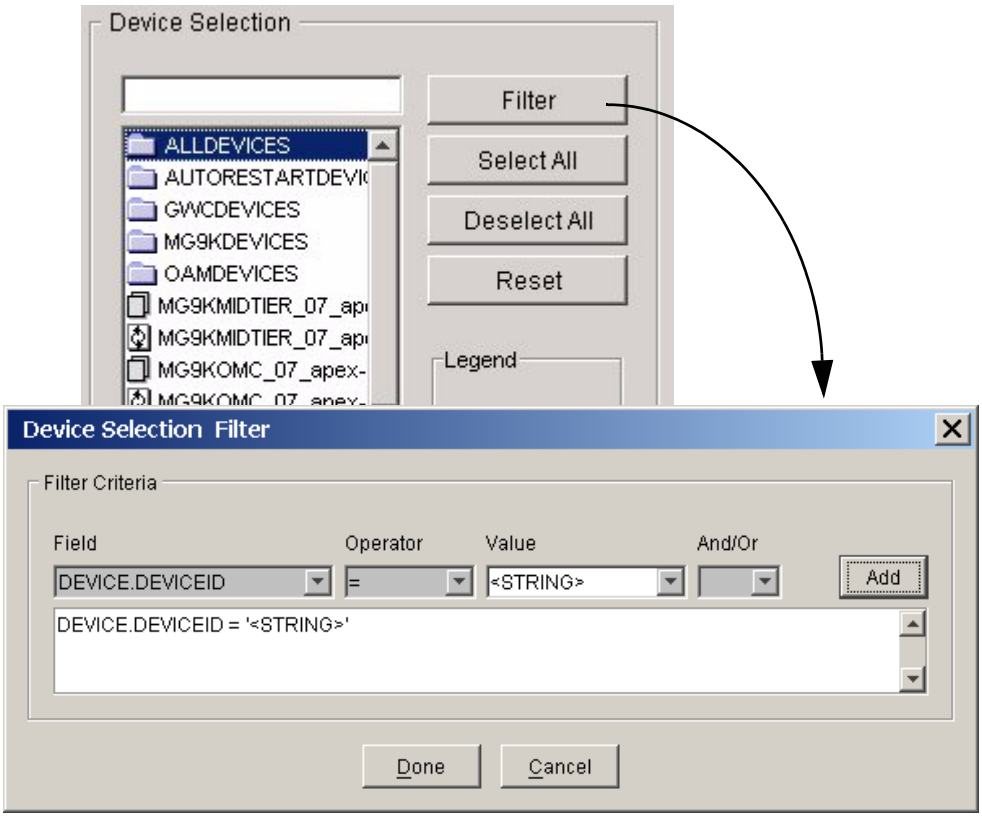



10 In the **Patch Selection** list, select the patch files or patch sets you want to activate, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box.

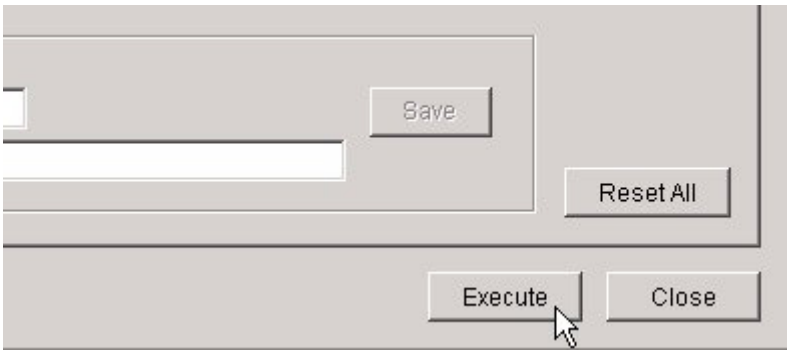
***Note:*** The patches must have a category of ACT.



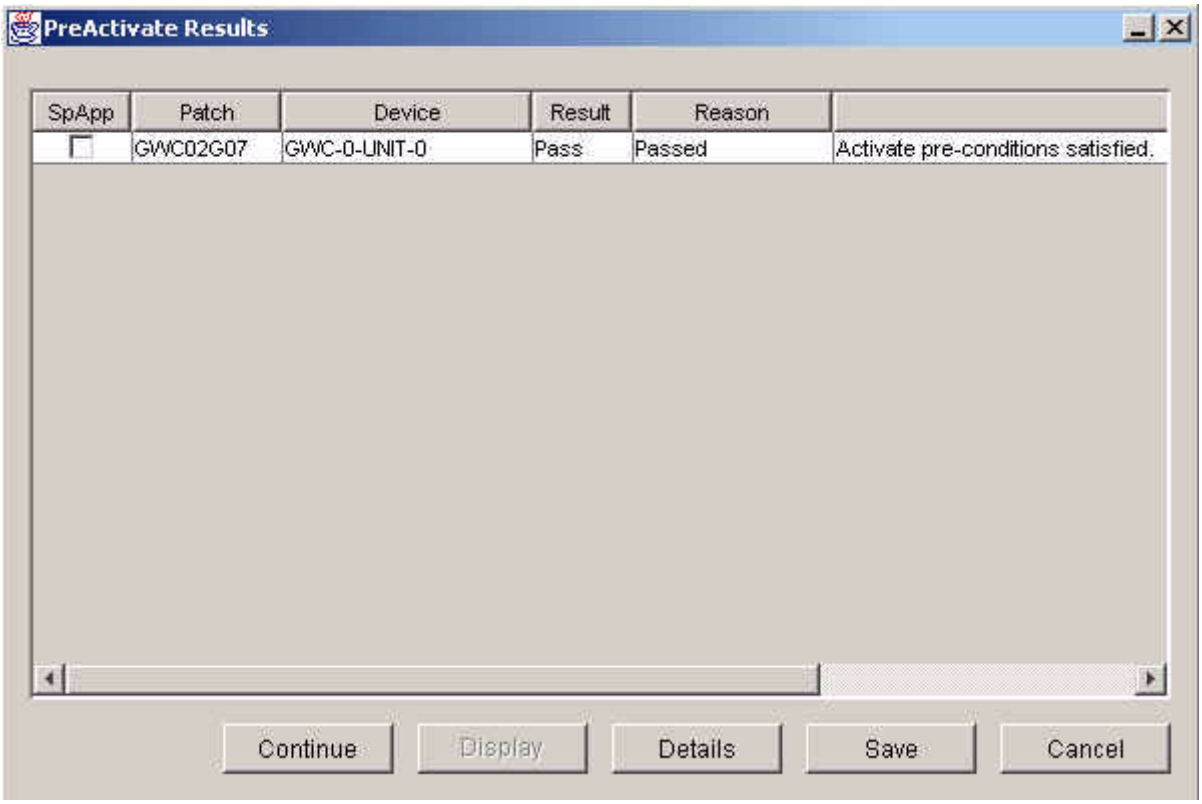
**11** In the **Device Selection** list, select the devices or device sets that have the applied patches you want to activate, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.




**12** Click **Execute** to begin the patch activation process.



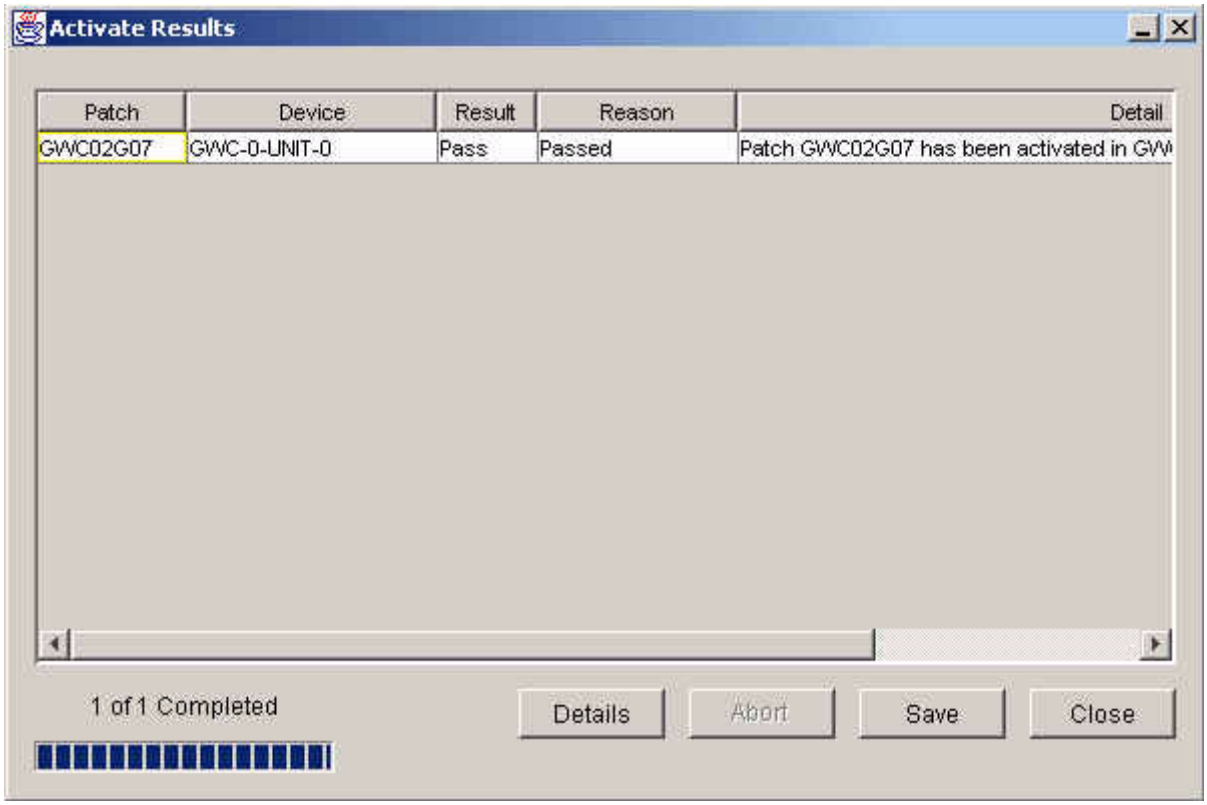

The results of the Pre-activate phase are displayed.




**13** Review the PreActivate Results, then click **Continue** to proceed.

***Note:*** If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Activate Results window is displayed with results added as each action is completed. Failures from the PreActivate phase are also included in the results.




**14** Click **Save** to save the results to a file, or click **Close**.

***Note:*** If the patches do not successfully activate, abort the patching procedure and contact your next level of support.

**15** You have completed this procedure.

# Deactivating patches using the NPM

## Application

Use this procedure to deactivate one or more ACT category patches using the Network Patch Manager (NPM). You can deactivate patches using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1702
- Using the NPM GUI on page 1703

***Note:*** Currently, only GWC can have ACT category patches.

## Prerequisites

You can deactivate a patch if the following criteria apply:

- the patch to be deactivated has been identified by your support team and Nortel as being applicable for your site and be recommended for deactivation
- the patch has been activated
- the patch is not on hold



**CAUTION**

Do not deactivate patches for your components that have not been identified as needing deactivation without first consulting with your network administrator and your Nortel customer support representative. Failure to do so can result in partial loss of service.

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

**1** Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

**2** Query the NPM for a list of patches that are activated by typing

```
npm> q actlist
```

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime. If no patches are in the actlist, then the NPM responds with the message “Empty Results”.

**3** Deactivate one or more patches for one or more devices by typing

```
npm> deactivate <patches> [in <devices>]
```

and pressing the Enter key.

where

**patches**
is a list of one or more patch IDs you want to deactivate - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

**devices**
is a list of one or more device IDs for which you want to deactivate the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and deactivates them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

**Example**
`npm> deactivate` ACT02GAX in GWC-8-UNIT-1

4 When prompted, press the Enter key.

5 Query the NPM to verify the patches are deactivated by typing

`npm>` **`q actlist`**

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime.

6 Verify from the list that the desired patches are deactivated.

***Note:*** If the patches do not successfully deactivate, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

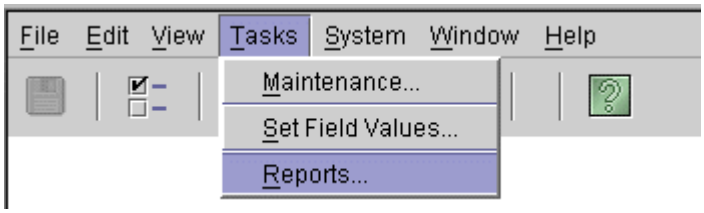
### Using the NPM GUI

#### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

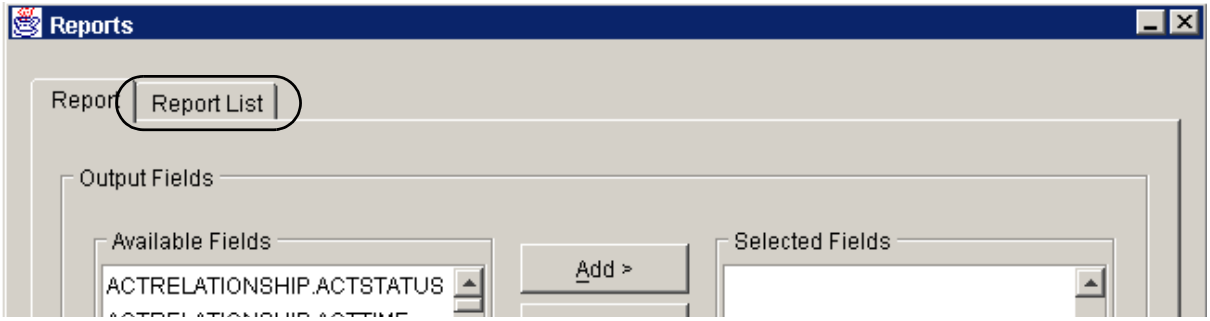
***At the NPM GUI***

**2** On the **Tasks** menu, click **Reports...**.

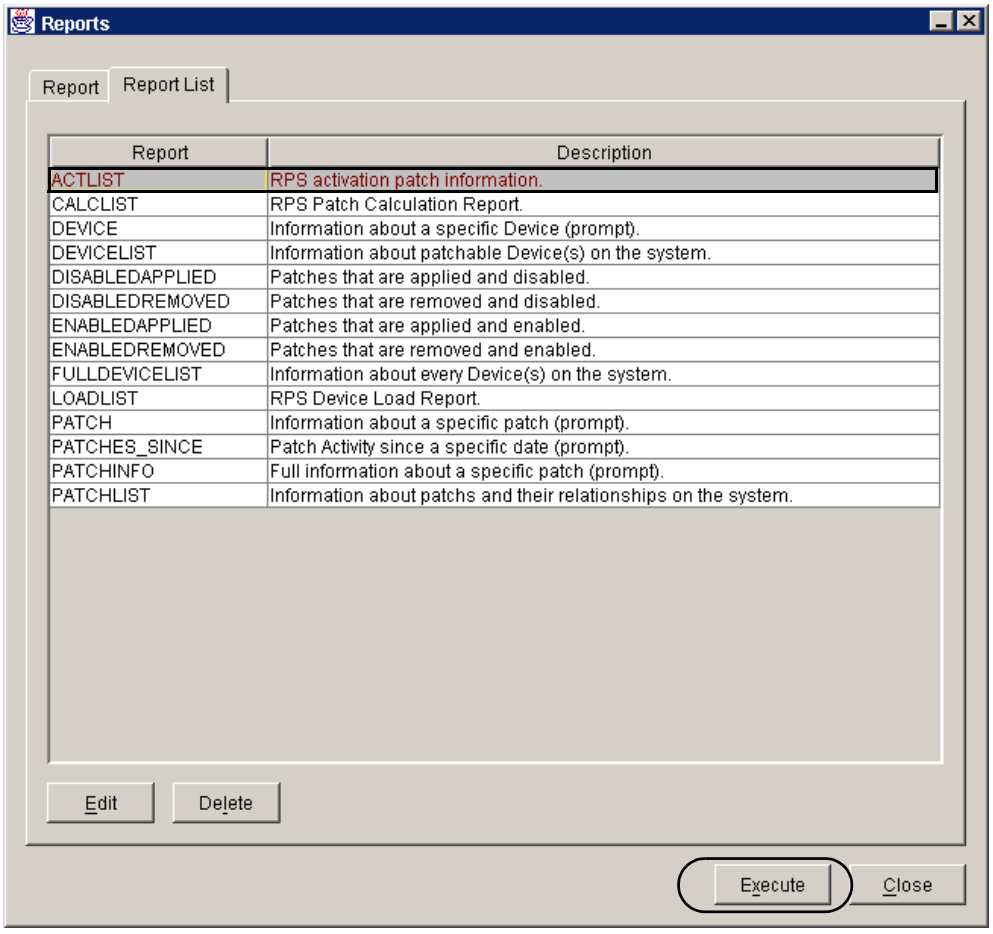



The Reports window is displayed.

**3** Click the **Report List** tab.

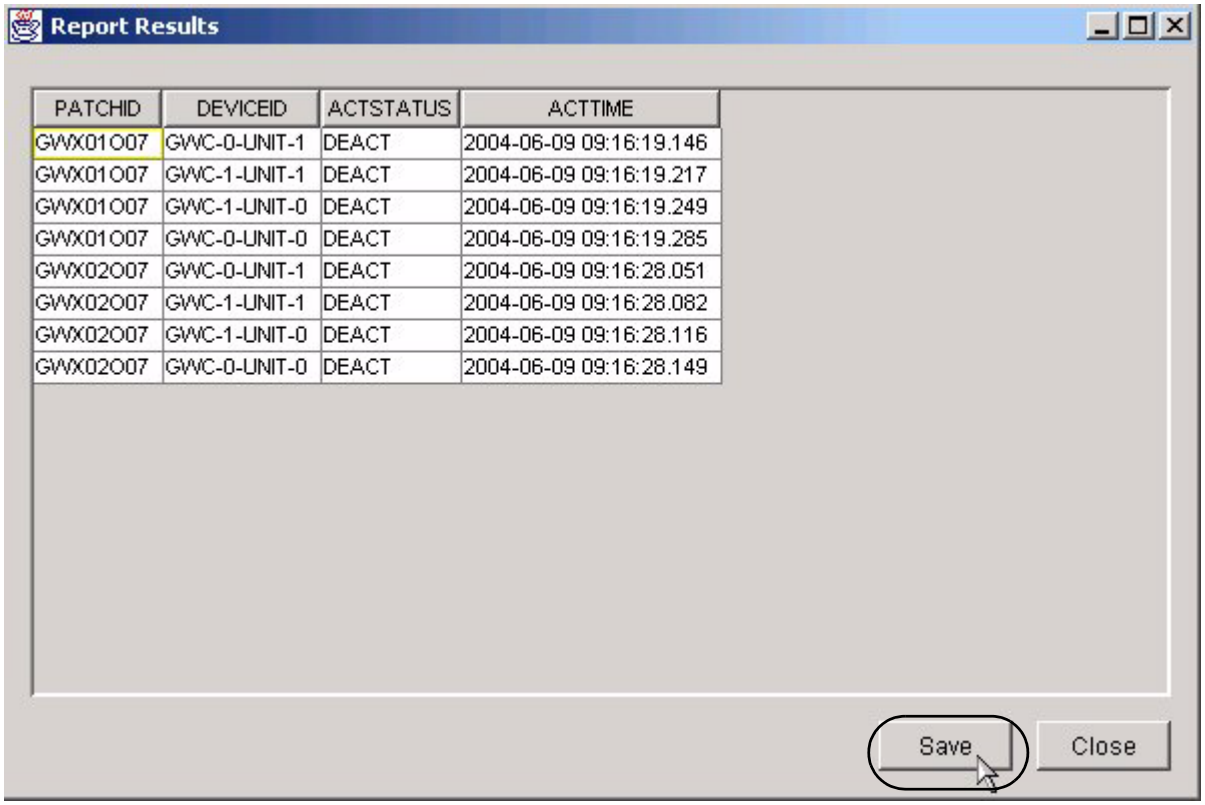


**4** Click the **ACTLIST** entry in the **Report** field, then click **Execute**.




**5** Review the list of patches displayed and note which are activated and which are deactivated. Consult with your Nortel customer support representative to determine which patch files are applicable to your site configuration and should be deactivated.

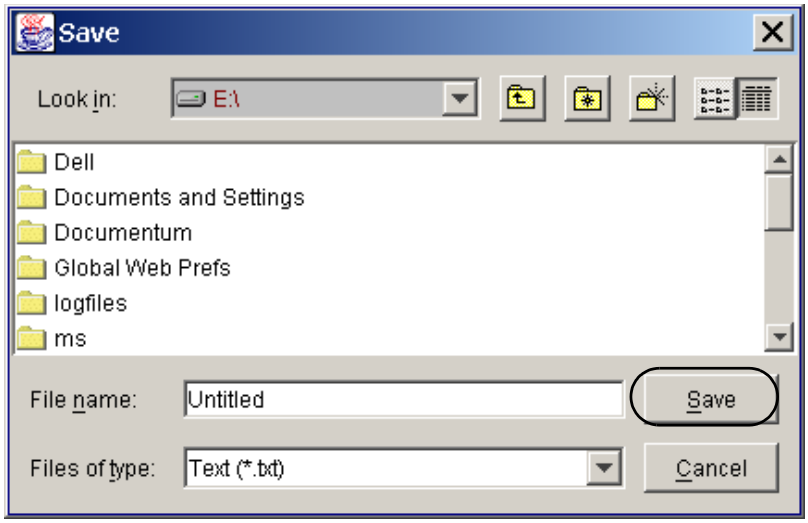
***Note:*** If there are no patches to deactivate, the system returns a dialog box indicating that the report has “empty results”.



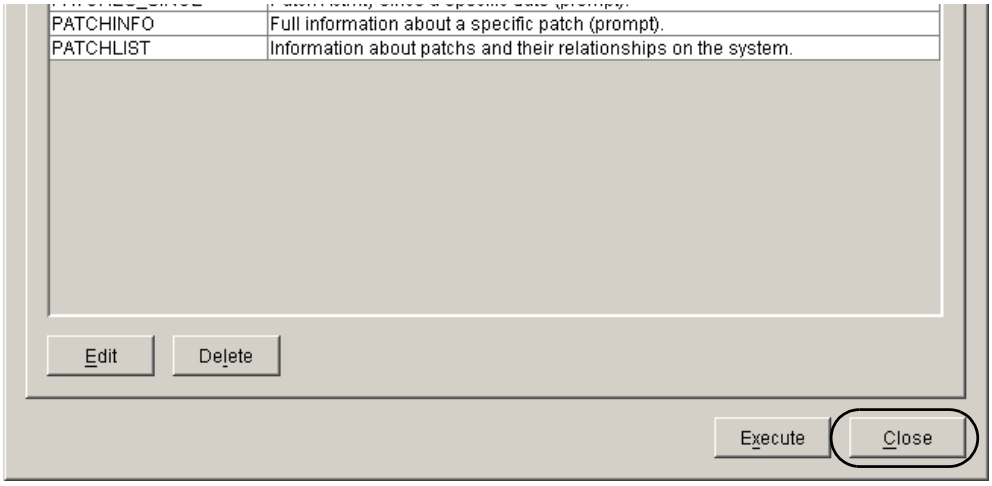

**6** If necessary, save a copy of the report to a text file as follows:

**a** Click **Save**.

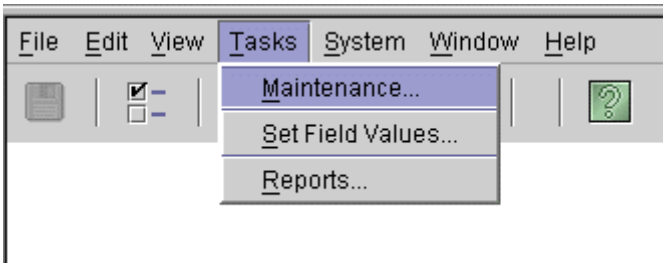
**b** Type a file name in the **File name:** box, and click **Save**.



7 Click **Close** to close the Reports window.

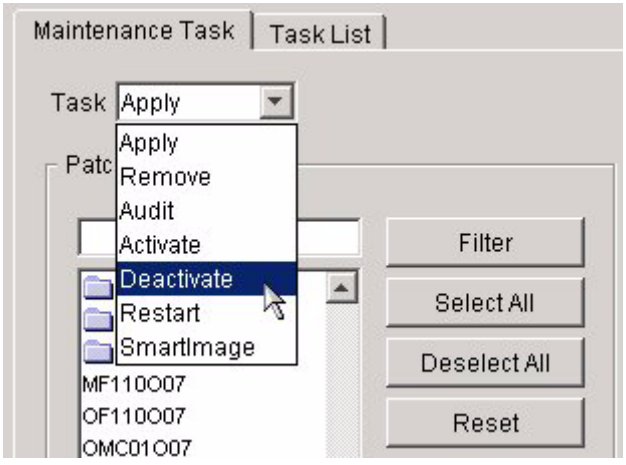



8 On the **Tasks** menu, click **Maintenance...**.

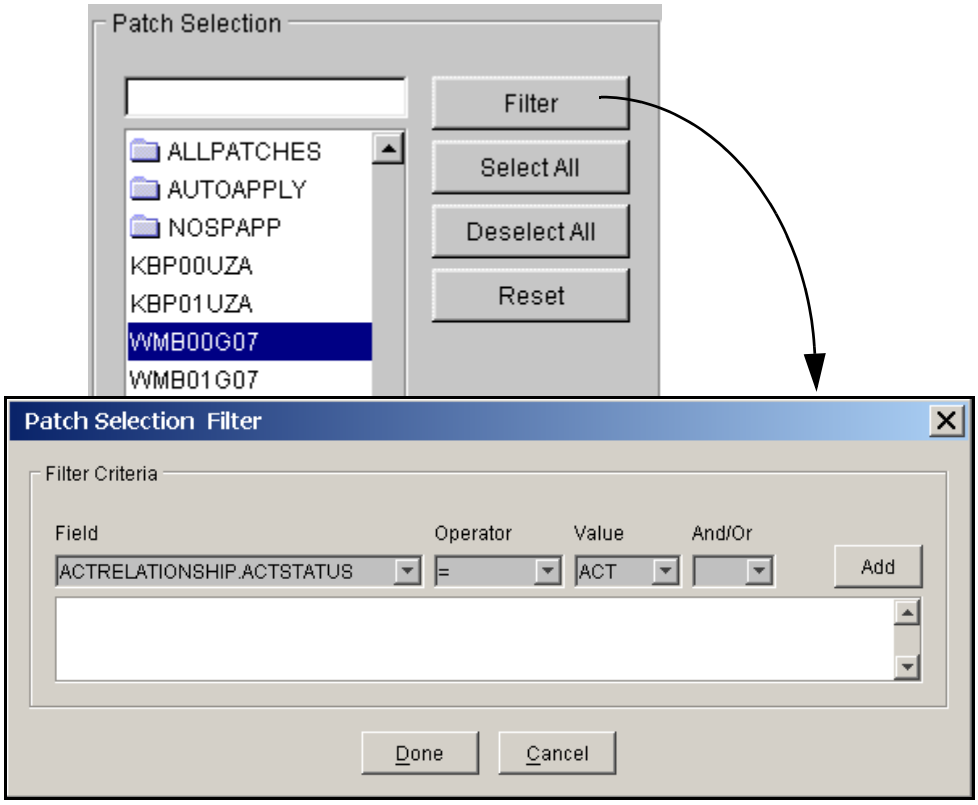



The Maintenance window is displayed.

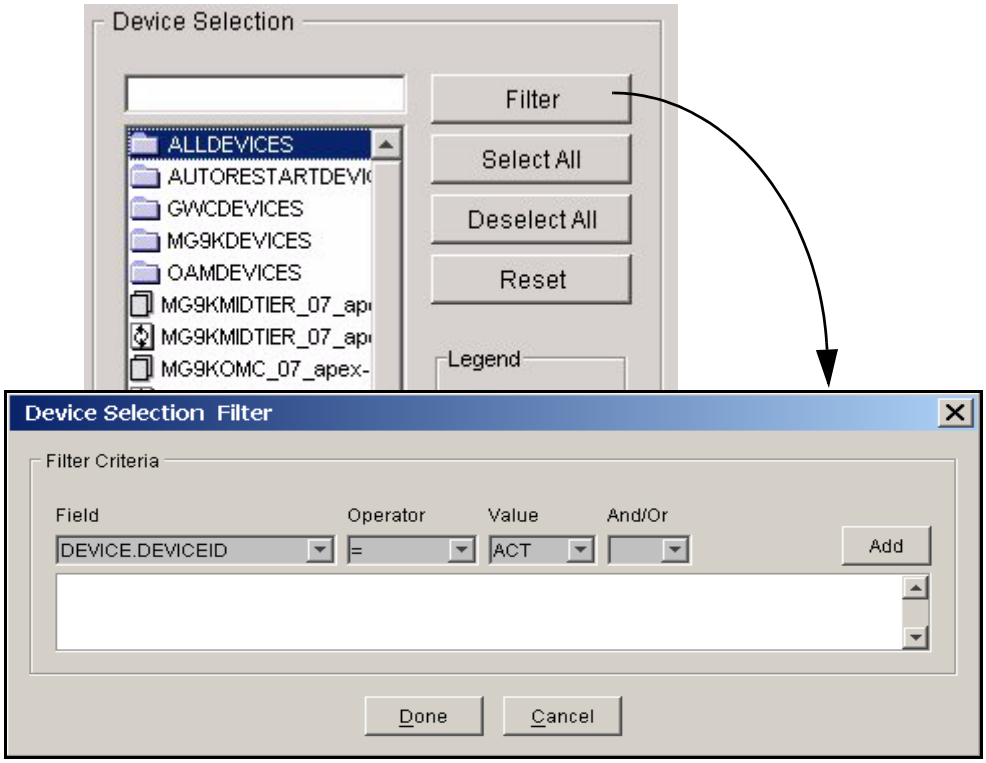
9 In the **Task** list, click **Deactivate**.



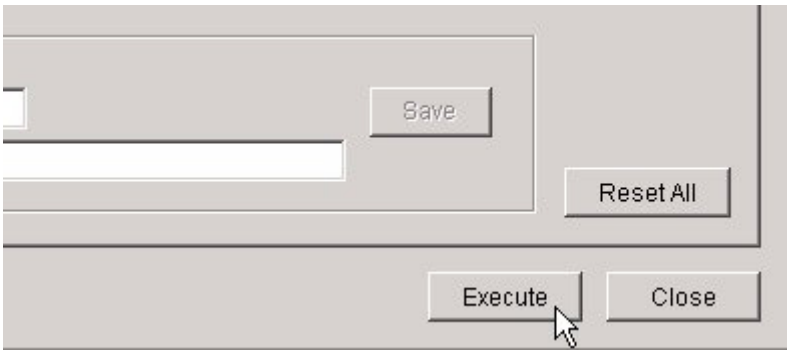
**10** In the **Patch Selection** list, select the patch files or patch sets you want to deactivate, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box.



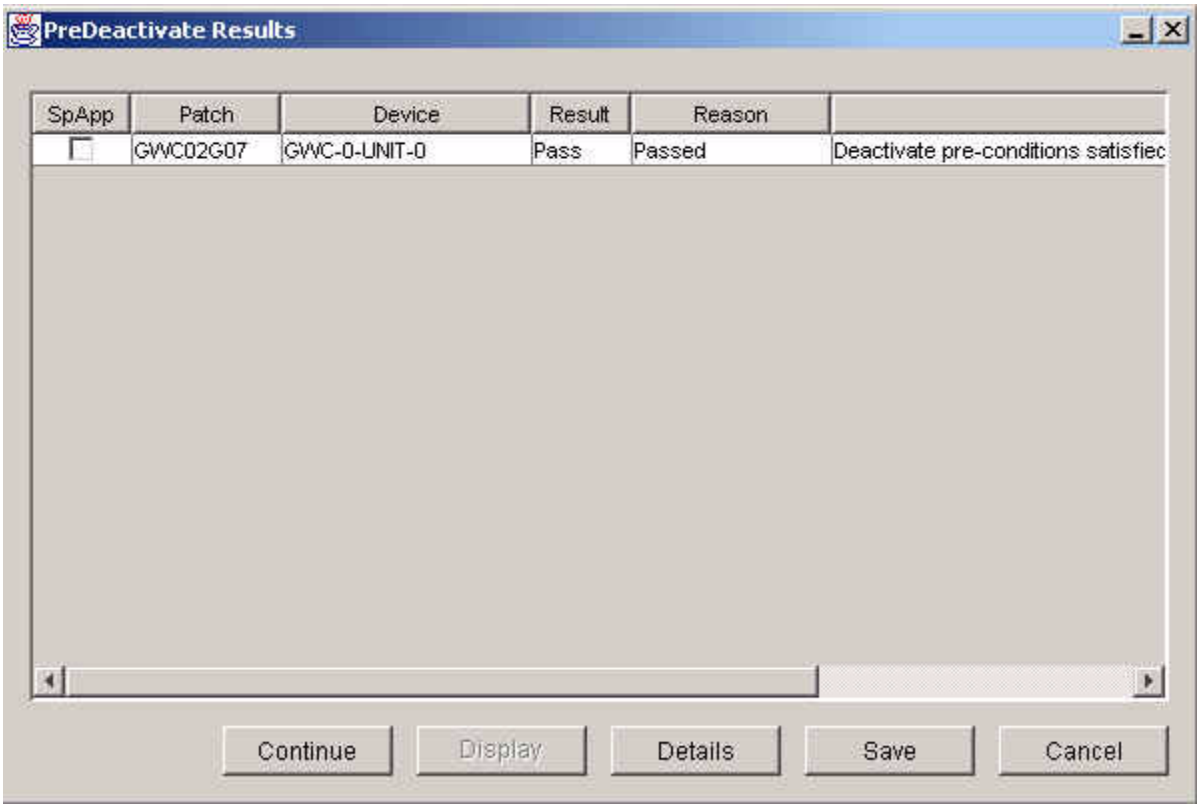
**11** In the **Device Selection** list, select the devices or device sets for which you are deactivating the patches, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.




**12** Click **Execute** to begin the patch deactivation process.

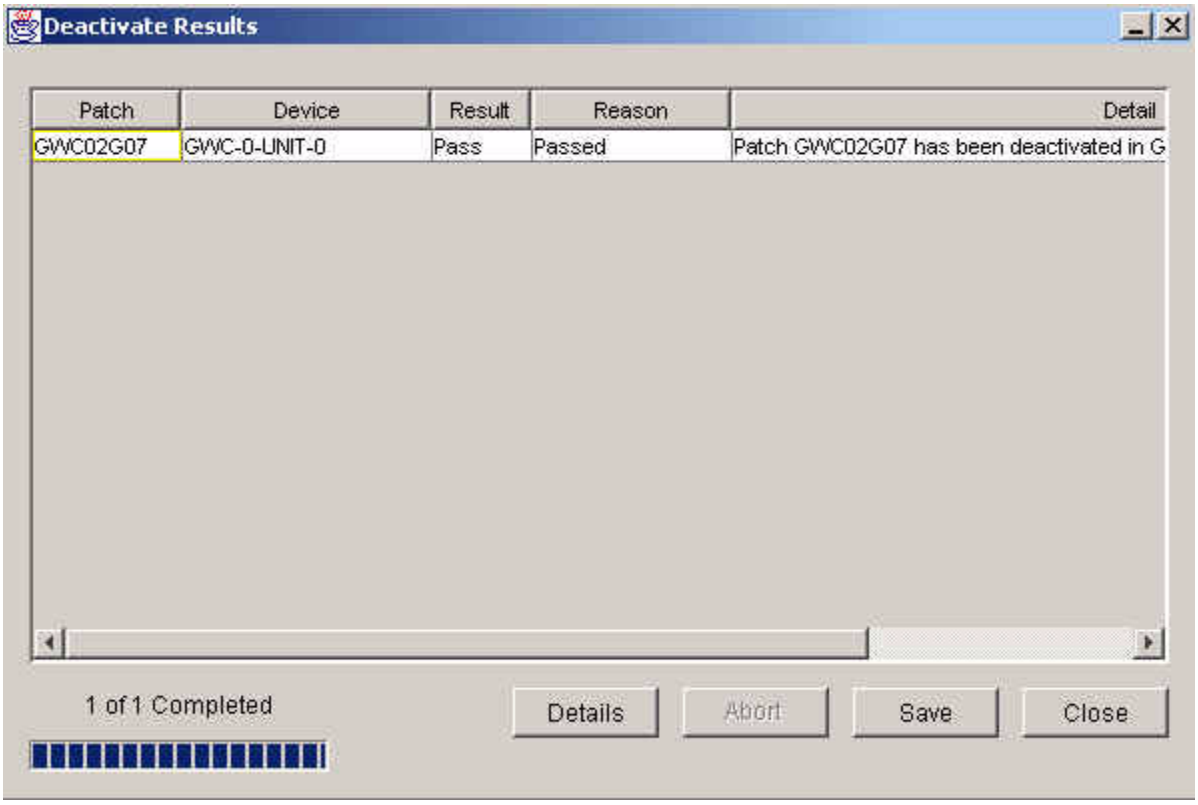



The results of the Pre-deactivate phase are displayed.




**13** Review the PreDeactivate Results, then click **Continue** to proceed.

The Deactivate Results window is displayed with results added as each action is completed. Failures from the PreDeactivate phase are also included in the results.




**14** Click **Save** to save the results to a file, or click **Close**.

***Note:*** If the patches do not successfully deactivate, abort the patching procedure and contact your next level of support.

**15** You have completed this procedure.

# Removing patches using the NPM

## Application

Use this procedure to remove patches using the Network Patch Manager (NPM). You can remove patches using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1712
- Using the NPM GUI on page 1715

## Prerequisites

Before you remove ACT category patches, you must first deactivate the patches. Refer to procedure Deactivating patches using the NPM on page 1701 if required.

Ensure the patch is not on hold.

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 if required.

***At the NPM CLUI***

**2** Remove one or more patches from one or more devices by typing

`npm> remove <patches> [in <devices>]`

and pressing the Enter key.

where

**patches**
is a list of one or more patch IDs you want to remove - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

**devices**
is a list of one or more device IDs from which you want to remove the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and removes them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

**Example**
`npm> remove` ACT02GAX in GWC-8-UNIT-1

**3** When prompted, press the Enter key.

**4** Generate a device query report to verify the patches are removed by typing

`npm> q device`

5 Enter the device name in the format **<deviceid>** that you input in step 2.

A device report of known patch activity for the particular device associated with the <device id> is returned.

6 Verify from the report that the desired patches are removed.

***Note:*** If the patches do not successfully remove, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

If you removed patches from any of the following devices, you need to restart the device in order to disable the patches on the device:

- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager (NPM)

To restart a device, refer to procedure Restarting a device using the NPM on page 1721 if required.

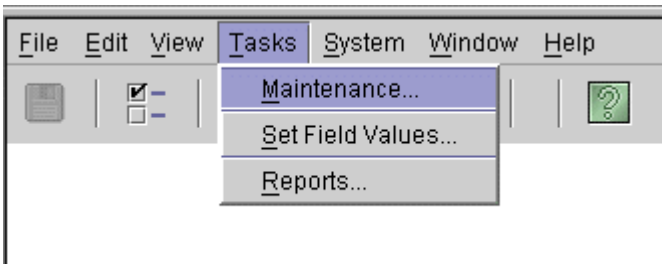
## Using the NPM GUI

### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 if required.

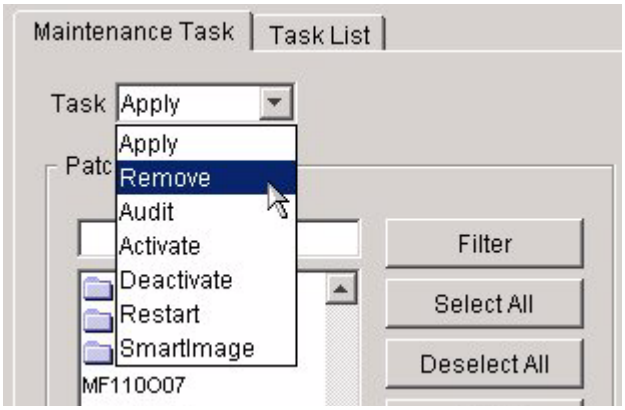
### *At the NPM GUI*

2 On the **Tasks** menu, click **Maintenance...**.

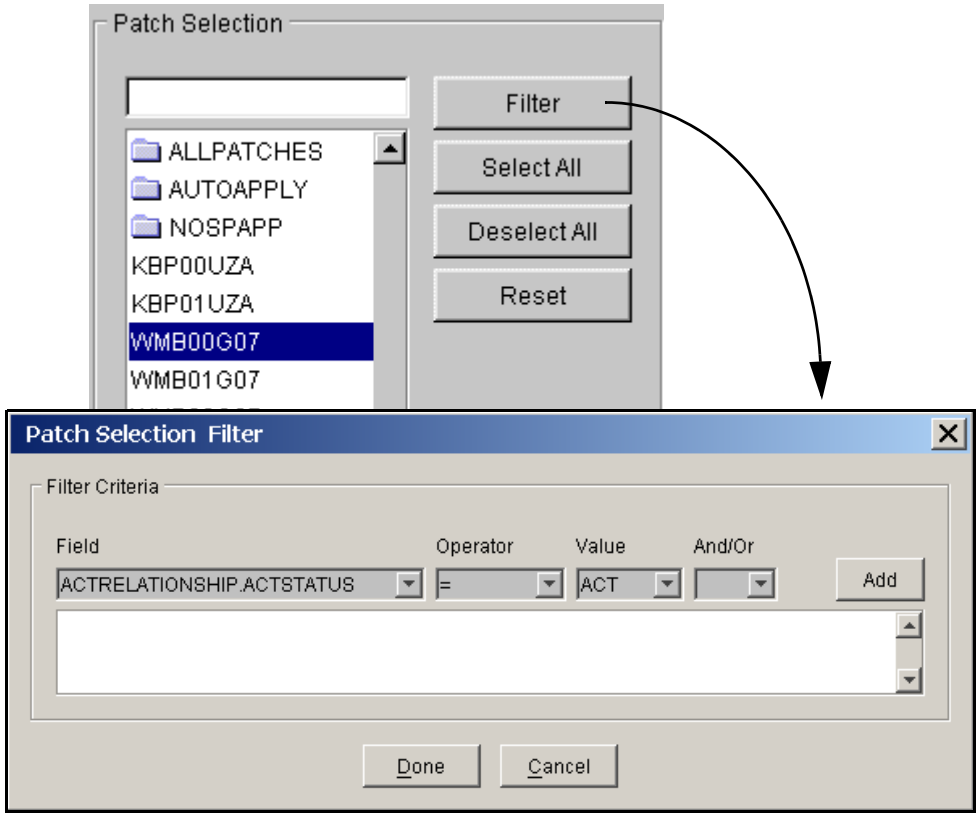



The Maintenance window is displayed.

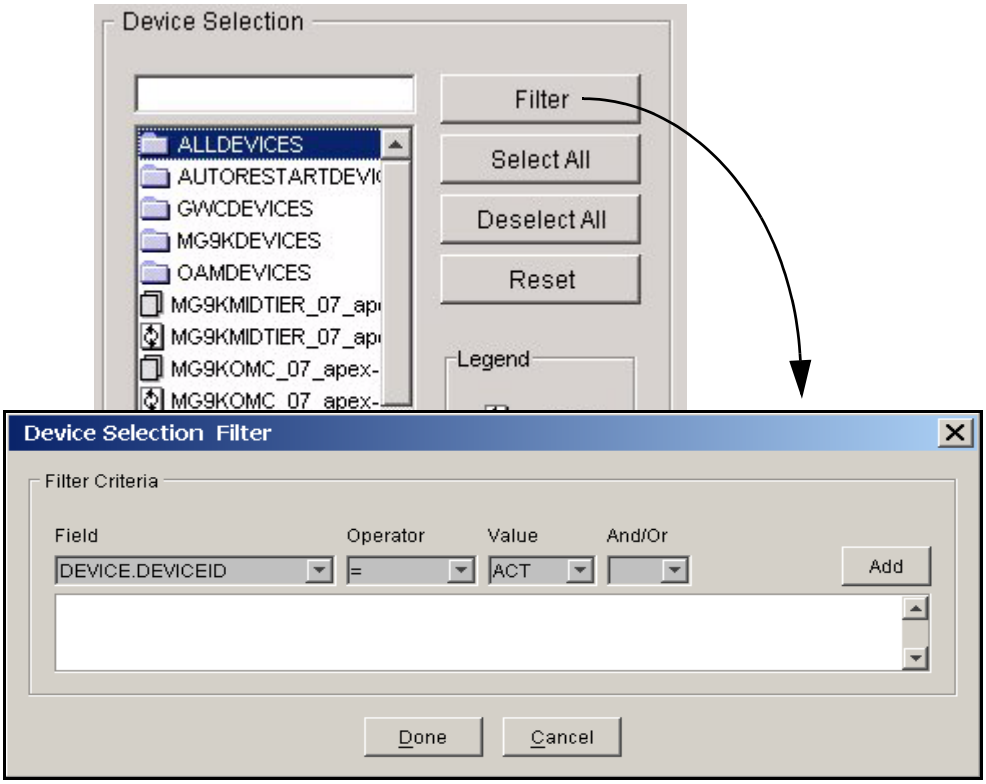
3 In the **Task** list, click **Remove**.



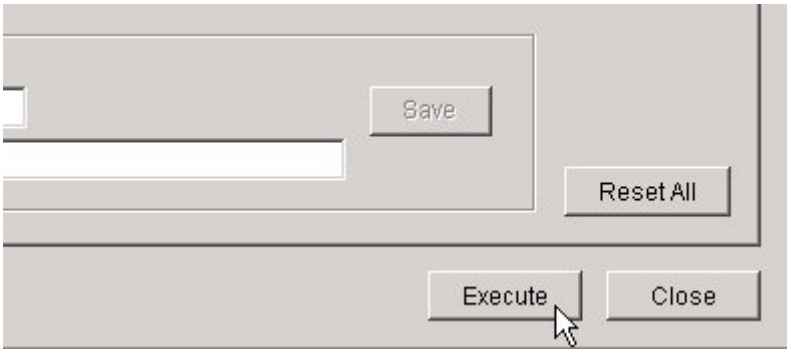
4 In the **Patch Selection** list, select the patch files or patch sets you want to remove from the Patch Selection list, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box.



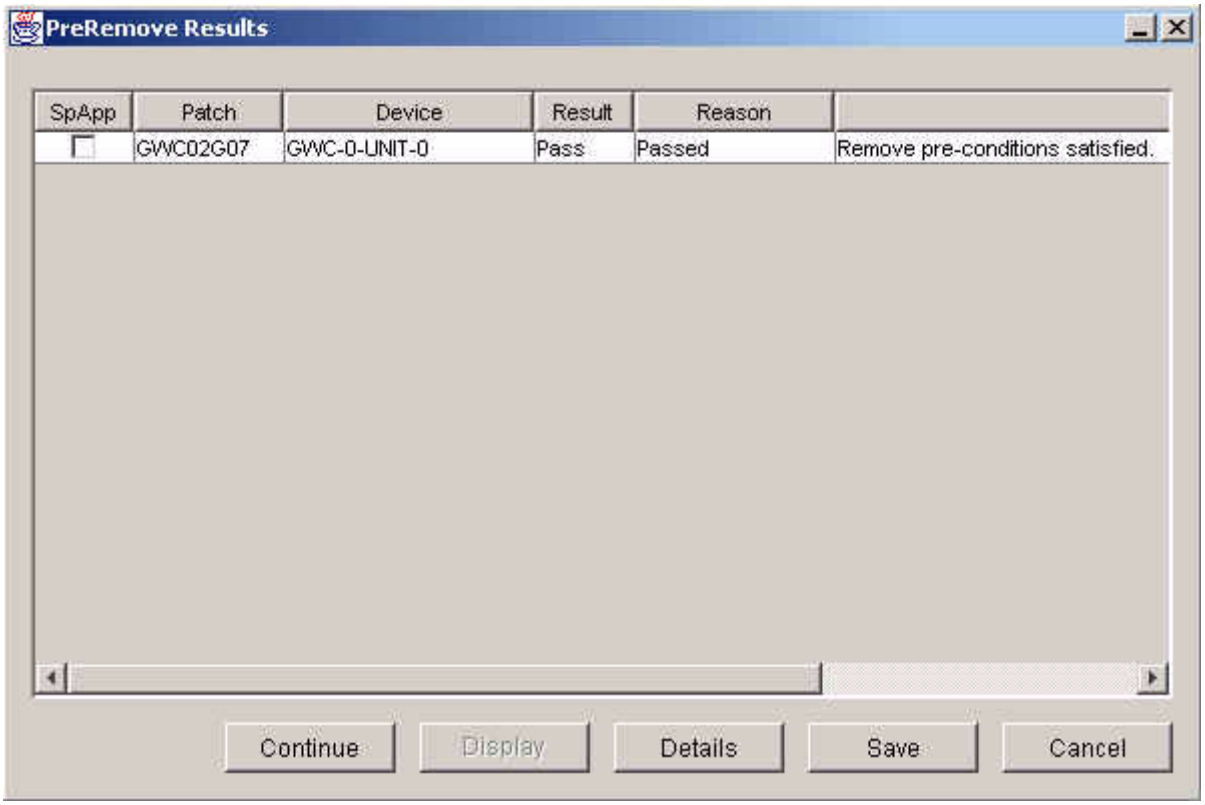
5 In the **Device Selection** list, select the devices or device sets from which the patches will be removed, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.



6 Click **Execute** to begin the patch removal process.



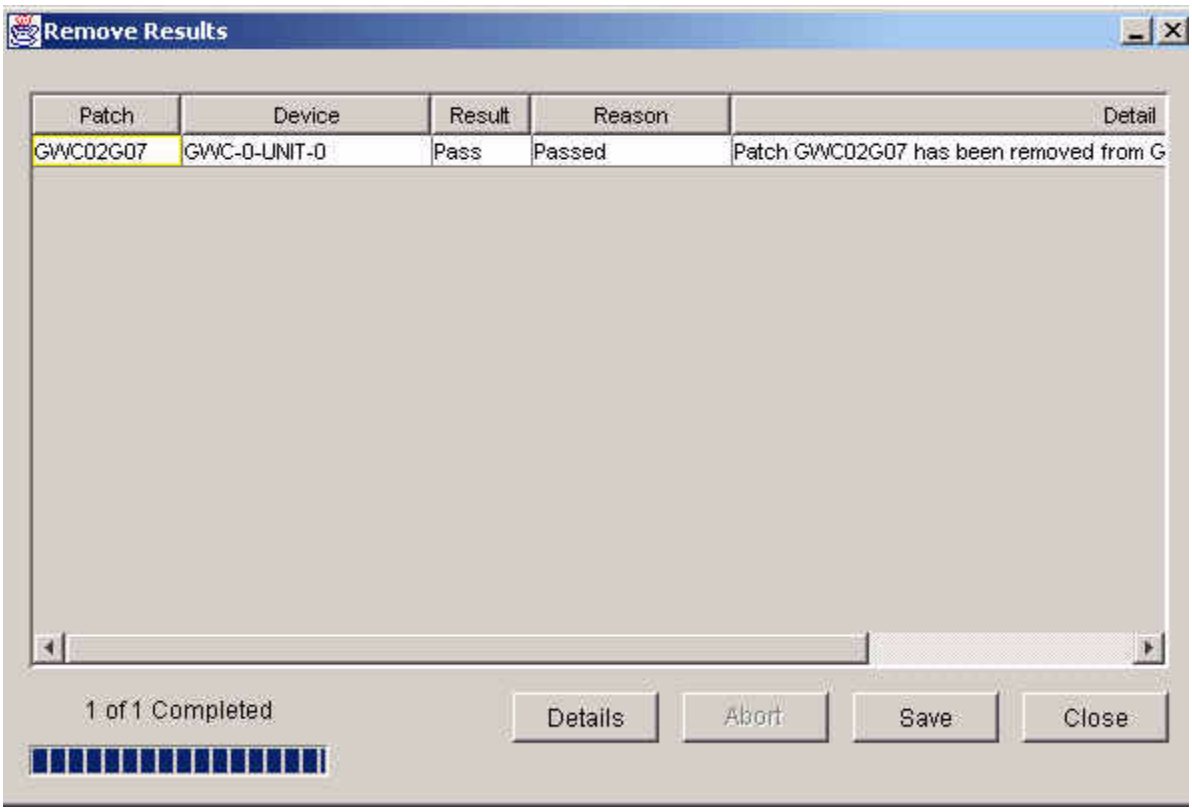

The results of the PreRemove phase are displayed.



7 Review the PreRemove Results, then **Continue** to proceed.

***Note:*** If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Remove Results window is displayed with results added as each action is completed. Failures from the PreRemove phase are also included in the results.




8 Click **Save** to save the results to a file, or click **Close**.

***Note:*** If the patches do not successfully remove, abort the patching procedure and contact your next level of support.

**9** You have completed this procedure.

If you removed patches from any of the following devices, you need to restart the device in order to disable the patches on the device:

- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager (NPM)

To restart a device, refer to procedure Restarting a device using the NPM on page 1721 if required.

# Restarting a device using the NPM

## Application

Use this procedure to restart a device using the Network Patch Manager (NPM). You can restart a device using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1722
- Using the NPM GUI on page 1724

If you applied or removed patches to or from any of the following devices, you need to restart the device in order to enable or disable the patches on the device:

- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager (NPM)

If you applied or removed patches to or from multiple devices, you must restart each device, one at a time, starting with the PSE and ending with the NPM.

In a two-server configuration, restart the device on the active side. Patches are automatically enabled or disabled on the inactive side with the exception of PSE patches. Therefore, the PSE must be restarted on both the active and inactive sides.

***Note:*** Restart is not supported for the Succession Server Platform Foundation Software (SSPFS). Refer to the specific SSPFS patch for further instructions on how to enable or disable.

A restart takes the application out of service temporarily, then returns the application to service.

## Prerequisites

This procedure has the following prerequisites:

- you have applied or removed all the patches to or from the device
- the device you are restarting is not on hold
- no users are logged in to the NPM GUI
- 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 1569 if required.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.



**CAUTION**

Stop or complete any maintenance activities associated with the patched device before you begin the restart.

### Using the NPM CLUI

***At your workstation***

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 if required.

***At the NPM CLUI***

**2** Restart a device by typing

```
npm> restart <devices>
```

and pressing the Enter key.

where

**devices**
is a list of one or more device IDs you want to restart - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Example
`npm> restart` GWC-8-UNIT-1

**3** When prompted, confirm you want to continue with the device restart by typing

**y**

and pressing the Enter key.

Example output

```
SpAPP: false
Patch: *
Device: SESM
Result: true
Reason: Passed
Details: Device SESM passed preRestart.
If you wish to continue with this maintenance
request, enter Yes (Y or y). Otherwise, just
enter return.
```

4 When prompted, confirm you want to continue with the device restart by typing

**y**

and pressing the Enter key.

Example output

```
npm>

Patch: *

Device: SESM

Reason: Passed

Detail: Restart passed on device SESM.

Hit <CR> to continue...
```

5 When prompted, press the Enter key.

***Note:*** Restarting the NPM makes it unavailable until it has successfully restarted. You will need to log in once it has restarted.

Once the device has been successfully restarted, Nortel Networks recommends that you perform an audit on the device to synchronize the NPM database with the updates to the patches on the device. The audit will automatically occur at a specified time, however, to perform an audit manually, see Performing a device audit using the NPM on page 1669 if required.

6 You have completed this procedure.

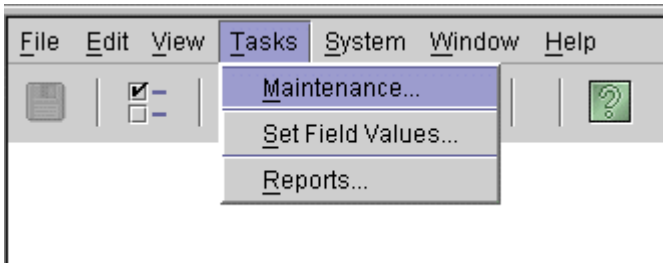
### Using the NPM GUI

#### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 if required.

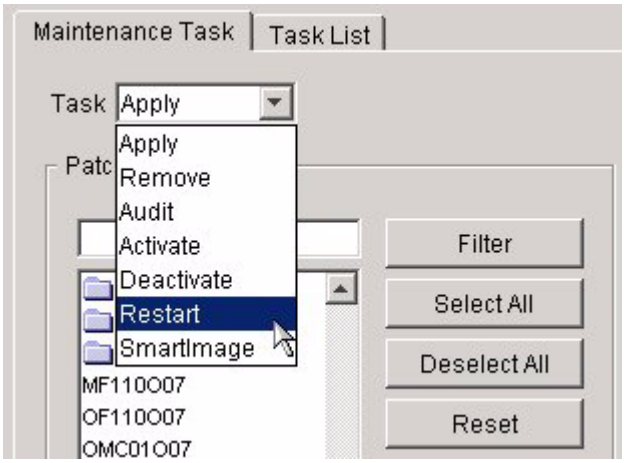
***At the NPM GUI***

**2** On the **Tasks** menu, click **Maintenance...**.

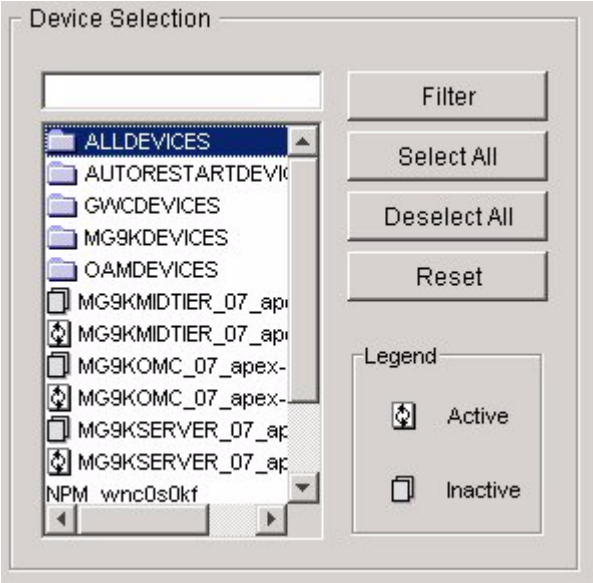



The Maintenance window is displayed.

**3** In the **Task** list, click **Restart**.

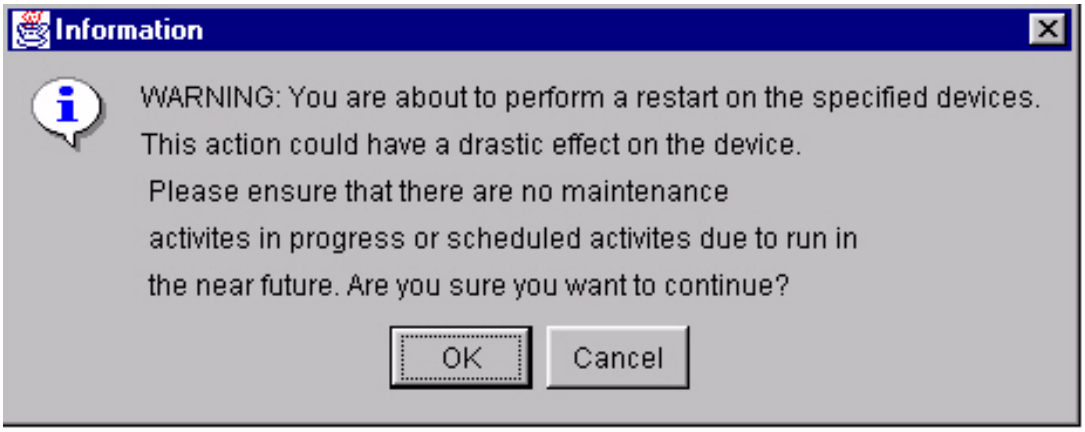


4 In the **Device Selection** list, select the device, device list, or device set that you want to restart.



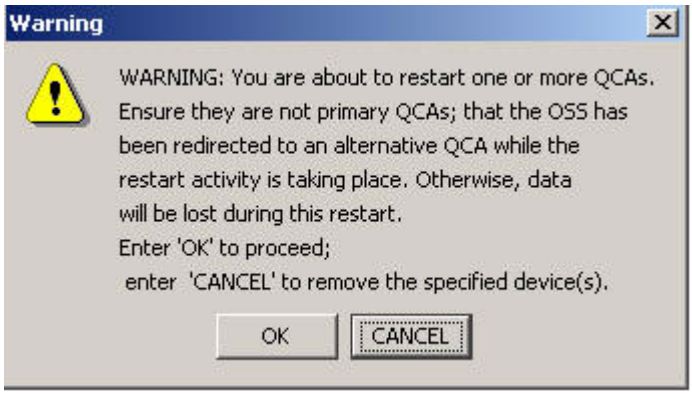

5 Click **Execute** to begin the restart.

The system returns the following dialog box.



6 Click **OK** to begin the restart.

If you are restarting a QCA device, the system returns the following warning:

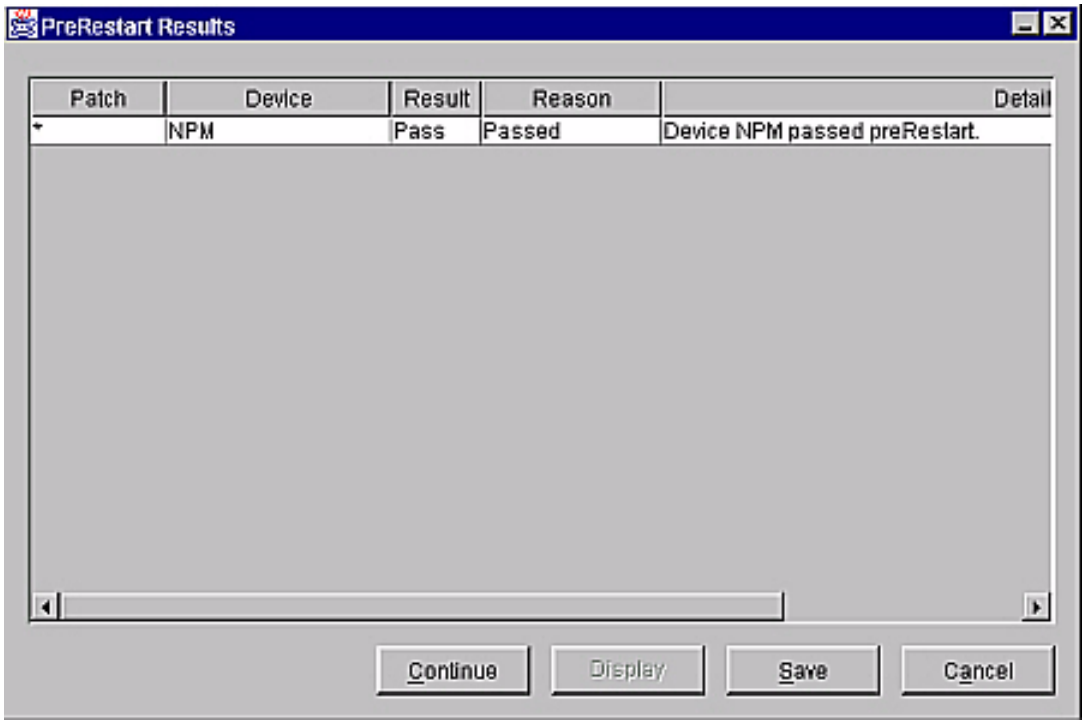



7

**CAUTION**
**Loss of data**
Carefully read the warning about QCAs before you proceed with a QCA restart.

If restarting a QCA is acceptable, click **OK** to proceed with the restart.

The results of the PreRestart phase are displayed.




8 Review the PreRestart Results, then click **Continue** to proceed.

***Note:*** Restarting the NPM makes it unavailable until it has successfully restarted. You will need to log in once it has restarted.

Once the device has been successfully restarted, Nortel Networks recommends that you perform an audit on the device to synchronize the NPM database with the updates to the patches on the device. The audit will automatically occur at a specified time, however, to perform an audit manually, see Performing a device audit using the NPM on page 1669 in this document.

9 You have completed this procedure.

# Defining sets using the NPM

## Application

Use this procedure to define sets using the Network Patch Manager (NPM). You can define sets using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1730
- Using the NPM GUI on page 1731

Sets provide a convenient grouping of patches and devices used in routine patching tasks. The sets are dynamic, based on database query statements, and are evaluated at execution time.

The NPM is initially configured with the following defined sets for Patch Selection:

- ALLPATCHES - all patches on the system
- AUTOAPPLY - all patches that can be auto-applied
- NOSPAPP - all patches with no special applications

The NPM is initially configured with the following defined sets for Device Selection:

- ALLDEVICES - all registered devices on the system
- OAMDEVICES - all registered devices that are of device type OAM (PSE, SESM, CS 2000 SAM21 Manager, MG 9000 Manager, QCA, NPM, and SSPFS)
- AUTORESTARTDEVICES - all registered devices that are of device type OAM and can be auto-restarted (this excludes QCA)
- MG9KDEVICES - all registered Media Gateway 9000 (MG 9000) devices on the system
- GWCDEVICES - all registered Gateway Controller (GWC) devices on the system

## Prerequisites

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

**1** Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

**1** Define a set by typing

```
npm> newset <report_type> <name> <description>
<fields> where <criteria>
```

and pressing the Enter key.

where

**report_type**
is either REPORT, PATCHSET, or DEVICESET

**name**
is the name of the set to be created

**description**
is a short description of the set

**fields**
is the name of one or more fields, separated by a space, to be included in the set

**criteria**
is the SQL statement that identifies the criteria by which to search the NPM database

Example

```
npm> newset PATCHSET BR12345PATCH "Patches for
CSR BR12345" where PATCH.CSR='BR12345'"
```

***Note:*** You can view the definition of a set using the "`viewset SET <setname>`" command, and you can view the contents of a set using the "`query <setname>`" command.

**2** You have completed this procedure.

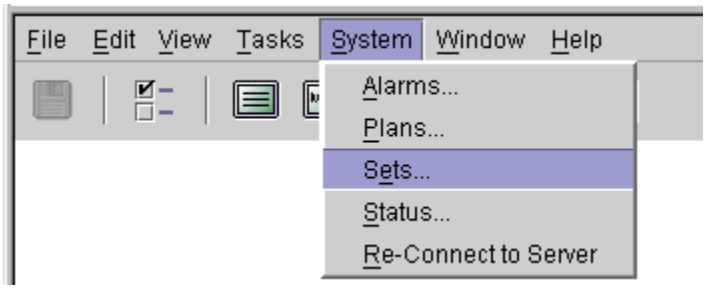
## Using the NPM GUI

### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

### *At the NPM GUI*

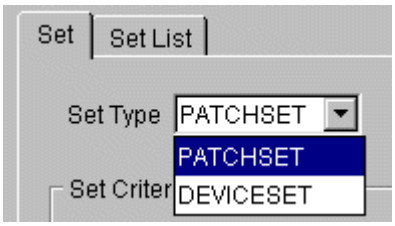
1 On the **System** menu, click **Sets...**.




The **Sets** window is displayed.

2 In the **Set Type** list, select PATCHSET to define a set of patches, or DEVICESET to define a set of devices.

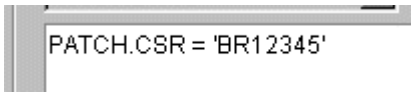
***Note:*** You can also edit an existing set definition listed under the **Set List** tab, that contains similar criteria to the set you want to create, and save it under a new name.



3 In the **Set Criteria** area, specify the criteria for the set using substep a or b

**a** Type the criteria for the set in the text box.

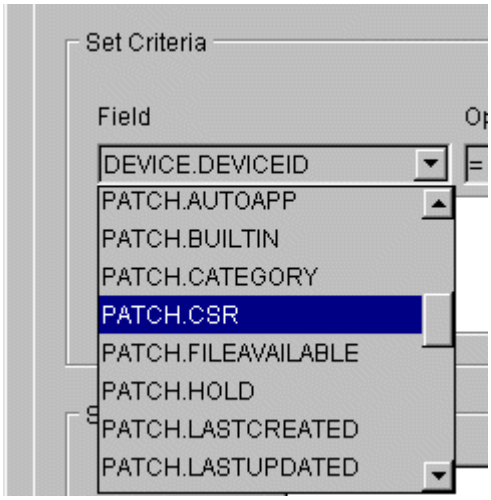
***Note:*** Parenthesis "()" may be inserted to define precedence for multiple criteria statements.



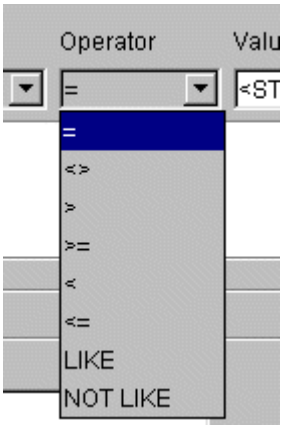

OR

**b** Specify the set criteria as follows:

**i** In the **Field** list, click the field of your choice.



ii In the **Operator** list, click the operator of your choice.

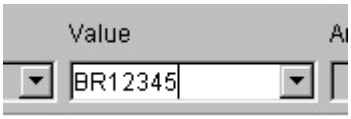



The following table lists the supported operators and their meaning.

| Operator | Meaning |
|---|---|
| = | Equal |
| <> | Not equal |
| > | Greater than |
| >= | Greater than or equal |
| < | Less than |
| <= | Less than or equal |
| LIKE | Matches string with wildcard (%) |
| NOT LIKE | Does not match string with wildcard (%) |

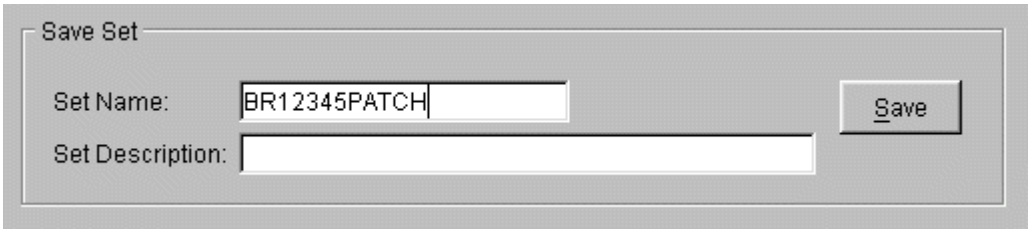
iii In the **Value** list, select the value of your choice.

***Note:*** The data type in the **Value** list will change depending on the data type selected in the **Field** list. For alphanumeric data, type the value. For boolean data, select the value.

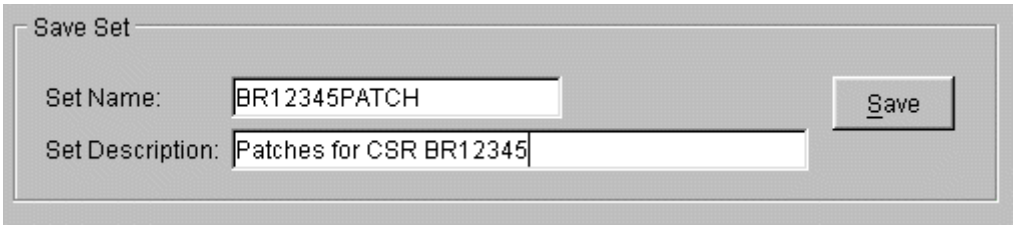



To combine multiple criteria statements, click **AND** or **OR** in the **And/Or** list.

4 Type a unique name for the set in the **Set Name** box.

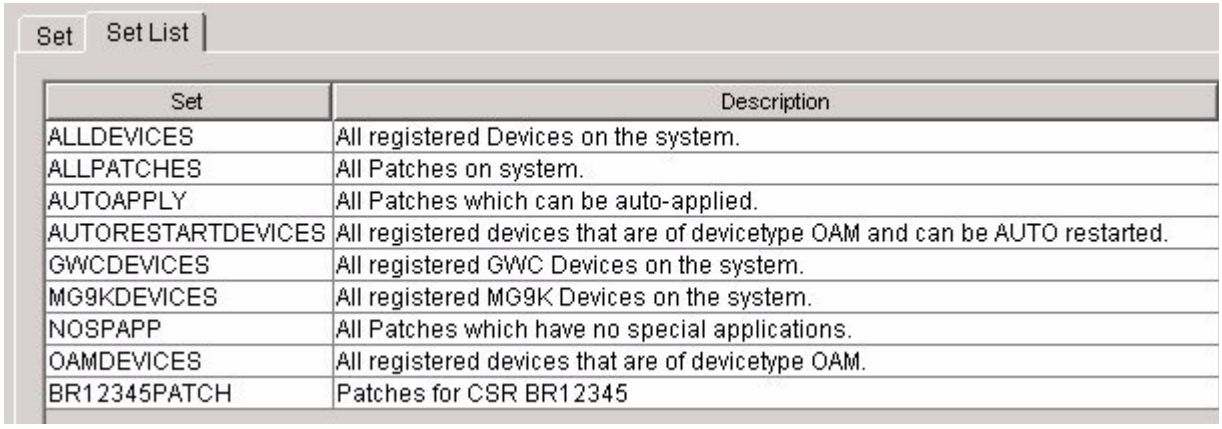



5 Type a description of the set in the **Set Description** box if desired.




6 Click **Save** to save the set.

The new set will be reflected under the **Set List** tab once the system has saved it.




| Set | Description |
|---|---|
| ALLDEVICES | All registered Devices on the system. |
| ALLPATCHES | All Patches on system. |
| AUTOAPPLY | All Patches which can be auto-applied. |
| AUTORESTARTDEVICES | All registered devices that are of devicetype OAM and can be AUTO restarted. |
| GWCDEVICES | All registered GWC Devices on the system. |
| MG9KDEVICES | All registered MG9K Devices on the system. |
| NOSPAPP | All Patches which have no special applications. |
| OAMDEVICES | All registered devices that are of devicetype OAM. |
| BR12345PATCH | Patches for CSR BR12345 |

***Note:*** You can view the definition of a set using the **View** button, and you can view the contents of a set using the **Evaluate** button.

7 You have completed this procedure.

# Saving a task using the NPM

## Application

Use this procedure to save a task using the Network Patch Manager (NPM). You can save tasks using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1735
- Using the NPM GUI on page 1737

A task is a definition of one type of maintenance activity that involves devices and may involve patches. The Network Patch Manager (NPM) allows tasks to be saved for automated execution.

The NPM is initially configured with the following defined tasks:

- AUTOAPPLY
- AUTORESTART
- AUDIT

## Prerequisites

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

**2** Define the task by typing

```
npm> newtask <task_name> <task_type>
<task_desc> <task_patchlist> <task_devicelist>
```

and pressing the Enter key.

where

**task_name**
the name of the task to be created

**task_type**
determines the type of task (APPLYTASK, REMOVETASK, ACTIVATETASK, DEACTIVATETASK, AUDITTASK, or RESTARTASK)

**task_desc**
is the description of the task

**task_patchlist**
is the set of patches associated with the task

***Note:*** The task_patchlist field is not used with AUDITTASK. For an AUDITTASK, use "" (two double quotes together).

**task_devicelist**
is the set of devices associated with the task

Following is an example to apply all NOSPAPP patches to all devices.

```
npm> newtask NOSPAPPALL APPLYTASK "NOSPAPP for
ALLDEVICES" NOSPAPP ALLDEVICES
```

Following is an example to audit all devices.

```
npm> newtask AUDITALL AUDITTASK "Audit all
devices" "" ALLDEVICES
```

**3** You have completed this procedure.

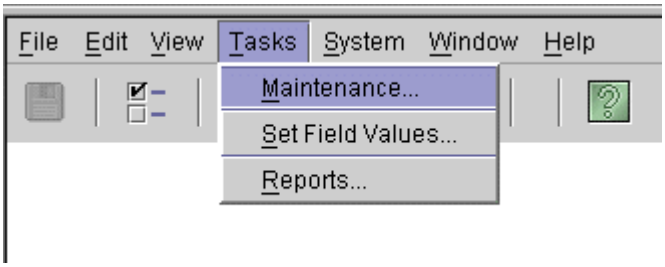
## Using the NPM GUI

### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

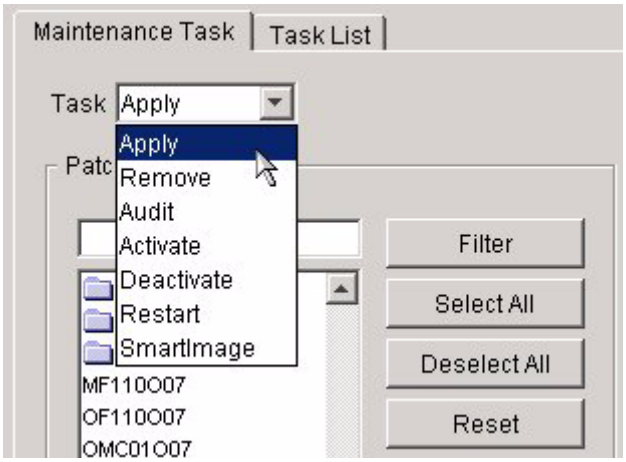
### *At the NPM GUI*

2 On the **Tasks** menu, click **Maintenance...**.

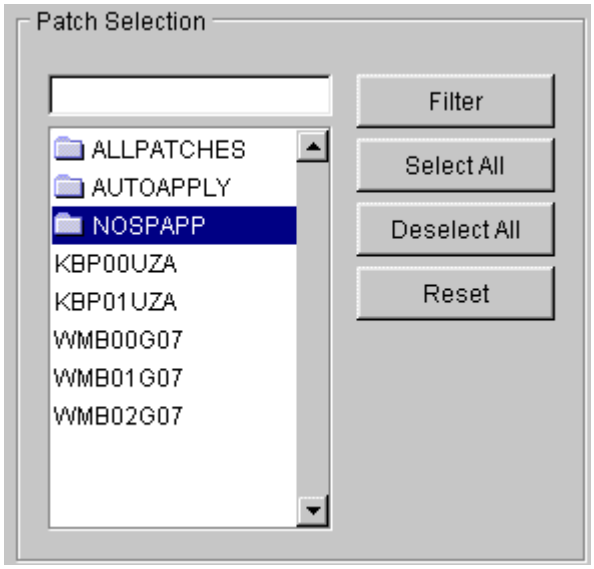



The **Maintenance** window is displayed.

3 In the **Task** list, click the task of your choice.

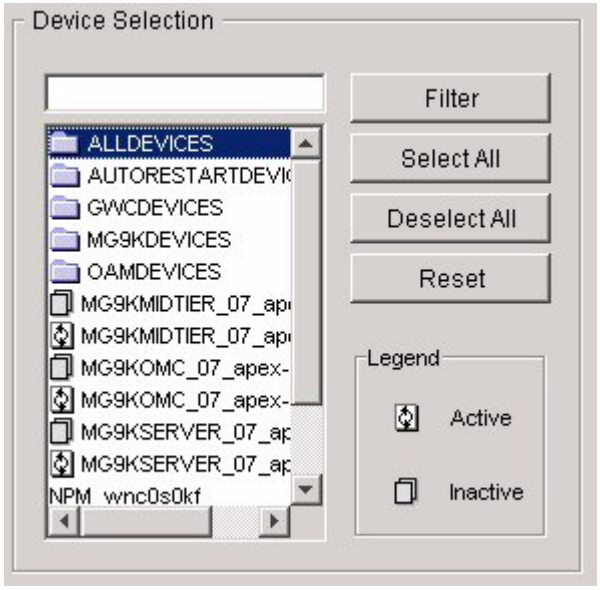


4 In the **Patch Selection** list, select the patch set (if applicable) you want to associate with the task.

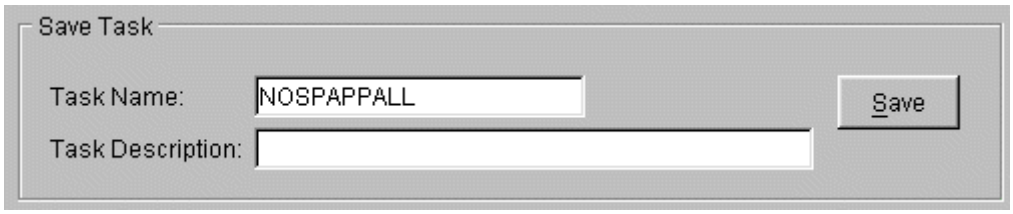



***Note:*** Saved tasks can only contain patchsets or devicesets, not single patches or devices. You can save a task that applies one patch to one device by putting the patch in a single-member patchset and the device in a single-member deviceset and then applying the patchset to the deviceset.

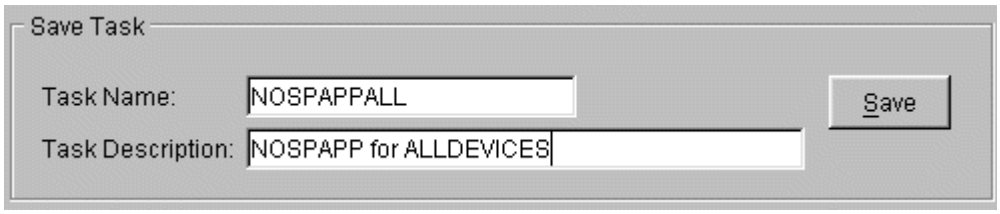
5 In the **Device Selection** list, select the device set you want to associate with the task.



6 Type a unique name for the task in the **Task Name** box.

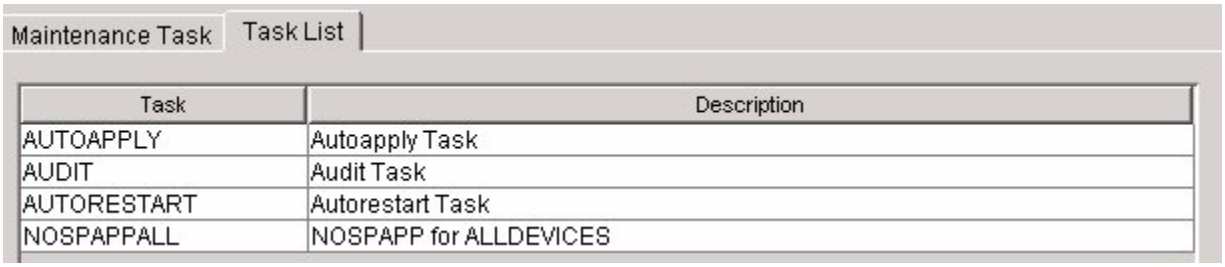



7 Optionally, type a description of the task in the **Task Description** box.




8 Click **Save** to save the task.

The new task will be displayed under the **Task List** tab once the system has saved the task.




9 You have completed this procedure.

# Setting field values using the NPM

## Application

Use this procedure to set field values using the Network Patch Manager (NPM). You can set field values using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1740
- Using the NPM GUI on page 1742

The NPM allows the exclusion and inclusion of patches or devices from manual or automated patching tasks. This is accomplished by setting database field values using the “assign” command. An example of when this option could be used is when a new patch is to be applied to a single device for a test period, without applying the patch to the remaining devices. After the test period, the patch would then be applied to the remaining devices.

## Prerequisites

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM CLUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

2 Assign field values by typing

```
npm> assign <pd_option> <val_field> <val_value>
<val_idset> <val_set>
```

and pressing the Enter key.

where

**pd_option**
identifies what is being assigned (PATCH or DEVICE)

**val_field**
is the field to be assigned (PATCH.HOLD or DEVICE.HOLD)

**val_value**
is the new value for the field (Y or N)

**val_idset**
identifies if you are assigning a singe patch or device or a set of patches or devices (ID or SET)

**val_set**
is the patch, device, or set to be assigned

*Example*

```
npm> assign PATCH PATCH.HOLD Y ID WMB00G07
```

Using the table below, determine the Field and Values to select.

**Field and Value combinations**

| Field | Value | Result |
|---|---|---|
| PATCH.HOLD | N | The patch will be applied to the remaining devices. This is typically after the test period is over. |
| PATCH.HOLD | Y | The patch will be excluded from manual or automated patching activities. |
| DEVICE.HOLD | N | The device will be included in patching tasks. This is typically after the test period is over. |
| DEVICE.HOLD | Y | The device will be excluded from manual or automated patching activities. |

**3** You have completed this procedure.

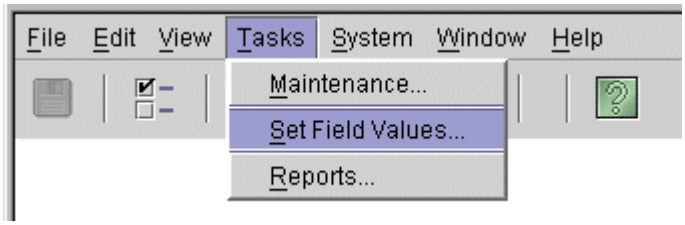
## Using the NPM GUI

### *At your workstation*

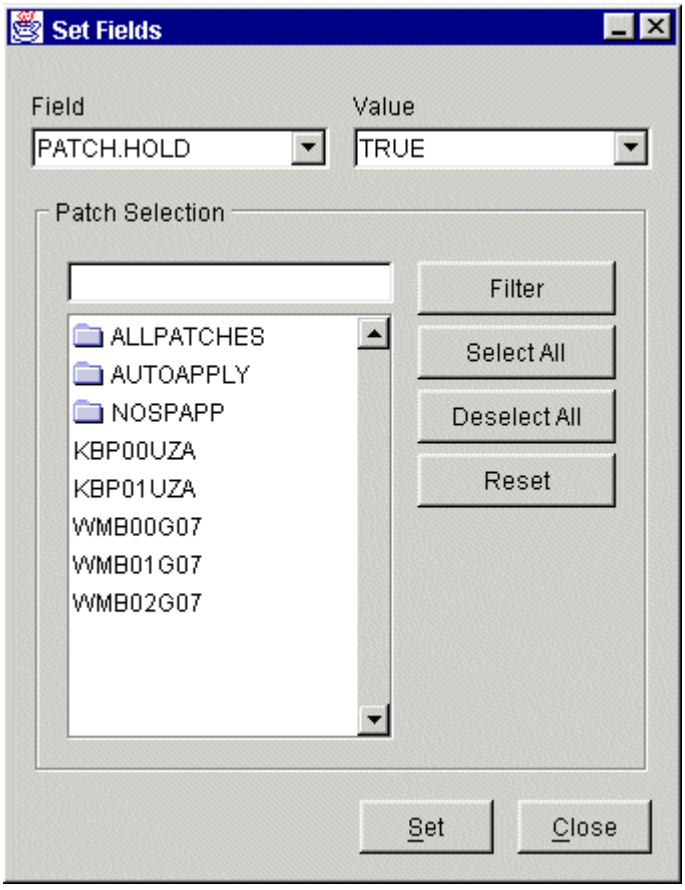
1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

### *At the NPM GUI*

2 On the **Tasks** menu, click **Set Field Values...**.




The **Set Field** window is displayed.

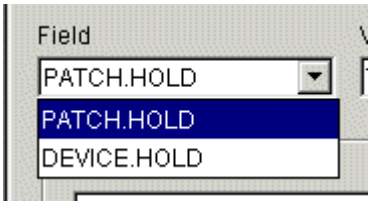


3 Using the table below, determine the Field and Values to select.

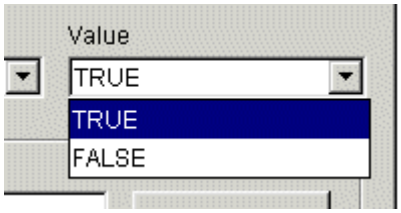
**Field and Value combinations**

| Field | Value | Result |
|---|---|---|
| PATCH.HOLD | FALSE | The patch will be applied to the remaining devices. This is typically after the test period is over. |
| PATCH.HOLD | TRUE | The patch will be excluded from manual or automated patching activities. |
| DEVICE.HOLD | FALSE | The device will be included in patching tasks. This is typically after the test period is over. |
| DEVICE.HOLD | TRUE | The device will be excluded from manual or automated patching activities. |

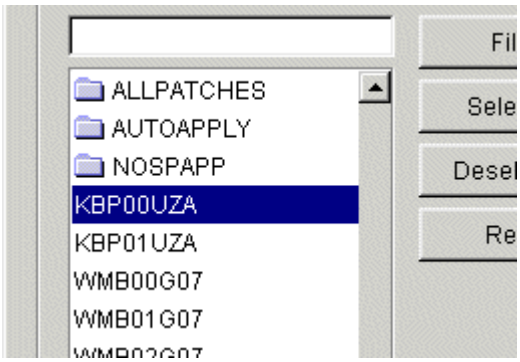
4 In the **Field** list, click PATCH.HOLD or DEVICE.HOLD.




5 In the **Value** list, click TRUE or FALSE.

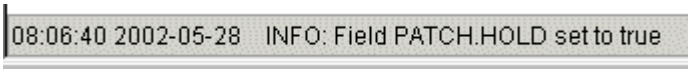


6 In the **Patch Selection** list (if you clicked PATCH.HOLD), select one or more patches, or in the **Device Selection** list (if you clicked DEVICE.HOLD), select one or more devices.




7 Click **Set**, to apply the changes.

The system displays a confirmation message at the bottom of the Network Patch Manager window.




8 You have completed this procedure.

# Defining reports using the NPM

## Application

Use this procedure to create a user-defined report and generate it using the Network Patch Manager (NPM). You can define reports using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1746
- Using the NPM GUI on page 1747

The reporting feature of the Network Patch Manager (NPM) allows you to select information from the database and display it. Report criteria determines what is displayed. In addition to the predefined reports for the NPM, users can create and save their own reports according to their application-specific criteria.

The NPM is initially configured with the following defined reports:

- ACTLIST - RPS activation patch information
- CALCLIST - RPS patch calculation report
- DEVICE - Information about a specific device (prompt report)
- DEVICELIST - Information about patchable devices on the system
- DISABLEDAPPLIED - patches that are applied but disabled
- DISABLEDREMOVED -patches that are disabled and removed
- ENABLEDAPPLIED - patches that are applied and enabled
- ENABLEDREMOVED - patches that are applied but removed
- FULLDEVICELIST - Information about every device on the system
- LOADLIST - RPS device load report
- PATCH - Information about a specific patch (prompt report)
- PATCHES_SINCE - Patch activity since a specific date (prompt report)
- PATCHINFO - Full information about a specific patch (prompt report)
- PATCHLIST - Information about patches and their relationships on the system
- DEVICE_ACTIVITY -Displays all devices and their activity states
- DEVICE_ACTLEVEL - Displays the number of patches activated in each device

- DEVICE_APPLEVEL - Displays the number of patches applied to each device
- INVALID_LOADNAME - Displays devices with invalid loads. An audit is required (see procedure Performing a device audit using the NPM on page 1669 in this document if required).

## Prerequisites

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

**1** Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

**1** Define the report by typing

```
npm> newset REPORT <report_name> <report_desc>
<report_fields> where <report_criteria>
```

and pressing the Enter key.

where

**report_name**
the name of the report to be created

**report_desc**
is a short description of the report

**report_fields**
is the name of one or more fields, separated by a space, to be included in the report

**report_criteria**
is the SQL statement that identifies the criteria by which to search the NPM database

Example

```
npm> newset REPORT DEVHOLDFALSE "All devices
with HOLD=FALSE" "DEVICE.DEVICEID DEVICE.HOLD
where DEVICE.HOLD='FALSE'"
```

2 Generate the report by typing

```
npm> query <report_name>
```

and pressing the Enter key.

where

**report_name**
the name of the report you previously created

3 You have completed this procedure.

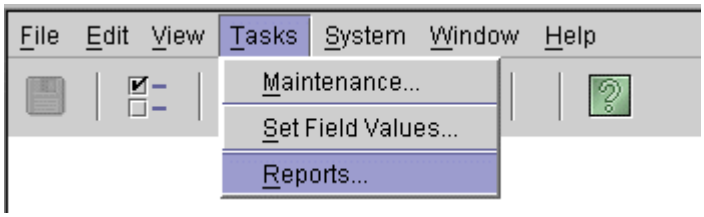
## Using the NPM GUI

### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

### *At the NPM GUI*

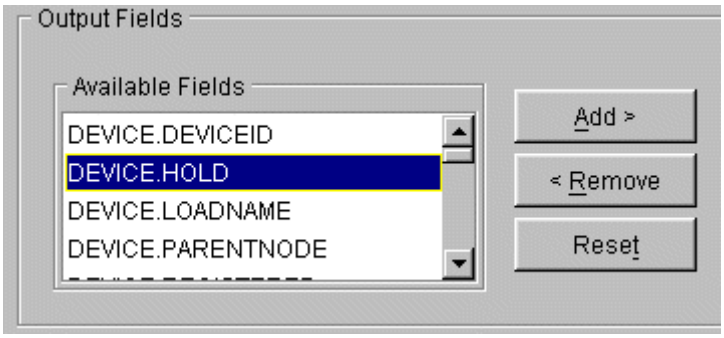
1 On the **Tasks** menu, click **Reports...**.



2 Specify the fields to be included in the new report as follows:

***Note:*** You can also edit an existing report listed under the **Report List** tab, that contains similar criteria to the report you want to create, and save it under a new name.

**a** In the **Available Fields** list, click a field of your choice.



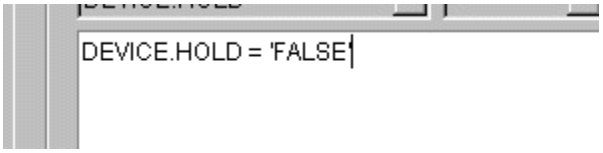

**b** Click **Add** to add the field to the **Selected Fields** list.

**c** Repeat Steps 2a and 2b for each field, then proceed to step 3.

3 In the **Report Criteria** area, specify the criteria for the report using substep a or b

**a** Type the criteria for the report in the text box.

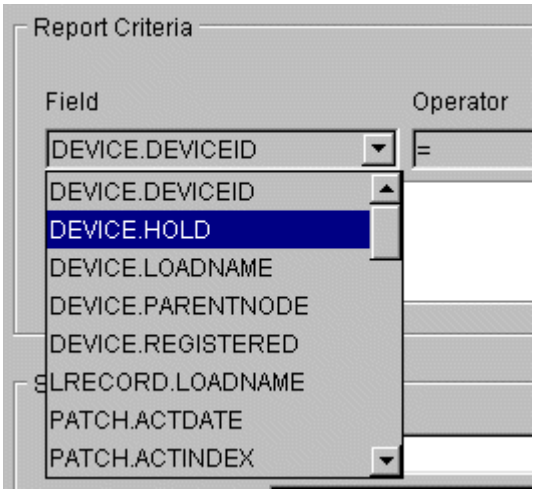
***Note:*** Parenthesis “()” may be inserted to define precedence for multiple criteria statements.



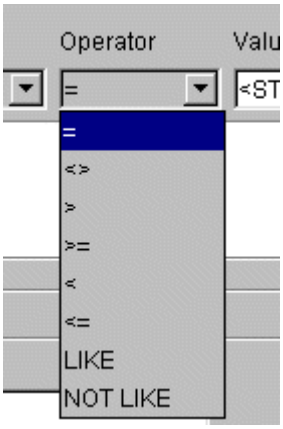

OR

**b** Specify the report criteria as follows:

**i** In the **Field** list, click the field of your choice.




**ii** In the **Operator** list, click the operator of your choice.



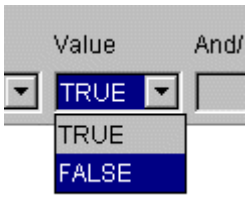

The table below lists the supported operators and their meaning.

| Operator | Meaning |
|---|---|
| = | Equal |
| <> | Not equal |
| > | Greater than |
| >= | Greater than or equal |
| < | Less than |
| <= | Less than or equal |

| Operator | Meaning |
|---|---|
| LIKE | Matches string with wildcard (%) |
| NOT LIKE | Does not match string with wildcard (%) |

**iii** In the **Value** list, select the value of your choice

***Note:*** The data type in the **Value** list will change depending on the data type selected in the **Field** list. For alphanumeric data, type the value. For boolean data, select the value.

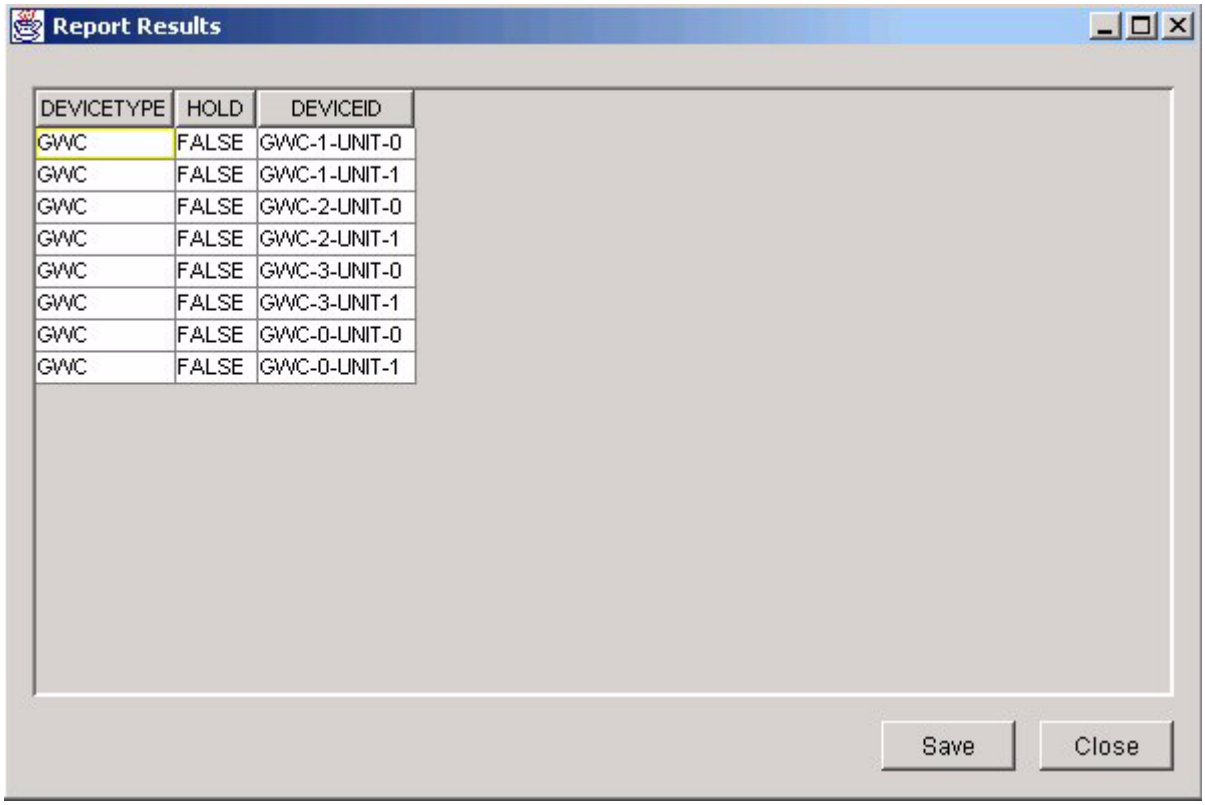



To combine multiple criteria statements, click **AND** or **OR** in the **And/Or** list.

4 Click **Execute** to generate the report.

The system displays the Report Results window.

***Note:*** The time required to generate the report depends on the number of patches and devices in the database and the complexity of the search criteria.




5 You have completed this procedure.

# Defining a plan using the NPM

## Application

Use this procedure to define a plan using the Network Patch Manager (NPM). You can define a plan using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1753
- Using the NPM GUI on page 1754

A Plan is a list of one or more tasks that are to be executed according to a specific schedule. The schedule may specify either a one time execution at a given time or repeated execution according to a frequency definition. A Plan may include the following tasks: apply, remove, audit, and reports.

There is one system-defined plan named SYSTEMPLAN. It cannot be renamed, but it can be modified or deleted. The SYSTEMPLAN is initially defined with the AUTOAPPLY and AUTORESTART tasks.

***Note 1:*** It is recommended to not have the patching autoapply task run at the same time as a line, trunk, V5.2 (International only), or CS2K data audit when an audit is scheduled.

***Note 2:*** The AUTORESTART task does not attempt to restart a device if any patches applicable to that device contain an auto restart record of “N”. In addition, the AUTORESTART task does not attempt to restart the SSPFS, as restart is not supported for the SSPFS.

A maximum of 5 plans can be defined in addition to the SYSTEMPLAN.

## Prerequisites

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

## Using the NPM CLUI

### *At your workstation*

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

### *At the NPM CLUI*

2 Define the plan by typing

```
npm> newplan <plan_name> <plan_freq>
<date_time> <max_time> <plan_desc>
```

and pressing the Enter key.

where

**plan_name**
is the name of the plan

**plan_freq**
is how often the plan should execute (Once, Hourly, Daily, Weekly, or Monthly)

**date_time**
is the date and time the plan is to be executed in mm-dd-yy hh:mm format. Plans executed more than once will begin executing at this time of day each interval.

**max_time**
is the maximum amount of time to execute the plan (No_Limit, 15_min, 30_min, 1_Hr, 2_Hr, 4_Hr, 8_Hr, or 16Hr)

**plan_desc**
is a brief description of the plan

Example

```
npm> newplan <plan_name> Weekly "07-15-03
16:59" 4_Hr "NPM weekly scheduled routine
activities"
```

3 Enable the plan by typing

```
npm> enableplan <plan_name> ON
```

and pressing the Enter key.

where

**plan_name**
is the name of the plan

4 Add a task to the plan by typing

```
npm> sched <plan_name> <tr_option> <tr_name>
<add_delete>
```

and pressing the Enter key.

where

**plan_name**
is the name of the plan

**tr_option**
determines whether a Task or Report is being added (TASK, REPORT)

**tr_name**
is the name of the task or report

**add_delete**
determines if the task or report is being added to or removed from the SystemPlan

Example

```
npm> sched <plan_name> TASK AUDIT ADD
```

5 You have completed this procedure.

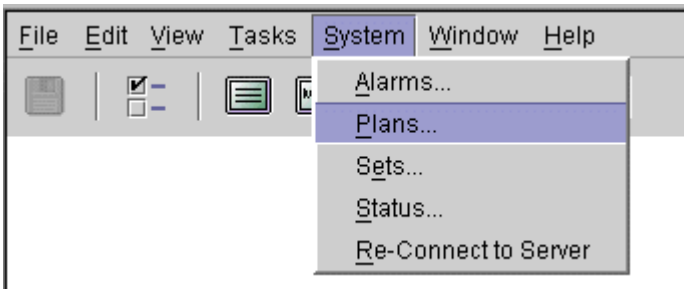
### Using the NPM GUI

#### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

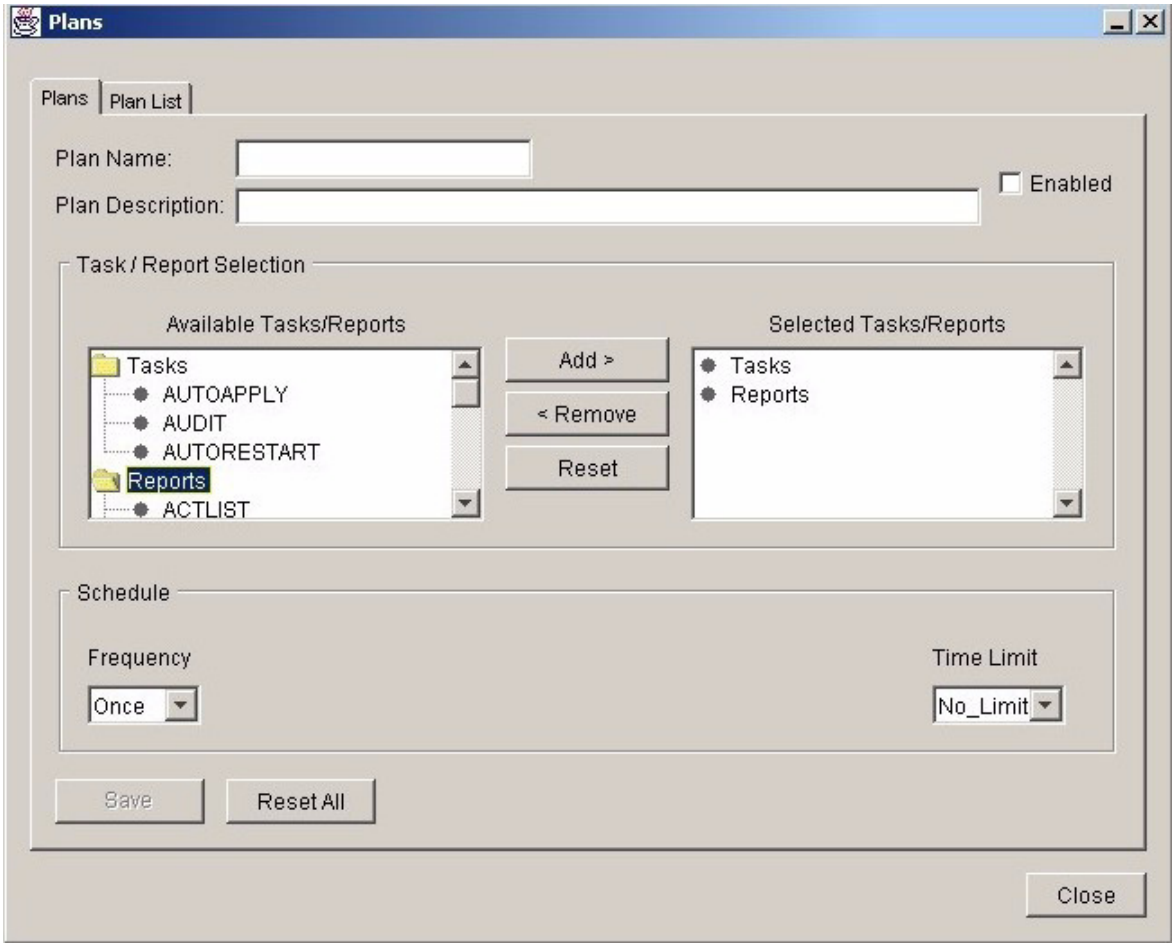
#### *At the NPM GUI*

2 On the **System** menu, click **Plans...**.




The **Plans** window opens.

3 Click the **Plans** tab if not already displayed, and click **Reset All**.




4 In the **Plan Name** box, type a unique name for the plan, and in the **Plan Description** box, type a description of the plan (optional).

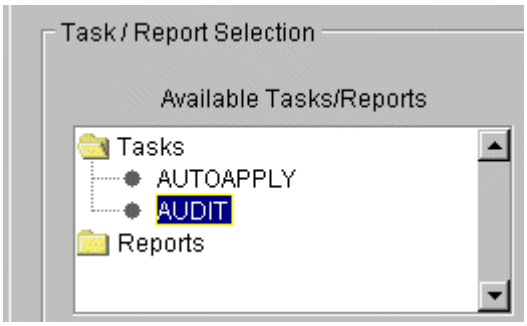



5 Click the **Enabled** check box.



6 Add tasks or reports to the plan as follows:

a In the **Available Tasks/Reports** list, double click on the **Tasks** or **Reports** folder to display the available tasks or reports.




b Click the task or report you want to add to the plan.

***Note:*** Only add reports that do not require any user input when they are run as a user may not be present at the time the plan runs. This includes pre-defined reports and user-defined reports. The pre-defined reports that require user input are as follows:

- DEVICE
- PATCH
- PATCHES_SINCE
- PATCHINFO

c Click **Add** to add the task or report to the **Selected Tasks/Reports** list.

***Note:*** The order in which the tasks and reports appear in the Selected Tasks/Reports list, is the order in which they will execute. The tasks in a plan are executed sequentially.

d Repeat step 6a and 6b for each task or report you want to add to the plan.

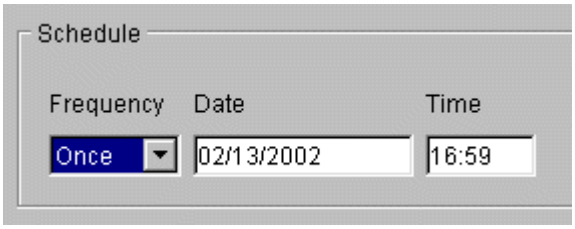
***Note:*** You can use the **Shift** key to select multiple tasks or reports consecutively, or the **Ctrl** key to select multiple tasks or reports non-consecutively.

7 Specify the execution schedule in the **Schedule** are as follows:

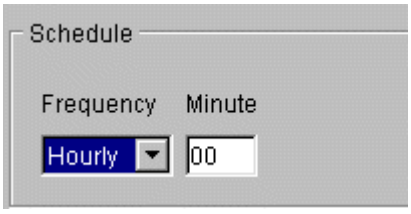
a In the **Frequency** list, click the frequency option of your choice.

When you select a frequency option, the related scheduling fields are displayed. An example of each frequency option and its related fields follows.

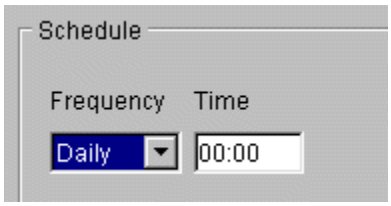
### Once option



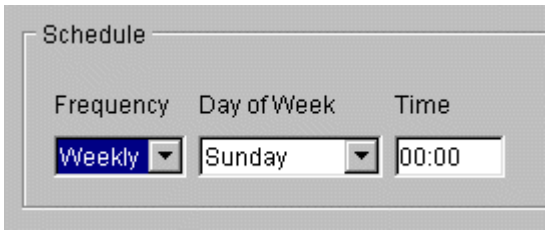

### Hourly option




### Daily option




### Weekly option

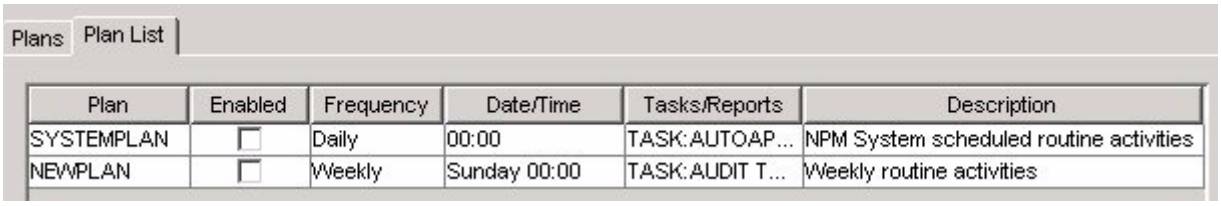



**b** Enter the appropriate scheduling information for the frequency option you selected.

**c** In the **Time Limit** list, click the time limit of your choice. The time limit defines how long the plan will be allowed to run.

8 Click **Save** to save the plan.

The new plan will be reflected on the **Plan List** tab once the NPM has saved the plan.




9 Click **Close** to close the Plans window.

10 You have completed this procedure.

# Modifying a plan using the NPM

## Application

Use this procedure to make one or more of the following modifications to a plan using the Network Patch Manager (NPM):

- enable or disable the execution of a plan
- add or delete a task or report to or from a plan
- modify the schedule of a plan
- modify the description of a plan

***Note:*** You cannot rename a plan, but you can save it under a new name and delete the original plan.

You can modify a plan using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1760
- Using the NPM GUI on page 1764

A Plan is a list of one or more tasks that are to be executed according to a specific schedule. The schedule may specify either a one time execution at a given time or repeated execution according to a frequency definition. A Plan may include the following tasks: apply, remove, audit, and reports.

There is one system-defined plan named SYSTEMPLAN. It cannot be renamed, but it can be modified or deleted. The SYSTEMPLAN is initially defined with the AUTOAPPLY and AUTORESTART tasks.

***Note 1:*** It is recommended to not have the patching autoapply task run at the same time as a line, trunk, V5.2 (International only), or CS2K data audit when an audit is scheduled.

***Note 2:*** The AUTORESTART task does not attempt to restart a device if any patches applicable to that device contain an auto restart record of “N”. In addition, the AUTORESTART task does not attempt to restart the SSPFS, as restart is not supported for the SSPFS.

A maximum of 5 plans can be defined in addition to the system-defined plan, SYSTEMPLAN.

## Prerequisites

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

**1** Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

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

| If you want to | Do |
|---|---|
| enable the execution of a scheduled plan | step 3 |
| disable the execution of a scheduled plan | step 4 |
| Add or delete a task or report to or from a plan | step 5 |
| Modify the schedule and description of a plan | step 6 |

**3** Enable the execution of a scheduled plan by typing

```
npm> enableplan <plan_name> ON
```

and pressing the Enter key.

where

**plan_name**
is the name of the plan (SYSTEMPLAN is the name of the system-defined plan)

***Note:*** If the start time for the plan has already passed, this step will fail. To correct this, modify the plan schedule to change the start time (see step 6). Then perform this step again.

Proceed to step 7.

**4** Disable the execution of a scheduled plan as follows:

**a** Disable the execution of the scheduled plan by typing

```
npm> enableplan <plan_name> OFF
```

and pressing the Enter key.

where

**plan_name**
is the name of the plan (SYSTEMPLAN is the name of the system-defined plan)

**b** Determine whether any tasks are running by typing

```
npm> qrunning
```

and pressing the Enter key.

| If | Do |
|---|---|
| a task is running | step c |
| the system response is “No maintenance commands are currently running” | step d |

**c** Allow any non-completed tasks to finish.

**d** Proceed to step 7.

5 Add or delete a task or report to or from a plan by typing

```
npm> sched <plan_name> <tr_option> <tr_name>
<add_delete>
```

and pressing the Enter key.

where

**plan_name**
is the name of the plan (SYSTEMPLAN is the name of the system-defined plan)

**tr_option**
is TASK or REPORT, which indicates whether a Task or Report is being added or deleted

**tr_name**
is the name of the task or report being added or deleted

**add_delete**
is ADD or DELETE, which indicates whether the task or report is being added or deleted to or from the plan

Example

```
npm> sched TASK AUDIT ADD
```

Proceed to step 7.

6 Modify the schedule and description of a plan by typing

```
npm> updplan <plan_name> <plan_freq>
<date_time> <max_time> <plan_desc>
```

and pressing the Enter key.

where

**plan_name**
is the name of the plan (SYSTEMPLAN is the name of the system-defined plan)

**plan_freq**
is Once, Hourly, Daily, Weekly, or Monthly, which indicates how often the plan should execute

**date_time**
is the date and time the plan is to be executed in mm-dd-yy hh:mm format. Plans executed more than once will begin executing on the day and time each interval.

**max_time**
is No_Limit, 15_min, 30_min, 1_Hr, 2_Hr, 4_Hr, 8_Hr, or 16Hr, which indicates the maximum amount of time to execute the plan

**plan_desc**
is a brief description of the plan

Example

```
npm> updplan Weekly "02-15-02 16:59" 4_Hr "NPM
System weekly scheduled routine activities"
```

7 Use the following table to determine your next step.

| If you have | Do |
|---|---|
| further modifications | step 2 |
| no further modifications | step 8 |

8 Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

9 You have completed this procedure.

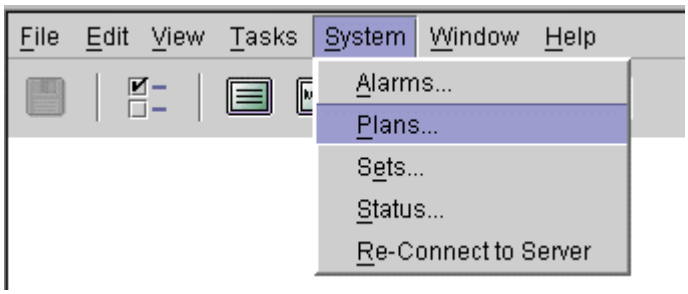
## Using the NPM GUI

### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

### *At the NPM GUI*

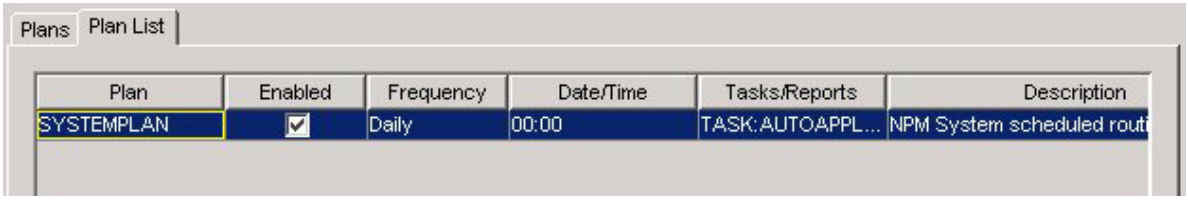
2 On the **System** menu, click **Plans...**.




The **Plans** window opens.

3 Click the **Plan List** tab.

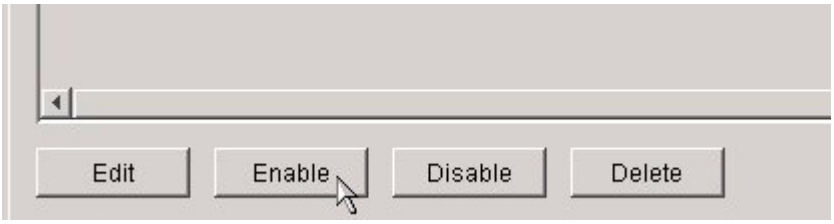
4 In the **Plans List** tab, click the plan you want to modify.




5 Use the following table to determine your next step.

| If you want to | Do |
|---|---|
| enable the execution of a scheduled plan | step 6 |
| disable the execution of a scheduled plan | step 7 |
| Modify the description of a plan | step 8 |
| Add or delete a task or report to or from a plan | step 9 |
| Modify the schedule of a plan | step 12 |

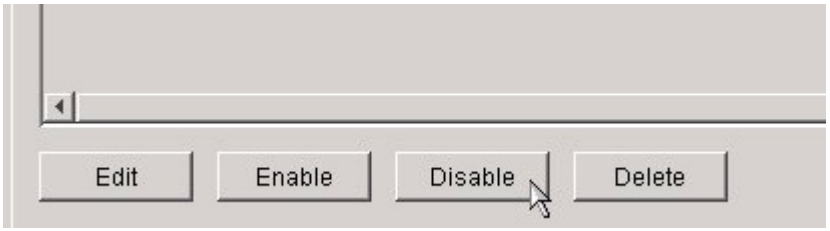
6 Click **Enable** to enable the execution of the plan.




Proceed to step 14.

7 Disable the execution of the plan as follows:

**a** Click **Disable**.




**b** On the **View** menu, click **Tasks Window** to determine whether any tasks are running.




The **Tasks** window opens.

| If the Tasks window | Do |
|---|---|
| shows that one or more tasks are running | step c |
| shows completed or no tasks | step d |

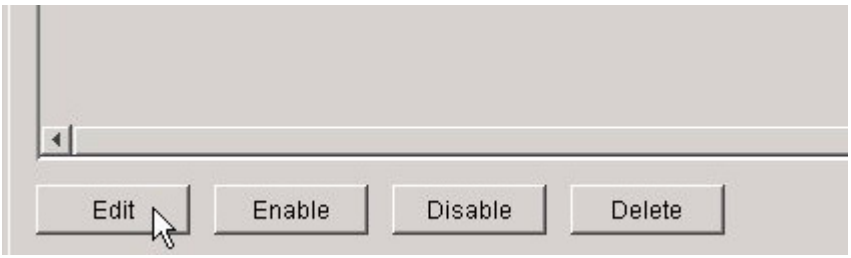
**c** Allow any non-completed tasks to finish.

**d** Click **Close** to close the Tasks window.

Proceed to step 14.

**8** Modify the description of the plan as follows:

**a** Click **Edit**.




**b** In the **Plan Description** box, type a new description of the plan.



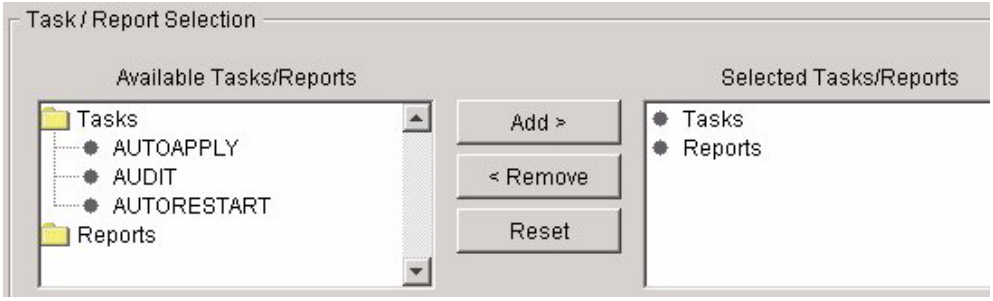

Proceed to step 13.

**9** Use the following table to determine your next step.

| If you want to | Do |
|---|---|
| add tasks or reports to the plan | step 10 |
| delete tasks or reports from the plan | step 11 |

**10** Add tasks or reports to the plan as follows:

**a** In the **Available Tasks/Reports** list, double click on the **Tasks** or **Reports** folder to display the available tasks or reports.



**b** Click the task or report you want to add to the plan.

***Note:*** Do not add reports that require user input when they execute, as a user may not be present at the time those reports execute. This includes pre-defined reports and user-defined reports. The pre-defined reports that require user input, and that you must not add, are as follows:

- DEVICE
- PATCH
- PATCHES_SINCE
- PATCHINFO

**c** Click **Add** to add the task or report to the **Selected Tasks/Reports** list.

***Note:*** The order in which the tasks and reports appear in the Selected Tasks/Reports list, is the order in which they will execute. The tasks in a plan are executed sequentially.

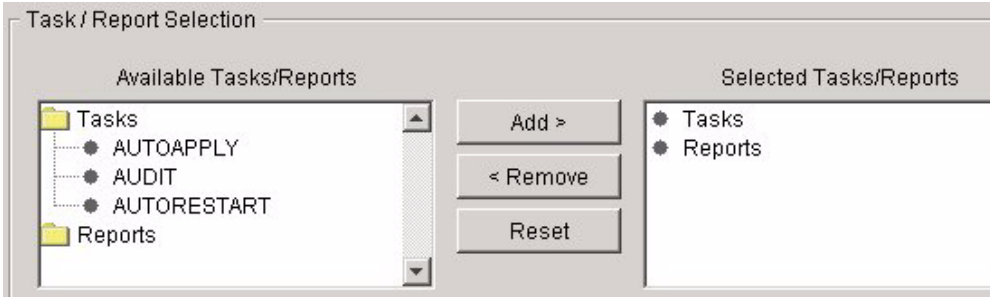
**d** Repeat step 10a and 10b for each task or report you want to add to the plan.

***Note:*** You can use the **Shift** key to select multiple tasks or reports consecutively, or the **Ctrl** key to select multiple tasks or reports non-consecutively.

Proceed to step 13.

**11** Delete tasks or reports from the plan as follows:

**a** In the **Selected Tasks/Reports** list, double click on the **Tasks** or **Reports** folder to display the selected tasks or reports.




**b** Click the task or report you want to delete from the plan.

**c** Click **Remove** to delete the task or report from the **Selected Tasks/Reports** list.

**d** Repeat step 11a and 11b for each task or report you want to remove from the plan.

***Note:*** You can use the **Shift** key to select multiple tasks or reports consecutively, or the **Ctrl** key to select multiple tasks or reports non-consecutively.

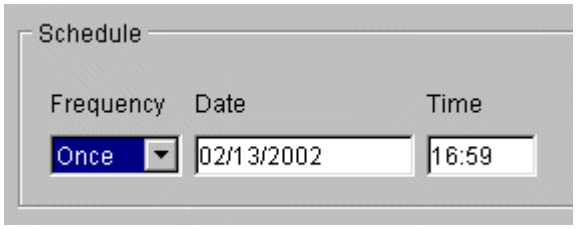
Proceed to step 13.

**12** In the **Schedule** area, update the plan schedule if required, as follows:

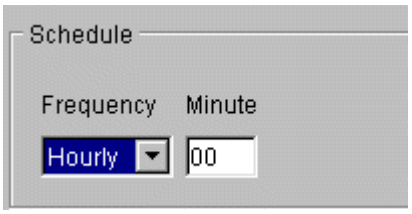
**a** In the **Frequency** list, click the frequency option of your choice.

When you select a frequency option, the related scheduling fields are displayed. An example of each frequency option and its related fields follows.

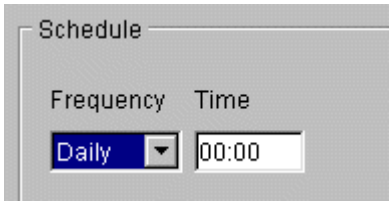
### Once option




### Hourly option




### Daily option



**Weekly option**

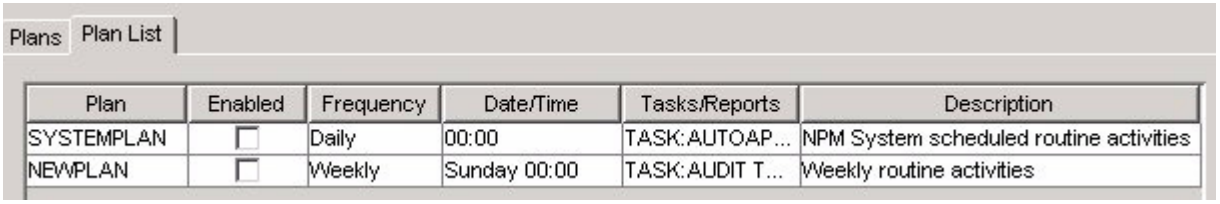



**b** Enter the appropriate scheduling information for the frequency option you selected.

**c** In the **Time Limit** list, click the time limit of your choice. The time limit defines how long the plan will be allowed to run.

**13** Click **Save** to save the plan.

The modified plan will be reflected on the **Plan List** tab once the NPM has saved the plan.




**14** Use the following table to determine your next step.

| If you have | Do |
|---|---|
| further modifications | step 5 |
| no further modifications | step 15 |

**15** Click **Close** to close the Plans window.

**16** You have completed this procedure.

# Deleting a plan using the NPM

## Application

Use this procedure to delete a plan using the Network Patch Manager (NPM). You can delete a plan using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1770
- Using the NPM GUI on page 1771

A Plan is a list of one or more tasks that are to be executed according to a specific schedule. The schedule may specify either a one time execution at a given time or repeated execution according to a frequency definition. A Plan may include the following tasks: apply, remove, audit, and reports.

There is one system-defined plan named SYSTEMPLAN. It cannot be renamed, but it can be modified or deleted. The SYSTEMPLAN is initially defined with the AUTOAPPLY and AUTORESTART tasks.

> ***Note:*** The AUTORESTART task does not attempt to restart a device if any patches applicable to that device contain an auto restart record of “N”. In addition, the AUTORESTART task does not attempt to restart the SSPFS, as restart is not supported for the SSPFS.

A maximum of 5 plans can be defined in addition to the system-defined plan, SYSTEMPLAN.

## Prerequisites

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

### *At the NPM CLUI*

**2** Disable the plan by typing

`npm> enableplan <plan_name> OFF`

and pressing the Enter key.

where

**plan_name**
is the name of the plan

**3** Delete the plan by typing

`npm> delplan <plan_name>`

and pressing the Enter key.

where

**plan_name**
is the name of the plan

**4** You have completed this procedure.

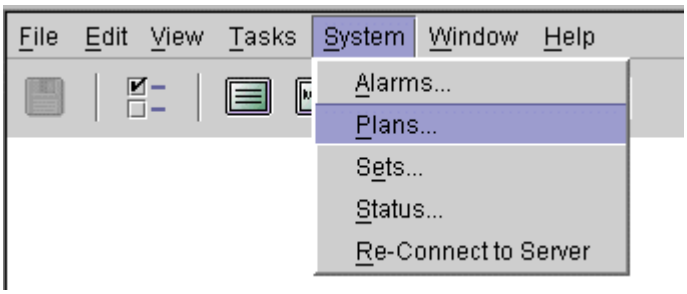
## Using the NPM GUI

### *At your workstation*

**1** Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

### *At the NPM GUI*

**2** On the **System** menu, click **Plans...**.




The **Plans** window opens.

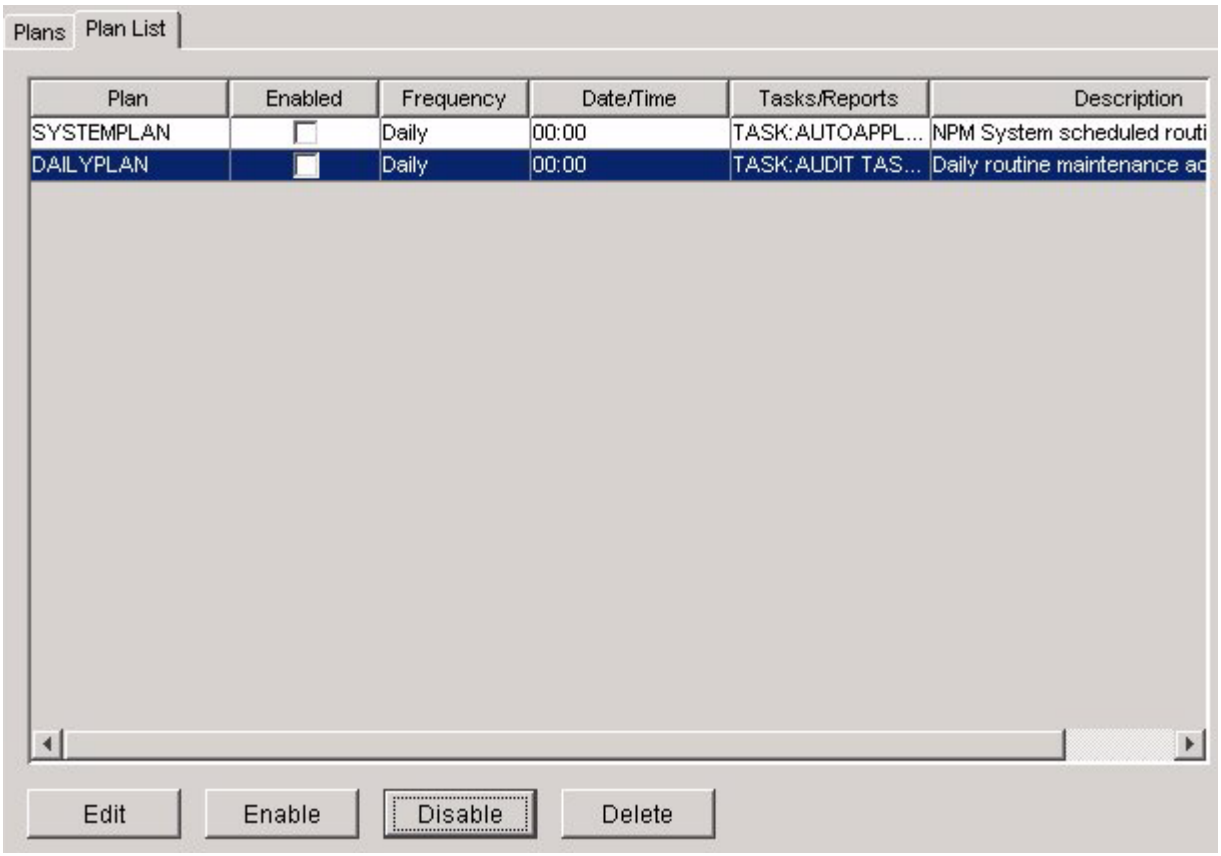
**3** Click the **Plan List** tab.

4 In the **Plan List** tab, click the plan you want to delete.

| If the plan is | Do |
|---|---|
| enabled | step 5 |
| not enabled | step 6 |

5 Click **Disable**.

6 Click **Delete**.




7 Click **Close** to close the Plans window.

8 You have completed this procedure.

# Prioritizing a patching maintenance request using the NPM

## Application

Use this procedure to move a specific patching maintenance request to the top of the queue for processing, using the Network Patch Manager (NPM). You can prioritize a request using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1773
- Using the NPM GUI on page 1774

## Prerequisites

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 1569 in this document.

## Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

### Using the NPM CLUI

***At your workstation***

**1** Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI on page 1649 in this document, if required.

***At the NPM CLUI***

**2** List the queued maintenance requests and their task ID by typing

```
npm> qrunning
```

and pressing the Enter key.

3 Move a specific maintenance request to the top of the processing queue by typing

```
npm> priority <task ID>
```

and pressing the Enter key.

where

**task ID**
is the number next to the task

The system moves the task to the top of the queue for processing.

4 You have completed this procedure.

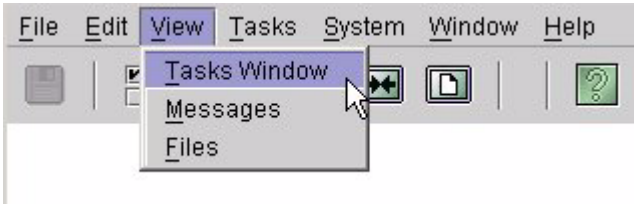
### Using the NPM GUI

#### *At your workstation*

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document, if required.

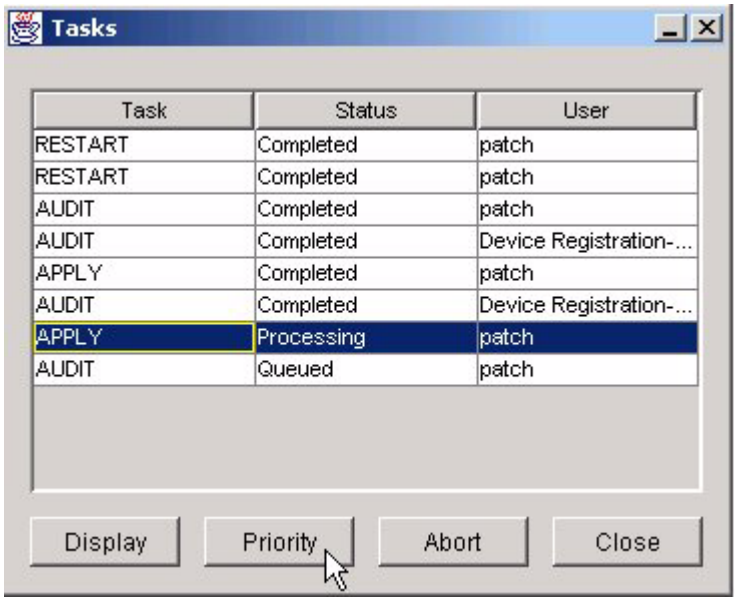
#### *At the NPM GUI*

2 On the **View** menu, click **Tasks Window**.




The **Tasks** window is displayed.

3 Select the queued task you want to move to the top of the processing queue, and click **Priority**.




The system moves the task to the top of the queue for processing.

4 You have completed this procedure.

# Patching MG 9000 Manager software

The MG 9000 Manager server, mid-tier, and OM Collector are patched using the Network Patching Manager (NPM) patching system. The user must restart the server, mid-tier, and OM Collector applications through the NPM following application or removal of patches.

For information and procedures for patching the MG 9000 Manager software using the NPM, refer to the Succession Patching chapter in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.

The following logs are generated when the MG 9000 Manager server shuts down or starts:

- MGEM700 - The element manger server is starting.
- MGEM702 - The mid-tier server is now starting.
- MGEM703 - The mid-tier server is shutting down.
- OMC700 - The OM Collector process was started.
- OMC701 - The OM Collector process is shutting down.

## Patching the MG 9000

The MG 9000 is patched using the Network Patching Manager (NPM) patching system. Any device to be patched must first be audited to determine the load name compatibility with the patch before applying the patch.

For information and procedures for patching the MG 9000 software using the NPM, refer to the Succession Patching chapter in *ATM Solutions Upgrades*, NN10261-450 or *IP Solutions Upgrades*, NN10344-450.

# Patching the CS 2000 Compact

## Patching software

Platform and call processing application software is patchable. Platform patching does not patch the Linux kernel.

## What's new in platform software patching

### SN07

The format for the name of platform patch files has changed from `3pclinuxpatch_6.20.1.1` to `ncgl_cca_patch_5.15.1.1`. The procedure for applying patches remains unchanged.

### SN06

For the SN06 release, the command to start the Call Agent Manager has changed from **tpcmtc** to **ccamtc**. The patching procedure remains the same as the patching procedure for the SN05 release.

For customers registered with Regional Patch Selector (RPS), platform patches can be delivered directly from the RPS server to the `/swd/3pc/patch` directory on the CS 2000 Core Manager. If customers have platform patches delivered to an electronic dropbox, the customer is responsible for transferring the Call Agent platform patches to the `/swd/3pc/patch` directory on the CS 2000 Core Manager.

For Linux warranty patching visit Nortelnetworks.com to retrieve the patches:
Nortelnetworks.com
Select: Software Downloads
Select: Families *(top right under Find Products)*
Select: Succession Product Family
Select: Succession Communication Server 2000-Compact

### SN05

For the SN05 and ISN05 releases, platform patching offers greater robustness than earlier releases. Patch files are no longer cumulative and the Call Agent Manager enables validation of patch files for out of order application of patches.

If a patch fails to apply, the patching software automatically rolls back the patch. This feature enables the application of patches on the active Call Agent rather than patching the inactive Call Agent as required in earlier releases. A timer automatically commits patches after 10 minutes. Unless the user requests otherwise, patches are applied on

the active Call Agent, success is verified, and then the patching software begins applying the same patch on the inactive Call Agent.

## Platform patching

Patch files have the following identification scheme:

ncgl_cc_patch_r.w.c.v

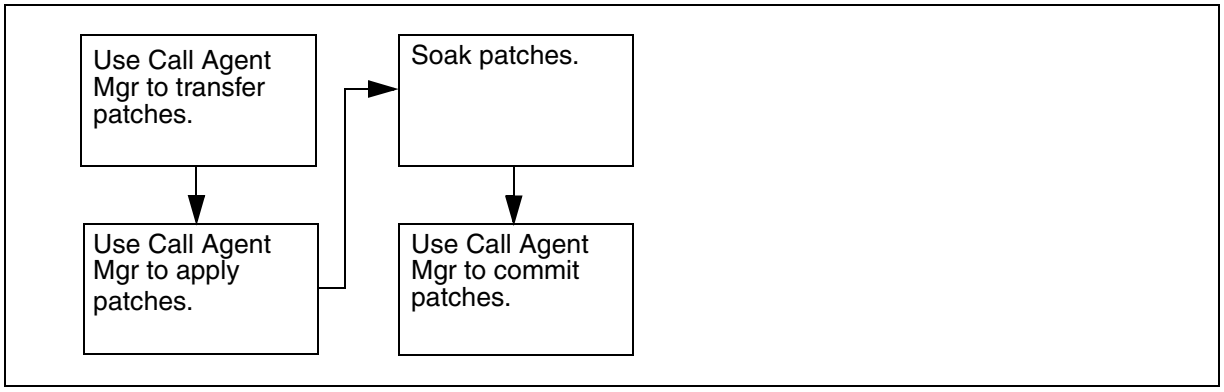
- **r** indicates the release. For example, 5.
- **w** indicates the week number of the load build. For example, 15.
- **c** indicates the compile. This value is equal to the fc value for an NCL or equal to (fc+i) for an MNCL. The patch is only applicable to a load that matches this number.
- **v** indicates the patch version.

***Note:*** Patches are only applicable to NCLs and MNCLs with matching r, w, and c values as the patch file.

Patching of the platform software is done through the Call Agent Manager.

Refer to the following flowchart for an overview of the platform patching procedure.

### Platform patching overview




## Call processing application patching

Patching of the call processing application is done through Post-Release Software Manager (PRSM). This tool is available through the MAP.

Refer to *Post-Release Software Manager Reference Manual*, 297-8991-540, for information about patching the call processing application.

# Transfer platform patch files

Verify that patch files are installed on the CS 2000 Core Manager or CBM before completing this procedure. Platform software patch files are stored in `/swd/3pc/patch` for the Call Agent.

For Linux warranty patching visit Nortelnetworks.com to retrieve the patches:
Nortelnetworks.com
Select: Software Downloads
Select: Families *(top right under Find Products)*
Select: Succession Product Family
Select: Succession Communication Server 2000-Compact

This procedure requires root privilege.

### *At the Call Agent Manager*

**1** Enter the Transfer level:

```
> Admin
> SWIM
> Transfer
```

```
CallAgent       SYS       CON       APPL              Unit: 0
    .            .         .         .

Transfer     Current Load : 5.15.1.0
 0 Quit      Source       : /3pc/patch
 2 Select
 3 Fetch      # Patch Description                    Version
 4 Source     1 ncgl_cca_patch                      5.15.1.9
 5            2 ncgl_cca_patch                      5.15.1.8
 6            3 ncgl_cca_patch                      5.15.1.7
 7            4 ncgl_cca_patch                      5.15.1.6
 8
 9
10
11 Up
12 Down
13 LogQuery
14 Alarm                        Filesets on the source: 1 to 4 of 4
15
16
17 Help
18 Refresh
  mtc
Time  13:06  >
```

***Note 1:*** If patch files do not appear in the list, verify that the patch files are installed on the CS 2000 Core Manager or CBM in `/swd/3pc/patch` and have read permissions such as 777 or 755.

***Note 2:*** If patch files are stored in a different directory, use the SOURCE command to change the source directory. The CS 2000 Core Manager or CBM prepends `/swd` to all values.

2 Use the Select command to select the patch file to transfer from the CS 2000 Core Manager or CBM:

```
> Select num
```

**num**
is the decimal value that indicates the fileset

3 Use the Fetch command to retrieve the selected patch file:

```
> Fetch
```

***Note 1:*** If the FETCH command fails, verify that the patch files are installed and applied on the CS 2000 Core Manager or CBM and that the files have read permission set such as 777 or 755.

***Note 2:*** The fetch command retrieves the patch file and stores it on the active and inactive Call Agent cards by default. ACTIVE and INACTIVE options enable storage to a specific Call Agent card.

***Note 3:*** If the patch fileset already exists, the Call Agent prompts to determine if the existing file should be overwritten. Patch filesets can be overwritten.

```
Fileset already present. Overwrite?
Please confirm ("YES", "Y", "NO", "N"):
```

4 This procedure is complete.

# Apply platform software patch



**CAUTION**
**Possible service interruption**
Do not perform any patching activity within the first ten minutes following a Call Agent unlock.

***At the Call Agent Manager***

**1** Enter the Patch level:

```
> Admin
> SWIM
> Patch
```

```
CallAgent       SYS       CON       APPL              Unit: 0
    .            .         .         .

Patch         Current Load : 5.15.1.0
 0 Quit       Filter       : ALL
 2 Select
 3 Apply       # Patch Description              Version        Status
 4 Delete      1 ncgl_cca_patch                 5.15.1.9       NEW
 5 Commit      2 ncgl_cca_patch                 5.15.1.8       VALIDATED
 6             3 ncgl_cca_patch                 5.15.1.7       VALIDATED
 7             4 ncgl_cca_patch                 5.15.1.6       VALIDATED
 8
 9
10
11
12
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
  mtc
Time  14:14  >
```

2 Use the Select command to select the patch file to apply:

```
> Select <num>
```

**num**
is the integer value that indicates the patch

3 Use the Disadmin command to display any warnings or special application instructions. Perform any special application instructions:

```
> Disadmin
```

4 Reselect the patch and use the Validate command to verify that all dependencies are met:

```
> Select <num>
> Validate
```

| If | Do |
|---|---|
| dependencies are met and the patch validates successfully | step 5 |
| dependencies are not met and the validate fails | Fetch, select, and validate earlier patches before attempting to apply this patch. For example, if the current patch level is 5.26.1.10 and patch file 5.26.1.13 fails validation, attempt to validate and apply patches 5.26.1.11 and 5.26.1.12. |

5 Reselect the patch and use the Apply command to apply the patch file:

```
> Select <num>
> Apply
```

| If | Do |
|---|---|
| the patch applied successfully | step 6 |
| the patch fails to apply | Refer to Troubleshooting. |
| the patch is an older version or requires special application instructions | Refer to Additional information. |

6

**ATTENTION**

At this point, the patch is applied and is part of the running load. Soak the patch according to telephone operating company procedure before committing the patch. Patches are automatically committed 10 minutes after application unless manually committed earlier.

Reselect and use the Commit command to write the change to persistent storage. The committed load boots the next time the card is reset or rebooted:

```
> Select <num>
> Commit
```

***Note:*** If the ACTIVE or INACTIVE options are used, committing a patch on one card raises a C_MisM alarm. Committing the same patch on the second card clears the alarm. No alarms are raised or cleared if this is the first patch being committed.

7 If additional patches need to be applied, repeat from step 2. Otherwise, this procedure is complete.

## Troubleshooting

The following table describes causes of possible problems, and what actions are required.

| Problem | Possible cause | Action |
|---|---|---|
| SWACT while running patch commands | The patch could be the cause of the SWACT. | Patching does not continue and patches are rolled back on the formerly active Call Agent. Contact Nortel Networks support personnel. |
| loss of mate communication while running patch commands | • link failures at router<br>• link pulls<br>• abnormal software process termination | Patching completes for the Call Agent on which patching was executing and looks for patch mismatch between the Call Agent cards.<br>If communication fails during inactive Call Agent patching, patching completes successfully because the active is already patched. |
| patch files available to only one Call Agent | • STORM failure<br>• failure to retrieve patch files and write them to storage | Correct STORM failure. Use the **TRANSFER** command to retrieve the files again. Attempt patch application again. |
| patch levels out of synchronization between active and inactive Call Agent cards | A previous attempt to apply patches failed. | Contact Nortel Networks support personnel for assistance with synchronizing the patch database files and determining the cause of failure. |

## Additional information

This section contains information about reverting to older patch levels and patch scenarios that require a platform upgrade.

### Reverting patches

Uncommit a patch from the running load with the **UNCOMMIT** command. Unless specified with the ACTIVE or INACTIVE options, the patch is uncommitted from the active Call Agent and then from the inactive Call Agent.

### Non-patchable versions

Non-patchable version patch files require a newer maintenance release than the currently running release.

Upgrade the platform software load first, then apply the patch file. Refer to the procedure “Upgrade strategy” in *Upgrading the CS 2000 Core Manager*, NN10060-461.

### Special application instructions

If the patch file contains special application instructions, use the **DISADMIN** to display the instructions. Execute the required instructions.

### PATCH level command reference

The following list of commands are available from the PATCH level.

**SELECT**

This command selects a patch file by integer value from the list of fetched patches for validation, display of administrative information, application, commit, or uncommit. For example, SELECT 5.

**APPLY**

This command applies a selected patch file to the running load. Unless specified with the ACTIVE or INACTIVE options, the selected patch is applied on the active Call Agent and then applied on the inactive Call Agent.

**DELETE**

This command deletes the selected patch file from storage. The patches cannot be in the APPLIED or COMMITTED state. Deleting patches in the APPLIED or COMMITTED state causes problems during booting and future attempts to remove the patches fail.

**COMMIT**

This command commits the selected patch file to the running load. The patch must be in the APPLIED state and when the card is reset or reboots, the patch is re-applied. This command accepts ACTIVE and INACTIVE options, though the options are expected to be used during platform and call processing application upgrades only.

**UNCOMMIT**

This command uncommits the selected patch file from the running load. The patch file remains in storage and remains applied, but will not be re-applied after reset or a reboot. If other applied patch files depend on the selected patch file, a warning message is generated. Uncommit is permitted, but the dependencies are broken. Nortel Networks does not recommend uncommitting patches that break dependencies. Use the **REMOVE** command to un-apply a patch from the running load.

**FILTER**

This command alters the list of patch files to show only the patch files that are in a specified state. The list of available states is ALL, NEW, VALIDATED, APPLIED, COMMITTED, and REMOVED.

**REMOVE**

This command un-applies the selected patch file from the running load. The patch file must not be in the COMMITTED state. The removed patch files are not deleted from storage. If other applied patches depend on the selected patch file, removal is refused. Remove uncommit and remove the patches that depend on the selected patch file first.

**VALIDATE**

This command validates that the selected patch file can be successfully applied to the running load. This command accepts ACTIVE and INACTIVE options though the options are only useful if the two Call Agent cards are running different patch levels.

**DISADMIN**

This command displays administrative data about the selected patch file.

**UP**

This command scrolls up the list of patch files.

**DOWN**

This command scrolls down the list of patch files.

# Passport 8600 Software Rollback for the CS-LAN

This procedure rolls back software upgrades to Passport 8600 pairs that support the Succession Communication Server LAN (CS-LAN). The rollback uses a phased approach to prevent service interruption.

**ATTENTION**

Nortel Networks strongly recommends thoroughly reading section Important rollback considerations *before* attempting procedure Rolling Back Software Upgrades on Passport 8600s Supporting CS-LANs.

## Important rollback considerations



**CAUTION**

Manually entered configuration changes executed since the completion of a Passport 8600 upgrade are lost when rolling back to version 3.7.0.0.

Nortel Networks strongly recommends re-entering configuration changes after the completion of the rollback procedure.

Beginning with SN07, this rollback procedure addresses Passport 8600 configurations with dual call processing units (CPU). Therefore, execute all CPU-related commands on the master CPU, except where otherwise noted. Also a Passport 8600 must be running with a v3.7.0.0 software load *before* a dual CPU with a high-availability (HA) mode is configured for it.

***Note:*** Also, if rolling back to pre-v3.7.0.0 software version after having attempted a v3.7.0.0 software upgrade for a dual CPU configuration, users must disable the dual CPU HA flag setting *before* the rollback begins.

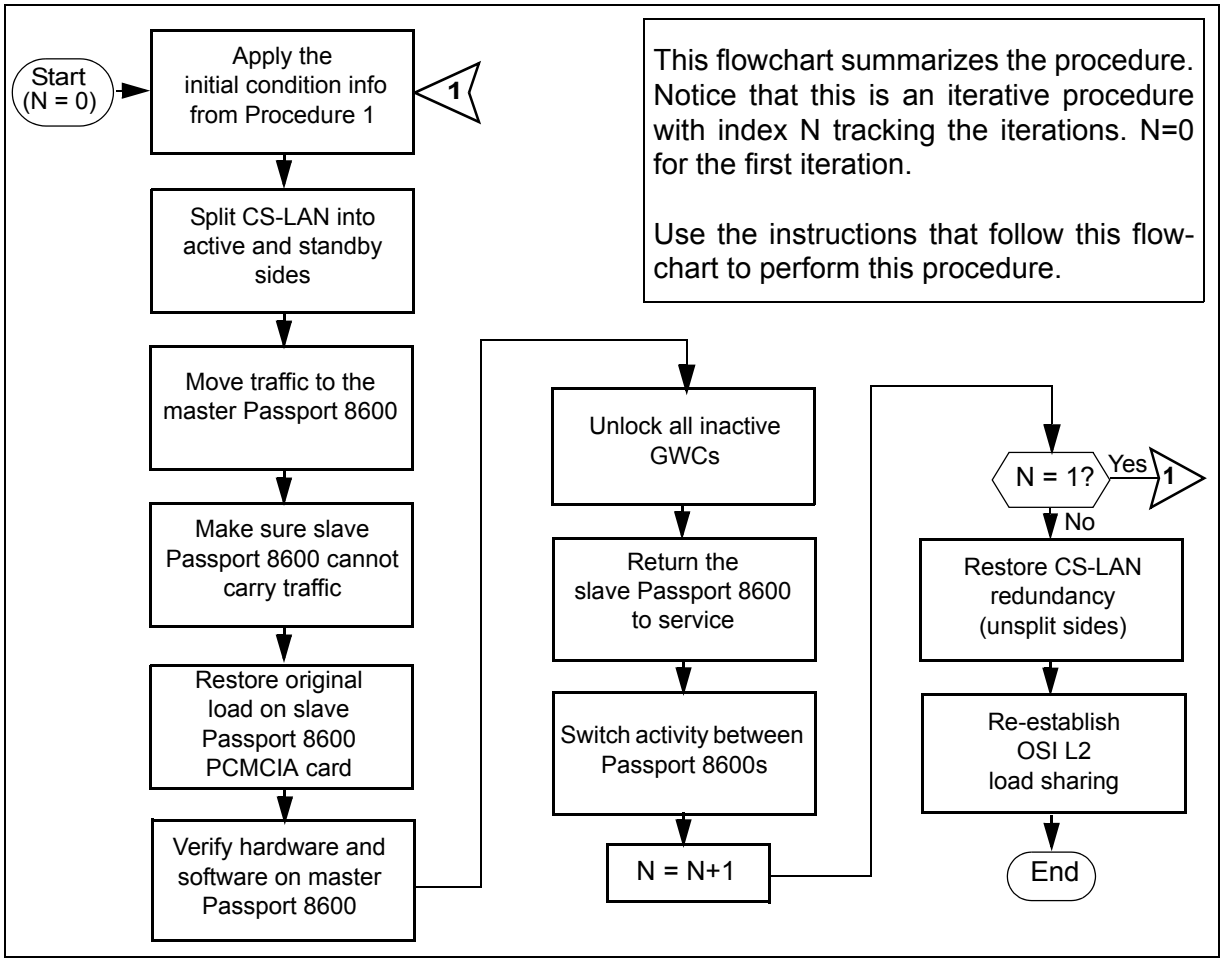
Customer rolling back to a fully patched SN06 (or greater) load can skip the following steps when addressing the Gateway Controller (GWC) in this procedure:

- step 31, step 32a through step 32c
- step 76

Also, refer to sub-section Text conventions for brief descriptions and examples of filenames that appear in commands throughout this procedure. This subsection also includes descriptions for distinguishing between the master and standby CPUs in the command line interface (CLI).

The following flowchart summarizes the Passport 8600 rollback procedure.

**Rolling back a software upgrade on Passport 8600s for the CS-LAN**



## Text conventions

This procedure uses the following text conventions for displaying filenames that appear in commands.

***Note:*** Refer to this section, as needed throughout the course of the upgrade and rollback procedures, for clarifications on the different software files.

**<a.b.c.d>**
is the IP address of the TFTP server

**<bootbkup>**
is the name of the backup copy of the boot configuration file on the PCMCIA card

**<cfgbkup>**
is the name of the backup copy of the software configuration file on the PCMCIA card

**<new3DES>**
is the name of the new Triple data encryption standard (3DES) file on the PCMCIA card

*for example:*
p80cXXX.img

*where:*
cXXX is the release number

**<newATM>**
is the name of the new ATM load file on the PCMCIA card

*for example:*
p80tXXXX.dld

*where:*
XXXX is the release number of the load

**<newboot>**
is the name of the new boot monitor image file on the PCMCIA card

*for example:*
p80bXXXX.img

*where:*
XXXX is the release number of the load (for example, p80b3320.img)

***Note:*** Use the boot monitor image file when executing a boot command.

**<newDES>**
is the name of the new data encryption standard (DES) file on the PCMCIA card

*for example:*
p80cXXX.des

*where:*
cXXX is the release number

**<newload>**
is the name of the new software image file on the PCMCIA card

*for example:*
p80aXXXX.img

*where:*
XXXX is the version of the software (for example, p80a3320)

***Note:*** Use the primary or secondary (or both) software image files when configuring a bootconfig command.

**<old3DES>**
is the name of the original DES file

*for example:*
p80cXXX.img

*where:*
cXXX is the release number

**<oldATM>**
is the name of the original ATM load file

*for example:*
p80tXXXX.dld

*where:*
XXXX is the release number of the load

**<oldboot>**
is the name of the original boot monitor image file

*for example:*
p80bXXXX.img

*where:*
XXXX is the release number of the load (for example, p80b3320.img)

**<oldDES>**
is the name of the original DES file

*for example:*
p80cXXX.des

*where:*
cXXX is the release number

**<oldload>**
is the name of the original software image file

*for example:*
p80aXXXX.img

*where:*
XXXX is the version of the software (for example, p80a3320)

**<slot>**
is the slot number for the Passport 8600

**<sonetif >**
is the Sonet interface on the ATM blade

**<swloadbkup>**
is the name of the backup version of the software image file

*for example:*
p80aXXXX.img

*where:*
XXXX is the version of the software (for example, p80a3320)

**<vid>**
is the identifier of each virtual local area network (VLAN)

**<vrid>**
is the VRRP identifier

### CPU syntax

The CLI prompt syntax for the CPUs is as follows:

**<Passport_chassis_name>:CPU-slot#**
*where:*

the absence or inclusion of the “@” symbol at the beginning of the command syntax identifies the master or standby CPU, respectively.

**8600_04:5#**
refers to the master CPU

**@8600_04:6#**
refers to the standby CPU

## Rolling Back Software Upgrades on Passport 8600s Supporting CS-LANs

**ATTENTION**

This roll-back procedure assumes that procedure Upgrading Passport 8600 software for the CS-LAN was aborted after some stage of progress.

This procedure further assumes that, as a minimum step 1 to step 9 of Upgrading Passport 8600 software for the CS-LAN were successfully completed.

***Refer to*** Procedure Upgrading Passport 8600 software for the CS-LAN***.***

**1** This procedure is iterative (iteration index is N). Use the conventions defined in the following table to complete this procedure.

| Iteration | Slave Passport 8600 | Master Passport 8600 |
|---|---|---|
| First Pass | Chassis N = 0 | Chassis X = 1 |
| Second Pass | Chassis N = 1 | Chassis X = 0 |

**2** Refer to step 5 in Upgrading Passport 8600 software for the CS-LAN and reproduce the **VRID**, **VID (P/V)**, and **PRIO**

information for Passport 8600 Chassis 0 and 1 in the following table.

**Passport 8600 - Initial conditions**

| | Status | | | | |
|---|---|---|---|---|---|
| | | Chassis 0 | | Chassis 1 | |
| VRID | VID | OSPF Metric | VRRP PRIO | OSPF Metric | VRRP PRIO |
| VRID 1 | | | | | |
| VRID 2 | | | | | |
| VRID 3 | | | | | |
| VRID 4 | | | | | |
| VRID 5 | | | | | |
| VRID 6 | | | | | |
| VRID 7 | | | | | |
| VRID 8 | | | | | |
| VRID 9 | | | | | |
| VRID 10 | | | | | |

***Note:*** As Passport 8600 does not carry call processing traffic in the the PT-AAL1 solution, not all the Succession componentry in this rollback procedure applies to PT-AAL1. Therefore if rolling back the upgrade of the Passport 8600 software in a PT-AAL1 solution, skip to step 62.

***Use the Passport 8600 CLI to split the Passport 8600 into active and standby sides***

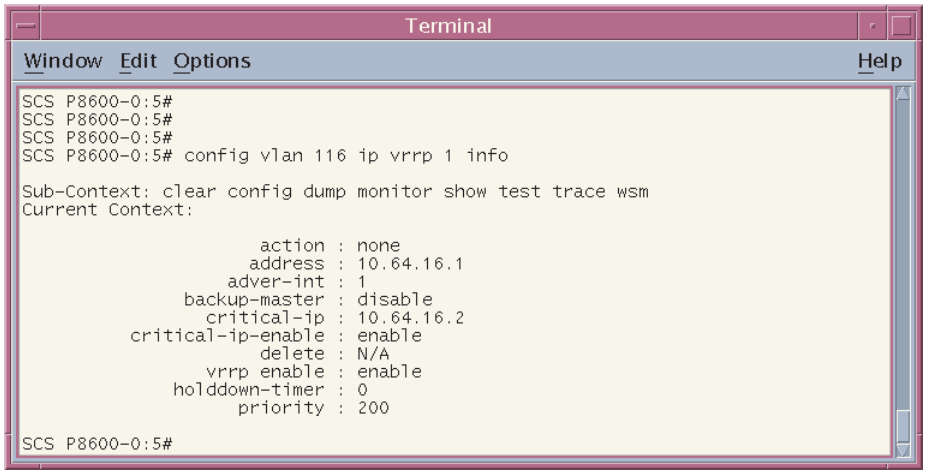
**3** Collect and record Passport 8600 Chassis N VRRP priority OSPF metrics as follows:

**a** type:

**config vlan <vid> ip vrrp <vrid> info**

where **<vid>** is the identifier of each VLAN and **<vrid>** is the VRRP identifier.

***Note:*** Refer to table Passport 8600 - Initial conditions to determine the **VID** and **VRID** information for Passport 8600 Chassis N.




**b** record **<vrid>** priority information for use in step 90

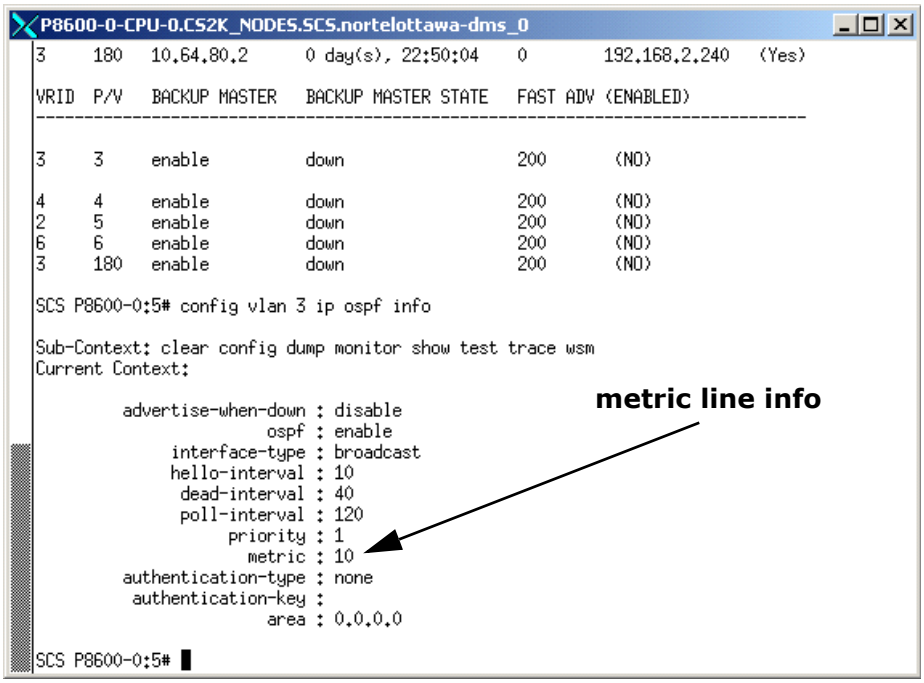
**c** type:

**config vlan <vid> ip ospf info**

*The CLI displays the OSPF information in the **metric** line item that appears near the bottom of the window (see figure on next page).*

**d** record the OSPF metric information for use in step 90

**e** repeat sub-step a to sub-step d for each VLAN provisioned on the router




4 Make sure Passport 8600 Chassis N is the slave as follows:

**a** set the VRRP priority to 1 by typing

**config vlan <vid> ip vrrp <vrid> prio 1**

***Note:*** Setting Passport 8600 Chassis N **<prio>** to 1 makes it slave.

**b** set the OSPF priority to 1000 by typing

**config vlan <vid> ip ospf metric 1000**

**c** repeat sub-step a and sub-step b for each VLAN provisioned

5 Save the new Passport 8600 Chassis N configuration by typing:

**sav config**

*This updates the new Passport 8600 configuration so that VRRP settings are maintained after any subsequent reboot.*

6 Select the next step as follows:

| If your CS-LAN: | Do |
|---|---|
| includes ATM PVGs directly connected to the Passport 8600 (i.e., a non-VR solution) | step 7 |
| includes PVGs connected by Gig Ethernet (GigE) | step 22 |

| If your CS-LAN: | Do |
|---|---|
| does not include PVGs | step 22 |
| includes ATM interfaces connected to a Passport 15000 chassis running VR or VrAp | step 22 |

### *Use the PVG CLI to determine the PVG IP addresses*

**7** Check the provisioning information for the VSPs, NSTA, and VGS subcomponents as follows:

**a** display media and signaling gateway IP addresses by typing:

**d -p nsta/* vgs ctrl/***

*The following list provides sample MG and SG IP addresses for a single VSP card provisioned in slot 7.*

```
+=====+====+---------------+---------------
|Nsta |Ctrl|    ipAddr     |    dnsList
+=====+====+---------------+---------------
|    7|mg  |172.16.201.2   |
|    7|sg  |172.16.201.6   |
```

***Note:*** *The ... **nsta/* vgs ctrl/**** *component of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows MG and SG IP addresses for a single VSP card provisioned in slot 7.*

**b** display the IPmcon IP address by typing:

**d -p nsta/* vgs ipmcon**

*The following list provides a sample IPmcon IP address for a single VSP card provisioned in slot 7:*

```
+=====+---------------+-----+---------------
|Nsta |    ipAddr     |udpBa|Response
|     |               | se  |
+=====+---------------+-----+---------------
|    7|172.16.201.10  |49152|
```

***Note:*** *The ... **nsta/* vgs ipmcon** component of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows IPmcon IP address for a single VSP card provisioned in slot 7.*

***Use each Passport 8600 CLI to verify that the PVGs are set up redundantly***

**8** Check the VLAN configuration file by typing the following command on each Passport 8600 chassis:

**sho config module vlan**

*This command outputs all VLANs provisioned on the Passport 8600 Chassis. The example that follows shows the output of this command for only one VSP blade:*

```
vlan 702 create byport 1 name "PVG40-vsp07-mg"
vlan 702 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 702 ports add 8/1 member portmember
vlan 702 ip create 172.16.201.1/255.255.255.252 mac_offset 5
vlan 706 create byport 1 name "PVG40-vsp07-sg"
vlan 706 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 706 ports add 8/1 member portmember
vlan 706 ip create 172.16.201.5/255.255.255.252 mac_offset 14
vlan 710 create byport 1 name "PVG40-vsp07-media"
vlan 710 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 710 ports add 8/1 member portmember
vlan 710 ip create 172.16.201.9/255.255.255.252 mac_offset 6
```

***Note:*** *Both Passport 8600s should display the identical PVG VLAN configuration. The **vlan ### ports add** entry identifies each VSP ATM Sonet connection. This information is required in* step 14*.*

**9** Select a Passport 8600 chassis (Chassis N or Chassis X) and record the routing table information for all of its VSP VLANs as follows:

***Note:*** Sub-step c repeats this step for the other chassis

**a** type:

**sho ip route info ip x.y.z**

where x.y.z specifies the IP Net address provided at step 7.

***Note:*** Specifying the x.y.z octets limits the command output to those nodes served by the specified IP Net.

Refer to the figure in step 16 of Upgrading Passport 8600 software for the CS-LAN for more information about IP Net addressing.

*The following list provides an example for the command output for one of the Passport 8600s:*

```
================================================================================================
                                Ip Route
================================================================================================
          DST             MASK              NEXT         COST   VLAN   PORT    PROT  AGE TYPE PRF
------------------------------------------------------------------------------------------------
   172.16.201.0 255.255.255.252   172.16.201.1     1  702   -/-    LOC    0 DB     0
   172.16.201.4 255.255.255.252   172.16.201.5     1  706   -/-    LOC    0 DB     0
   172.16.201.8 255.255.255.252   172.16.201.9     1  710   -/-    LOC    0 DB     0

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.
------------------------------------------------------------------------------------------------
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW
```

*The following list provides an example for the command output for the other Passport 8600 Chassis:*

```
================================================================================================
                                Ip Route
================================================================================================
          DST             MASK              NEXT         COST  VLAN   PORT  PROT    AGE TYPE PRF
------------------------------------------------------------------------------------------------
   172.16.201.0 255.255.255.252   172.30.242.230   20    80  -/-  OSPF    0 IB    120
   172.16.201.4 255.255.255.252   172.30.242.230   20    80  -/-  OSPF    0 IB    120
   172.16.201.8 255.255.255.252   172.30.242.230   20    80  -/-  OSPF    0 IB    120

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.
------------------------------------------------------------------------------------------------
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW
```

***Note 1:*** *The routing information under the PROT column heading should indicate either VSP subnet LOC or OSPF.*

***Note 2:*** *If both Passport 8600s indicate the same status for the same VSP subnet, this is a non-standard condition. Contact your next level of support.*

**ATTENTION**

To prevent service interruption Passport 8600 VSP VLANs must be OSPF on Chassis N and LOC on Chassis X. Detailed steps forcing compliance to this requirement begin at step 16.

**b** repeat sub-step a for each VSP VLAN on the selected Passport 8600 chassis.

**c** select the other Passport 8600 chassis and repeat sub-step a and sub-step b.

***Use the PVG CLI to verify the correct provisioning of each VSP***

**10** Check the SPVCAP subcomponent of each VSP VGS Ctrl/<mg,sg> and IPmcon as follows:

**a** display the provisioning information for each VSP by typing:

**d -p -no nsta/* vgs ctrl/* spvcap**

*The following list shows VSP provisioning information for slot 7. The actual command output lists all VSP information.*

```
Nsta/ 7 VGS Ctrl/mediaGateway SpvcAp
   atmServiceCategory = nrtVariableBitRate
   peakCellRate  = 800 cells
   sustainedCellRate= 400 cells
   maximumBurstSize= 100 cells
   retryLimit    = 0
   localAddress  = 45613512123400002F000000010020480D527001
   remoteVpiVci  = 7.2
   addressToCall = 45613512123400002F000000010020480D008D00
Nsta/ 7 VGS Ctrl/signalingGateway SpvcAp
   atmServiceCategory = nrtVariableBitRate
   peakCellRate  = 450 cells
   sustainedCellRate= 210 cells
   maximumBurstSize= 60 cells
   retryLimit    = 0
   localAddress  = 45613512123400002F000000010020480D527002
   remoteVpiVci  = 7.2
   addressToCall = 45613512123400002F000000010020480D008D00
```

**b** type:

**d -p -no nsta/* vgs ipmcon spvcap**

*The following list shows information for the IPmcon in slot 7. The actual command output lists information for all IPmcon sub-components of the NSTA VGS.*

```
Nsta/ 7 VGS IpMcon SpvcAp
   atmServiceCategory = rtVariableBitRate
   peakCellRate       = 336000 cell/s
   sustainedCellRate  = 336000 cell/s
   maximumBurstSize   = 1 cells
   retryLimit    = 0
   localAddress  = 45613512123400002F000000010020480D517000
   remoteVpiVci  = 7.10
   addressToCall = 45613512123400002F000000010020480D008D00
```

**11** Confirm that the VSP VGS **addressToCall** (ATMIF UNI address) for **Ctrl/mediaGateway**, **Ctrl/signaling Gateway**, and **IpMcon** are identical.

***Note:*** If they are not identical, contact your next level of support.

**12** Check the ATMIF UNI addresses provisioned as primary and alternate by typing:

**l atmif/* uni addr/***

*A sample of the command output for the ATMIFs present on the PVG shelf follows:*

```
Atmif/141  Uni Addr/45613512123400002F000000010020480D008D00, primary

Atmif/151 Uni Addr/45613512123400002F000000010020480D008D00,alternate
Atmif/151 Uni Addr/45613512123400002F000000010020480D009700,primary
```

***Note:*** *Make sure the ATMIF UNI provisioning reflects a Primary and Alternate configuration for the same address for each VSP (Refer to your engineering guidelines for more information). If they do not match, contact your next level of support.*

***Use the PVG CLI to verify the PVG ATM (software) connection to the Passport 8600s***

**13** Determine which ATMIF the VSP VGS Ctrl/<mg,sg> and IPmcon ATMCON subcomponents point to as follows:

**a** display the VGS Ctrl/<mg,sg> ATMCON subcomponent for all VSPs by typing:

**d nsta/* vgs ctrl/* atmconn**

*A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.*

```
+=====+====+--------------------+------
|Nsta |Ctrl|      nextHop       |state
+=====+====+--------------------+------
|    7|mg  |AtmIf/141 Vcc/7.2 Ep|connec
|    7|sg  |AtmIf/141 Vcc/7.6 Ep|connec
```

***Note:*** *Make sure the AtmIf information for each VSP is identical to the primary interface information listed in* step 12*. If it is not contact your next level of support.*

**b** display the NSTA VGS IPmcon ATMCON subcomponent for the VSPs by typing:

**d nsta/* vgs ipmcon atmcon**

*A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.*

```
+=====+-----------------+-------+--------
| Nsta|     nextHop     |state  |Response
+=====+-----------------+-------+--------
|    7|AtmIf/141 Vcc/7.10|connec |
```

***Note:*** *Make sure the AtmIf information for each VSP is identical to the primary interface information listed in* step 12*. If is not contact your next level of support.*

**14** Check the physical connections between each PVG ATM interface and their related Passport 8600s.

***Note:*** See step 8 for the Passport 8600 local route tables for the VSPs to be offloaded and verify the fiber connectivity between the PVGs and Passport 8600s. Refer to your engineering guidelines for additional information.

***Use the PVG CLI to disable the ATM interface to the Passport 8600 undergoing the software upgrade.***

**15** Select the next step as follows (refer to step 9):

| If all VSP VLANs for Passport 8600 Chassis N are | Do |
|---|---|
| OSPF (see Note) | step 22 |
| LOC | step 16 |

***Note:*** OSPF routing does not require manual maintenance to reduce the risk of call processing outages, as the link redundancy on PVGs fails over nearly immediately.

**16** Disable the ATM interface for each VSP as follows:

**a** identify the ATM interfaces and Sonet layer by typing:

**d -p -no lp/* sonet/* sts/0**

*A sample of the command output for the first Sonet interface on each card follows. The actual command output lists all Sonet interfaces on the PVG.*

```
Lp/14 Sonet/1 Sts/0
   applicationFramername     = Atmif/141
   txPathTrace               = ""
   expectedReceivePathTrace  = ""
   concatNumber              = 0
   customerIdentifier        = 0
   ifAdminStatus             = up
   ifIndex                   = 6
Lp/15 Sonet/1 Sts/0
   applicationFramername     = Atmif/151
   txPathTrace               = ""
   expectedReceivePathTrace  = ""
   concatNumber              = 0
   customerIdentifier        = 0
   ifAdminStatus             = up
   ifIndex                   = 472
```

**b** LOCK all Sonet layer connections related to the ATM ports connected to Passport 8600 Chassis N by typing:

**lock -force lp/<slot> sonet/<sonetif>**

where **<slot>** is the slot number of the Passport 8600, and **<sonetif>** is the Sonet interface on the ATM blade

***Note:*** This command results in Sonet layer ALARMS.

**c** record all locked Sonet interfaces

**17** Confirm the ATM (software) connection switch over is successful as follows:

**a** display the VGS Ctrl/<mg,sg> ATMCON subcomponent for the VSPs by typing:

**d nsta/* vgs ctrl/* atmconn**

*A sample of the command output for the switched ATMCON for the Ctrl/* to the ATMIF in slot 7 follows. This example shows a switchover from Atmlf/141 (see step 13) to Atmlf151.*

```
+=====+====+------------------+------
|Nsta |Ctrl|      nextHop       |state
+=====+====+------------------+------
|    7|mg  |AtmIf/151 Vcc/7.2 Ep|connec
|    7|sg  |AtmIf/151 Vcc/7.6 Ep|connec
```

**b** display the VGS IPmcon ATMCON subcomponent for the VSPs by typing:

**d nsta/* vgs ipmcon atmcon**

*A sample of the command output for the switched ATMCON for the IPmcon in slot 7 follows. This example shows a switchover from Atmlf/141 (see step 13) to Atmlf/151.*

```
+=====+------------------+------+------
|Nsta |      nextHop       |state |Response
+=====+------------------+------+------
|    7|AtmIf/151 Vcc/7.10  |connec|
```

***Use the Passport 8600 CLI to verify the IP route table for the offloaded VSP VLANs***

**18** Display the routing table for both Passport 8600s by typing:

**sho ip route info ip x.y.z**

where x.y.z is the IP Net address (see step 9)

***Note:*** The routing information under the PROT column heading should indicate OSPF for all VSP VLANs on Passport 8600 Chassis N.

**19** Select the next step as follows:

| If all VSPs are: | Do |
|---|---|
| not switched over (incomplete) | step 16 |
| switched over (complete) | step 20 |

***Use the PVG CLI to re-enable all disabled ATM ports***

**20** Unlock all Sonet ports locked at step 16 by typing:

**unlock lp/<slot> sonet/<sonetif>**

where **<slot>** is the slot number of the Passport 8600, and **<sonetif>** is the is the Sonet interface on the ATM blade

Or unlock a four-port GE card by typing:

**unlock lp/<slot> Ethernet /<port>**

where **<port>** is the port number

***Use the Passport 8600 CLIs to check the IP route tables***

**21** Make sure all VSP VLANs remain OSPF on Passport 8600 Chassis N and LOC on Passport 8600 Chassis X by typing:

**sho ip route info ip 172.16.201**

*The routing information under the PROT column heading must indicate OSPF for all VSP VLANs on Passport 8600 Chassis N. If it does not, contact your next level of support.*

***Use CS 2000 Management Tools to make the devices that subtend Passport 8600 Chassis N inactive:***

**22** Launch CS 2000 Management Tools from your web browser.

***Note:*** If Java Web Start is not installed on your workstation, you will be prompted to install Java Web Start.

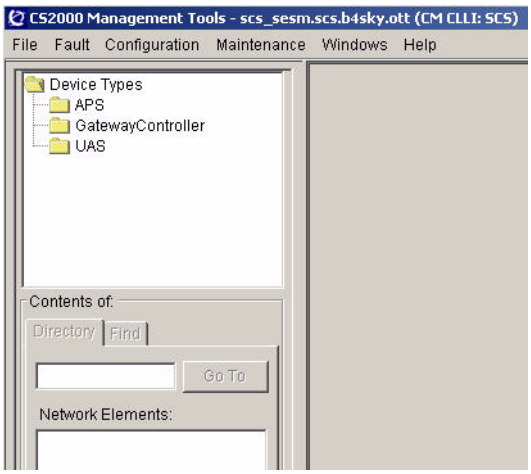
**23** Click on the CS2000 Management Tools link.

*The Login window appears.*

**24** Enter your Login Name. Press the tab key or click in the Password field and enter your Password, which is not echoed for security purposes. Click the Log In button.

***Note:*** Make sure to login with RWA privileges. (See subsection Instructions in *Passport 8600 Software Upgrade for the CS-LAN* for details.)

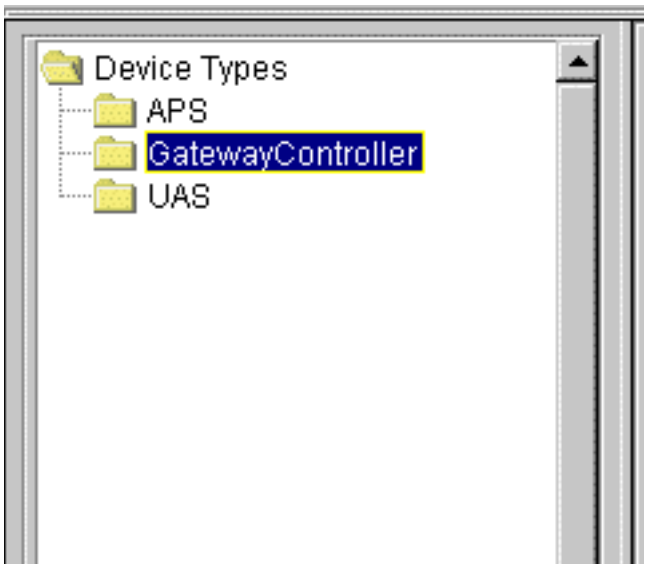
*The CS 2000 Management Tools GUI opens in a new browser window.*




**25** Activate the Maintenance information window for the GWCs as follows:

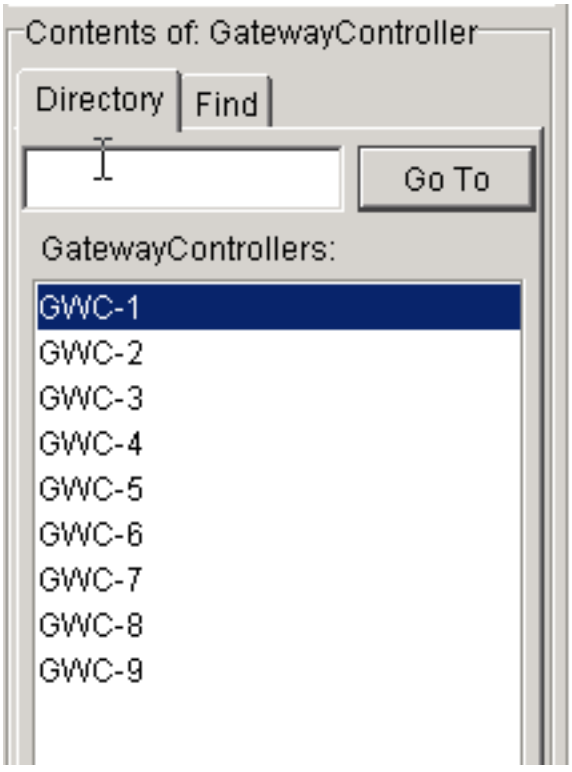
**a** select **GatewayController** from the **Device Types** field of the CS2000 Management Tools GUI

*The **GatewayController** folder in the **Device Types** field is highlighted.*




**b** select the **Directory** tab on the **Contents of: Gateway Controller** field

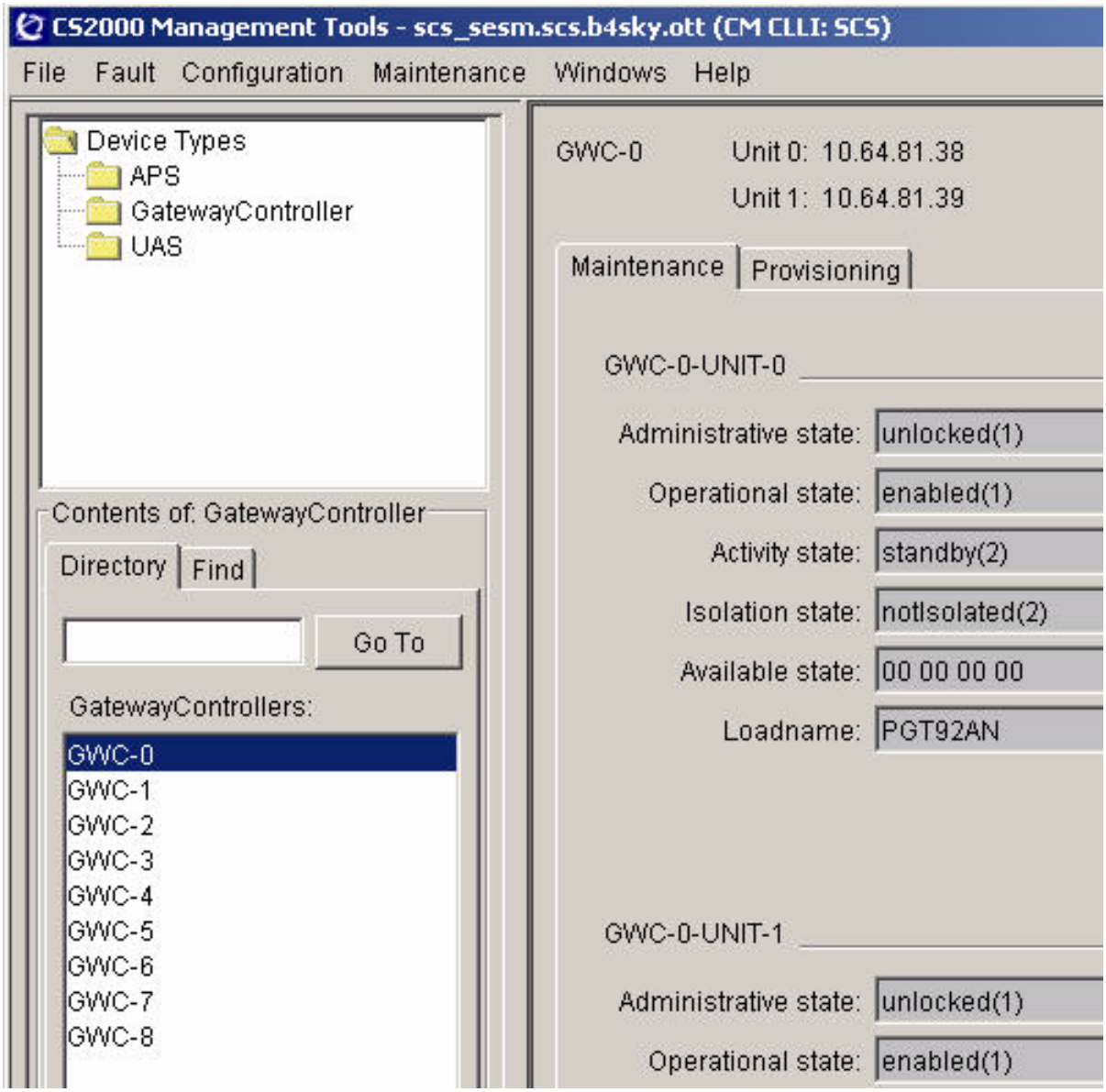
*The list of Gateway Controllers appears.*



**c** select the first GWC in the list displayed in the **Contents of: Gateway Controller** field

*The GWC is highlighted and the related Maintenance or Provisioning information, depending on the active tab, appears in the large right hand field.*

**d** select the **Maintenance** tab to make sure the Maintenance information is active.



**26** Move all traffic onto Passport 8600 Chassis **X** as follows (see note below):

***Note:*** This step makes the following assumptions:

- Unit 0 network elements subtend Passport 8600 Chassis 0
- Unit 1 network elements subtend Passport 8600 Chassis 1
- N = 0 **[X = 1]** for the first iteration of this procedure
- N = 1 **[X = 0]** for the second iteration of this procedure

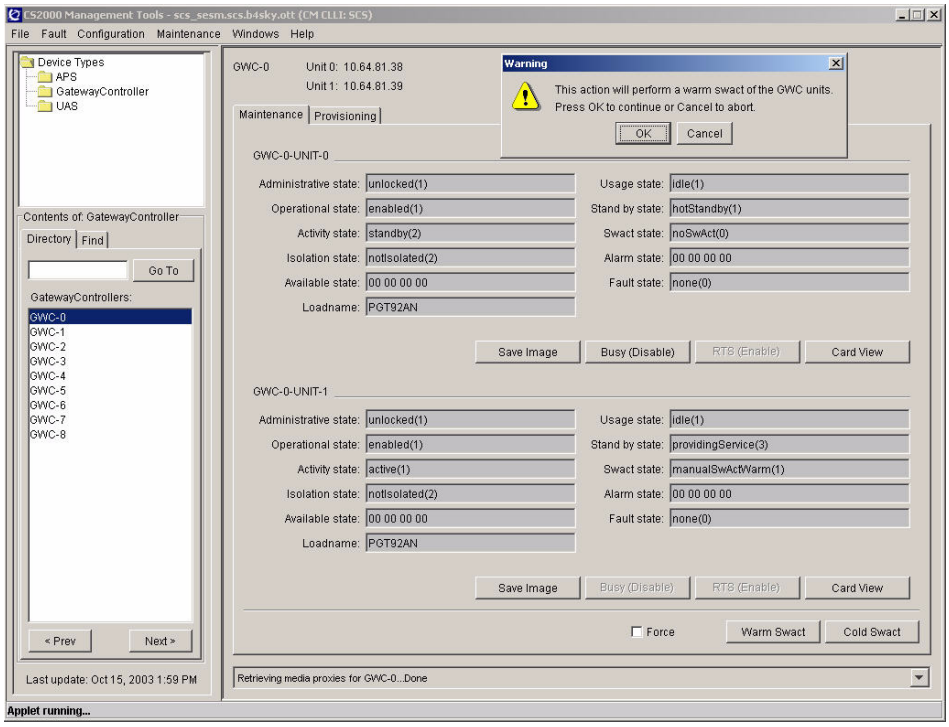
**a** check the **Activity State** field to determine which unit is **active** and which is **standby**

***Note:*** if the **Activity State** field for **GWC-#-Unit-#** is standby, instead of **inactive,** go to sub-step f

**b** press **WarmSwact**

*A warning window appears.*

***Press OK to continue or Cancel to abort.***




**c** press OK and wait for the activity change to complete

*The selected GWC undergoes a change of activity. The change of activity can take a minute or two.*

**d** Select the next step as follows.

| If the GWC software release is | Do |
|---|---|
| from lower than SN06 | step 26e |
| from SN06 or greater | step 26f |

**e** press **Busy (Disable)** button to manually busy the selected inactive GWC unit (the button is located at the bottom of the **Maintenance** information window).

***Note:*** A warning message may appear for GWC Units provisioned with MG9Ks that are set up with the ABI option. Check the Force option and re-press the **Busy (Disable)** button to complete this sub-step.

*The selected inactive unit of the GWC is set to the manually busy state.*

**f** select the next GWC in the **Contents of: Gateway Controller** list and repeat these substeps until the **Activity State** field for **Unit: N Status** is **inactive** for all GWCs in the list.

**27** Select the next step as follows:

| If the Communication Server uses: | Do |
|---|---|
| an XA-Core | step 28 |
| a Compact chassis | step 30 |

***Use the XA-Core MAP terminal to disable the Ethernet link with Passport Chassis N***

**28** Access the ETHR level of the MAP display by typing:

**>MAPCI;MTC;XAC;ETHR**

**29** Refer to the tables below and disable the Ethernet link between the XA-Core and Passport 8600 Chassis N by doing either sub-step a or sub-step b as appropriate.

***Note:*** Refer to the figures supporting step 35 and step 37 in Upgrading Passport 8600 software for the CS-LAN for more information.

**a** if the XA-Core uses HIOPs or HCMICs, type (otherwise do sub-step b):

**bsy <slot> r link force**



| HIOPs/HCMICs | N = 0 | N = 1 |
|---|---|---|
| **<slot>** | 5 | 14 |

go to step 30

**b** if the XA-Core uses IOPs with ETHR packlets, type:



**bsy <slot1> r l link force**

wait for the command to complete then type:

**bsy <slot2> r l link force**

| IOP with ETHRs | N = 0 | N = 1 |
|---|---|---|
| **<slot1>** | 5 | 6 |
| **<slot2>** | 13 | 14 |

**30** Select the next step as follows.

| If the GWC software release is | Do |
|---|---|
| from lower than SN06 | step 31 |
| from SN06 or greater | step 32d |

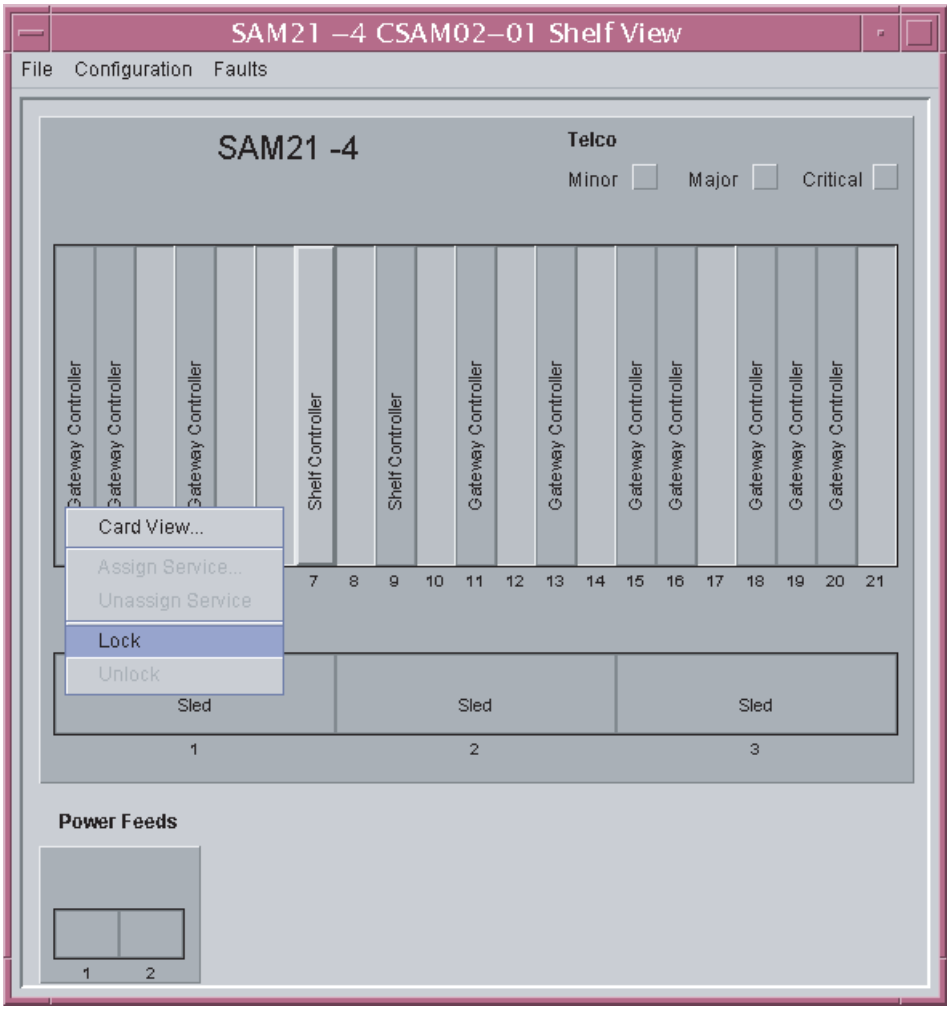
***Use the SAM21 Element Manager to lock the inactive GWCs:***

**31** Launch the SAM21EM client.

*The SAM21 EM GUI appears.*

**32** Lock the inactive GWCs as follows:

**a** from the SAM21 EM shelf view, right click on each **standby** Gateway Controller Unit (see step 26a) in turn




**b** select **Lock** from the drop-down menu that appears.

*This sets the **standby** GWC Units to Locked.*

***Note:** If the SAM21 EM displays a warning message stating the GWC Unit is in service, abort the lock, go to step 26, and make sure the GWC Unit is inactive. If the warning persists contact your next level of support.*

**c** repeat sub-step a and sub-step b until all **standby** Gateway Controller Units are locked.

**d** select the next step as follows:

| If you have | Do |
|---|---|
| a 3PC with a USP Compact | step 33 |
| a 3PC with a standard USP | step 50 |
| an XA-Core | step 58 |

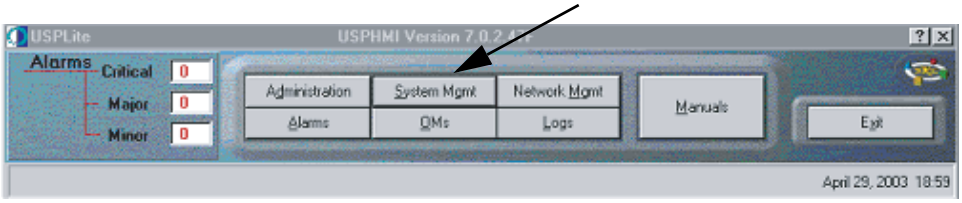
***Use the USP Compact (USPc) GUI to lock the slave USPc blade:***

**33** Refer to your network diagram and determine the USPc blade to Passport 8600 connectivity as follows:

***Note:*** The USPc slave blade must connect to Chassis N of the Passport 8600, master blade to Chassis X (see step 34).

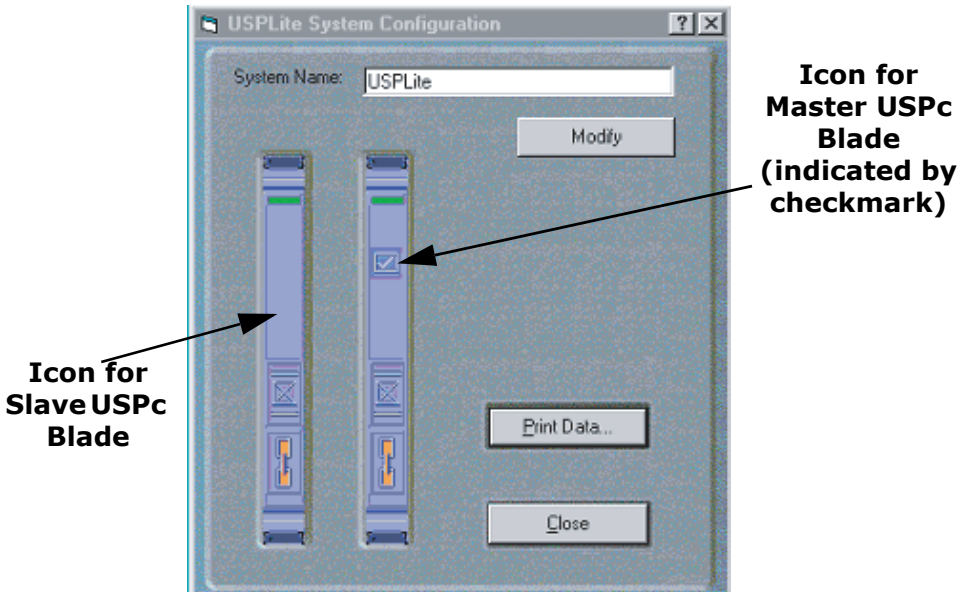
**a** launch the USPc GUI.

**System Management Button**




**b** click the System Management button on the USPc GUI Main Toolbar to start the System Configuration GUI

*The System Configuration window appears.*



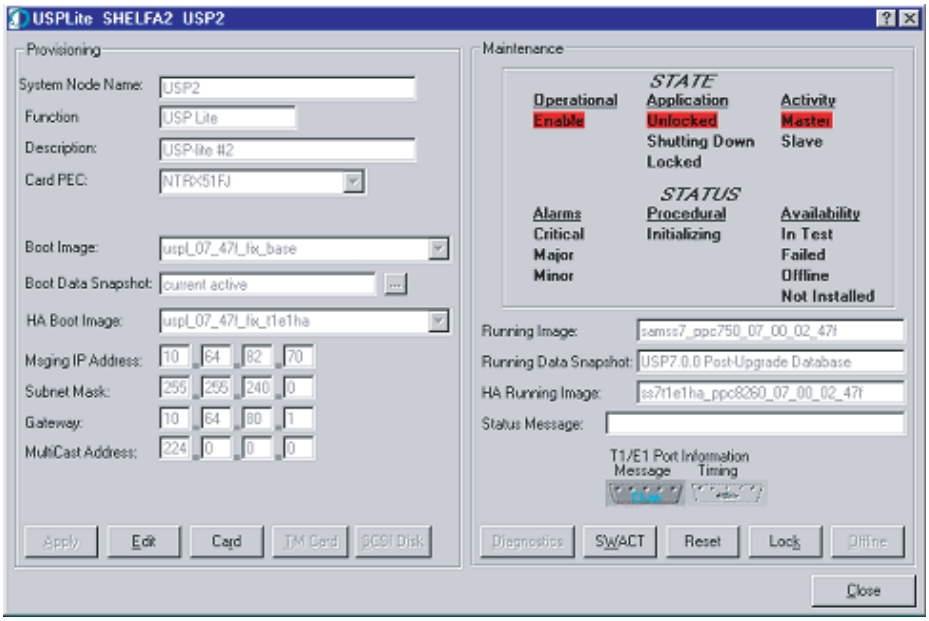

**c** Determine the master / slave status for each USPc blade icon in the System Configuration window.

***Note:*** Both USPc blades carry traffic and are inservice. The blade icon with a checkmark identifies the master USPc. The icon with no checkmark identifies the slave USPc.

**34** Make slave USPc blade subtend Passport 8600 Chassis N as follows:

**a** click on the USPc blade icon connected to the Passport 8600 Chassis N

*The GUI for the slave USPc Shelf appears.*

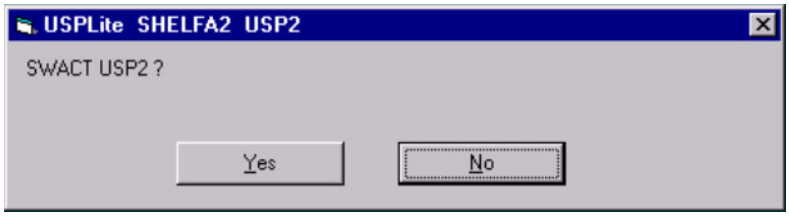



**b** check the *STATE* activity information for the slave USPc blade and continue as follows:

| If the slave USPc blade STATE Activity is | Do |
|---|---|
| Master | step 35 |
| Slave | step 37 |

**35** Click the SWACT button to change the USPc blade *STATE* Activity to **Slave**.

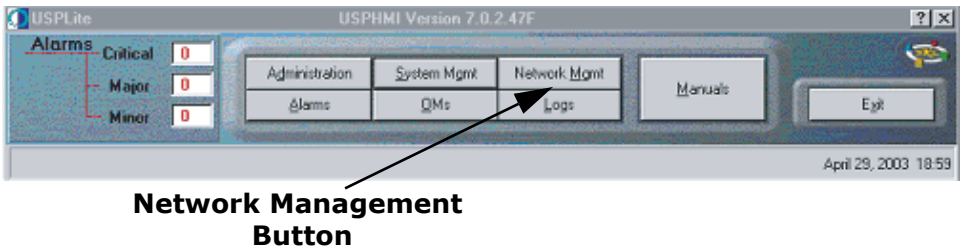
*Press Yes in the SWACT confirmation window to continue*



**36** Go to step 34.

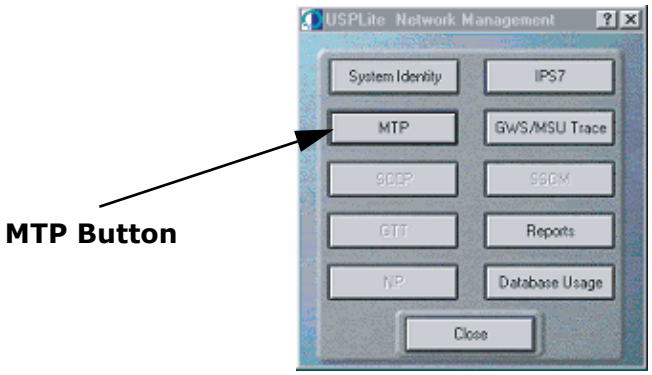
***Note:*** Return to step 34 to confirm the change in *STATE* Activity to **Slave**. If the *STATE* Activity did not change and you return to this step in the same iteration (same value for N), contact your next level of support

**37** Click the Network Management button on the USPc GUI Main Toolbar.



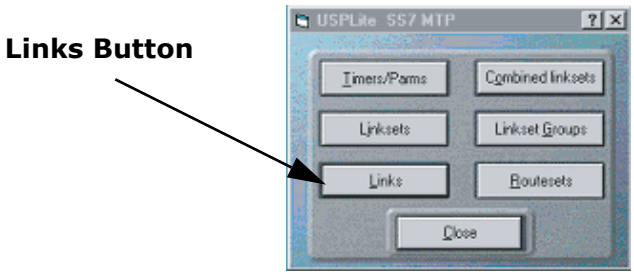

*The Network Configuration window appears.*

**38** Click the MTP button in the Network Management window.




*The SS7 MTP window appears.*

**39** Click the Links button in the SS7 MTP window.

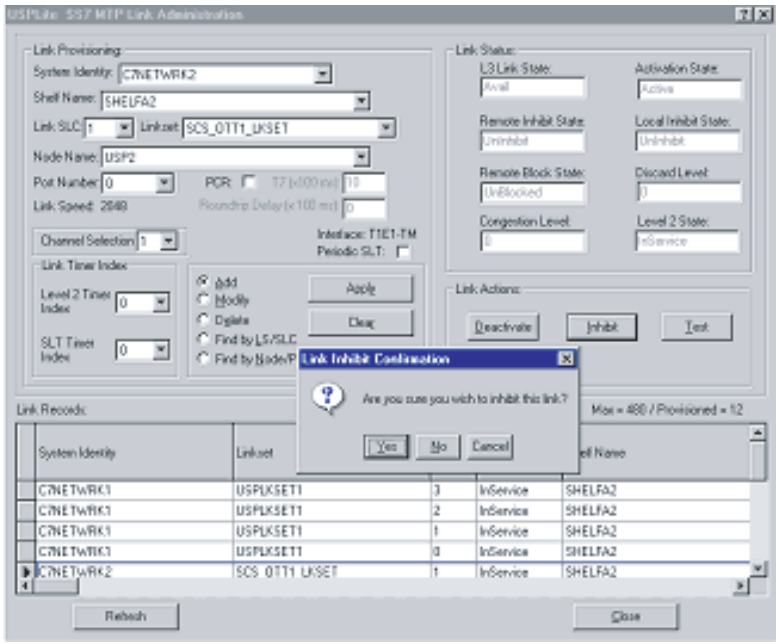


*The Link Management window appears.*

**40** Click the Inhibit button for the slave USPc links.

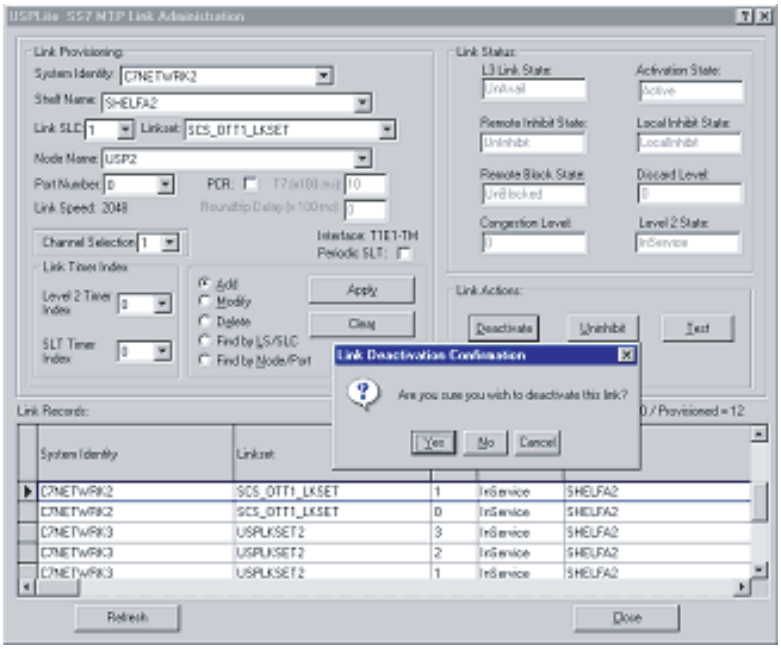
***Note:*** At least one linkset must be available on the master.

*A confirmation window appears. Select OK to continue.*



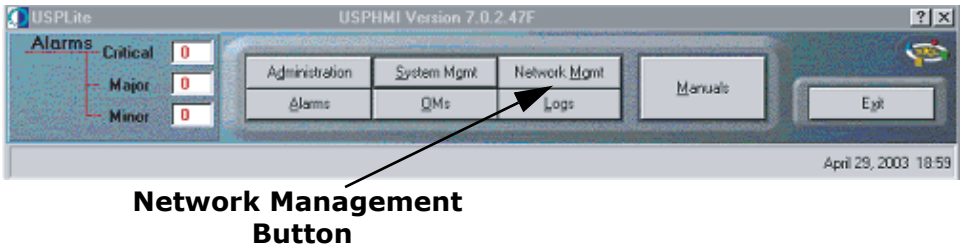

**41** Click the Deactivate button for the slave USPc links.

*A confirmation window appears. Select OK to continue.*

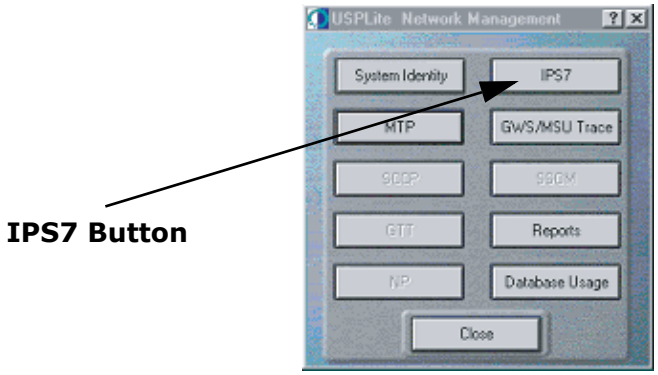



**42** Click the Network Management button on the Main Toolbar.

*The Network Configuration window appears.*




**43** Click the ISP7 button in the Network Management window.



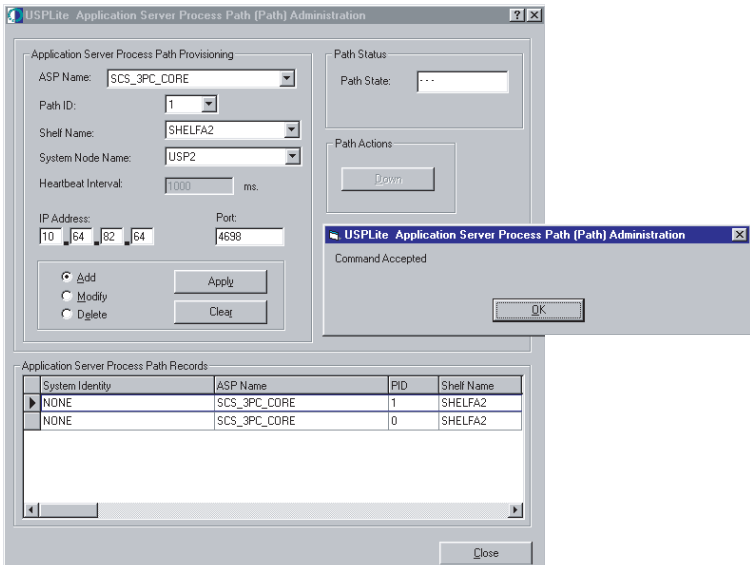
**44** Click on the ASP Paths button in the USP Compact ISP7 window.

*The USP Compact Application Server Process Path window appears.*

**45** Click the Path Actions button for all Application Server Process (ASP) paths on the slave USPc.

***Note:*** At least one ASP path must be available on the master.

*Click OK in the Path Deactivation confirmation window to continue.*

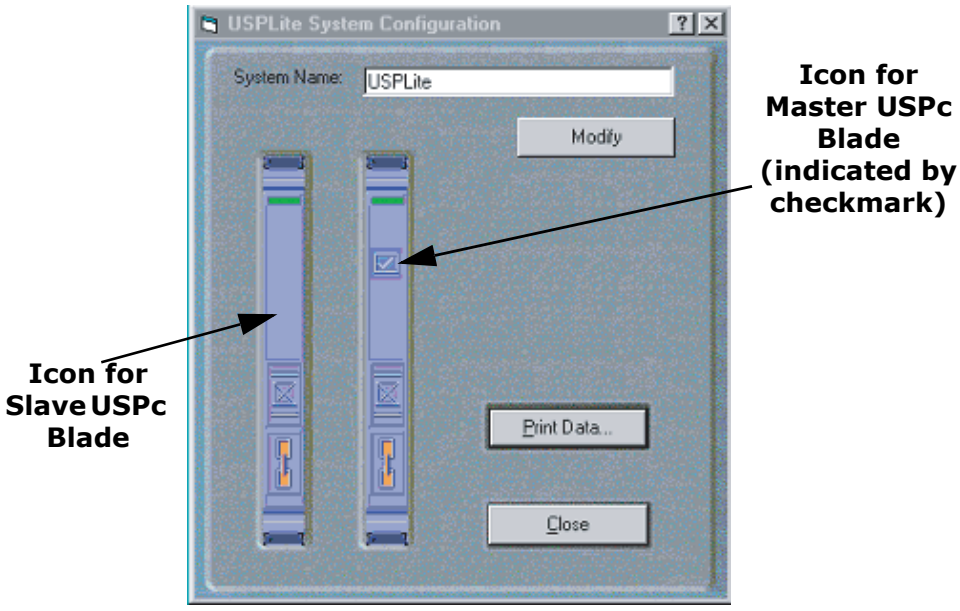



**46** Click the System Management button on the USPc GUI Main Toolbar.

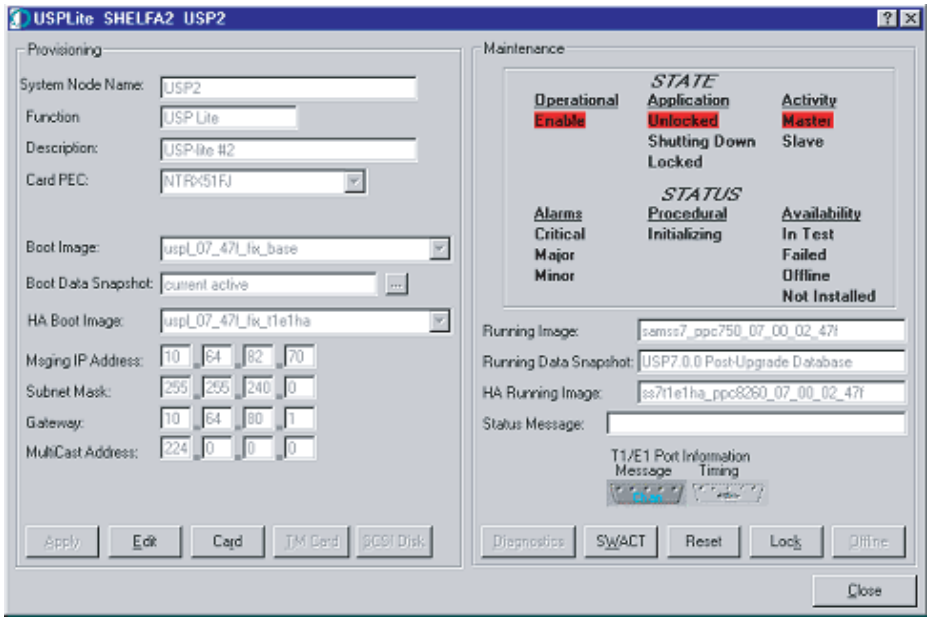
*The System Configuration window appears.*

**47** Click on the slave USPc blade icon to start the GUI for Shelf management.

***Note:*** The blade icon with no checkmark identifies the slave USPc (the blade icon with a checkmark is the master USPc).




*The GUI for the slave USPc Shelf appears.*




**48** Click Lock to manually busy the slave USPc blade.

*A confirmation window appears. Select OK to continue.*

***Use the SAM21 EM to lock the inactive USPc blade and disable the USPc GUI:***

**49** Lock the inactive USPc blade (disable the USPc GUI) as follows:

**a** activate the GUI for CALL-AGENT-N.

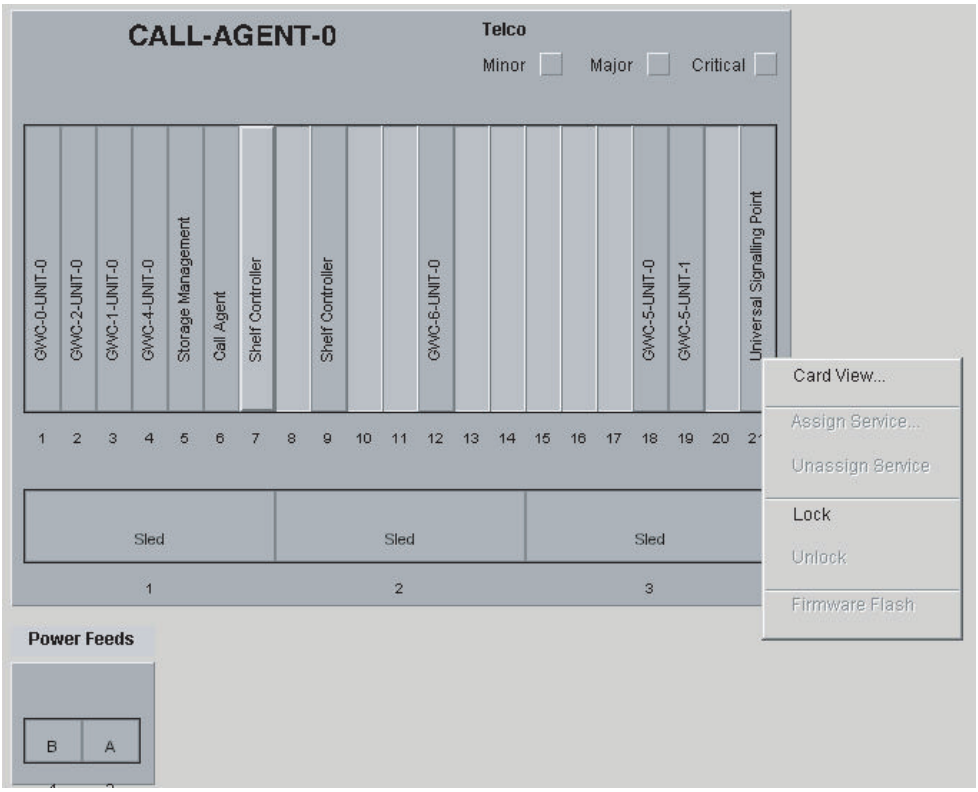
*The GUI for CALL-AGENT-N appears.*

***Note 1:*** *The Universal Signaling Point blade icon must not appear to be raised. A raised icon indicates the blade is active. If the icon appears to be raised consider the recommendation (unit 0s subtend Passport 8600 Chassis 0, and unit 1s subtend Chassis 1).*

***Note 2:*** *To verify that the Universal Signaling Point blade on the GUI for CALL-AGENT-N is inactive, right-click on the blade icon and select* ***Card View****. From the card view* ***Provisioning*** *tab confirm the status is inactive.*

**b** right-click the Universal Signaling Point icon

*A sub-window appears with the* ***Card View*** *and* ***Lock*** *selections enabled.*




**c** click the **Lock** option

***Before rebooting the Passport 8600 that connects the SOS to one of the STORM disks***

**50** Select the next step as follows

| If | Do |
|---|---|
| the volumes on any STORM disk (for example, sd01) are actively mounted in DIRP | step 51 |
| the volumes on the STORM disk are not actively mounted in DIRP, or use a STORM IA configuration | step 58 |

***Note 1:*** Loss of network connectivity between SOS, the call processing application, and the active STORM disk can cause some or all DIRP volumes to be marked “INERROR,” resulting in permanent loss of data.

***Note 2:*** Refer to your network diagram and determine the STORM blade to Passport 8600 connectivity as follows.

Volumes prefixed with sd00 reside on STORM device 0, which must be connected to Passport 8600 Chassis X. Volumes prefixed with sd01 reside on STORM device 1, which must be connected to Passport 8600 Chassis N. Verify this setup in your CS 2000 - Compact. Adjust this procedure, if necessary.

For the first iteration (where N=0), all actions are performed for volumes prefixed with sd01. For the second iteration (where N=1), all actions are performed for volumes prefixed with sd00.

**51** From the Core MAP command line, list all available DIRP subsystems (field SYSSNAME in table DIRPSSYS) for the Core.

**>table dirpssys; lis all**

**52** Access the DIRP level in SOS by typing:

**>mapci nodisp;mtc;iod;dirp**

**53** Query all volumes associated with the subsystem.

**>query <subsystem> all**

where:
<subsystem> is from the list of available subsystems executed in step 51.

*The following figure shows an example of this command for the dlog subsystem with an active file highlighted.*

```
>query dlog all
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
DLOG      1     1       3      7  NONE     ***YES***

REGULAR
FILE(S)   STATE VOLUME   RECCOUNT BLOCK E  V V_B VLID FNUM FRN#
ACTIVE    AVAIL SD01DLG1         1     1 0 71 NO  8448 000D 1014
STANDBY1 AVAIL SD00DLG1          0     0 0 70 NO  8408 0015 3012

PARALLEL
FILE               STATE VOLUME   BLOCK E  V V_B VLID FNUM FRN#
                    NONE

REGULAR VOLUME(S)
VOL# VOLNAME  STATE          IOC CRD PORT VOL FSEG ROOM VLID FILES
  70 SD00DLG1 READY          N/A N/A N/A    8   10   11 8408 S1
  71 SD01DLG1 READY          N/A N/A N/A    8  112  116 8448 A

REGULAR SPACE
VOL# VOLNAME  STATE          SEGS   EXP UNEXP TOTAL
  70 SD00DLG1 READY            10     1     0    11
  71 SD01DLG1 READY           112     4     0   116
```

**54** Only rotate the active volume for each subsystem if it is located on a STORM blade connected to the router being upgraded for this iteration. Manually rotate all subsystems until the active files reside on STORM volumes connected to the Passport 8600 chassis that is not to be upgraded for this iteration.

***Note:*** To minimize the risk, rotate and demount the AMA subsystem last. Then restore the AMA subsystem first.

**>rotate <subsystem> <variable>**

where:
**<variable>** is regular, paralel, or both (Enter regular to rotate regular volumes. Enter paralel to rotate parallel volumes. Enter both to rotate both volumes.)

***Note:*** Parallel is intentionally misspelled.

*The following figure shows example of input for variable regular.*

```
>rotate dlog REGULAR
ACTIVE FILE WILL BE CLOSED IF POSSIBLE (ROTACLOS).
SENDING REQUEST TO SUBSYSTEM
Please confirm ("YES", "Y", "NO", or "N"):
>y
REQUEST SENT TO SUBSYSTEM, CHECK DIRP LOG FOR DETAILS
```

**55** Repeat step 53 to ensure that all volumes have been successfully rotated.

**56** Demount all DIRP volumes connected to the Passport 8600 chassis that is to be upgraded.

**>dmnt <subsystem> <volume> <variable>**

where:
**<volume>** is the volume on the device (prefixed with sd01 for iteration N=0, and prefixed with sd00 for iteration N=1)

**<variable>** is regular or paralel

***Note 1:*** The **<variable>** parameter is not required when mounting and demounting regular DIRP volumes.

***Note 2:*** Nortel Networks recommends recording all subsystems, volume, and variable information for each volume being demounted in this step.

**57** Busy all STORM volumes connected to the Passport 8600 chassis to be upgraded.

**>diskadm sdXX; bsy all**

where:
XX=01 for iteration N=0
XX=00 for iteration N=1

***Note 1:*** Nortel Networks does not recommend using option bsy all force.

***Note 2:*** Issuing a bsy all command affects all volumes serviced by that STORM blade, not just those used by DIRP.

**58** Select the next step as follows:

| If the CS-LAN is used with: | Do |
|---|---|
| an ATM-based solution | step 59 |
| an IP-based solution | step 61 |

***Use the SAM21 EM to lock the inactive Shelf Controller blade:***

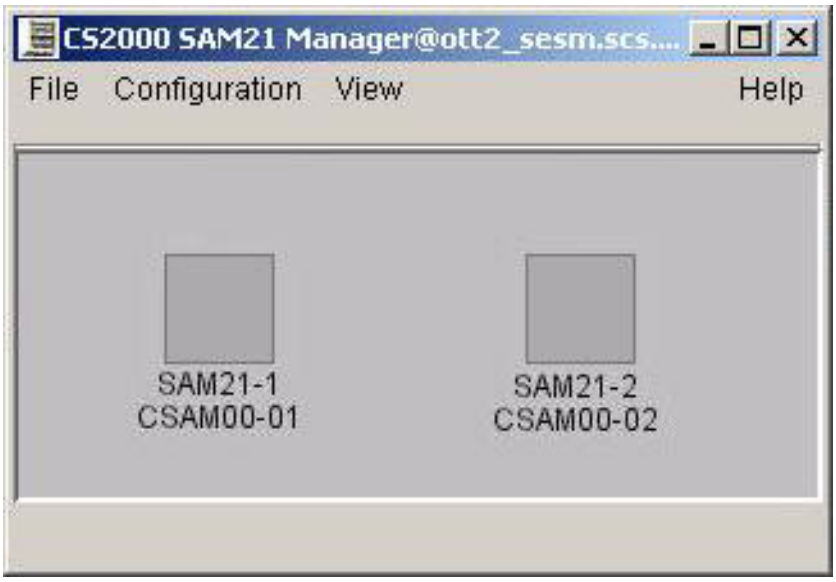
**59** Confirm that Shelf Controller (SC) blade connectivity complies with all topology recommendations.

***Note:*** The recommendation at in Upgrading Passport 8600 software for the CS-LAN requires SC unit 0s (in slot 7) subtend Passport 8600 Chassis 0, and SC unit 1s (in slot 9) subtend Passport 8600 Chassis 1. If the SAM21shelf varies from this recommendation, adjust this procedure accordingly.

**60** Lock the inactive SAM21 SC blade for each SAM21 shelf in turn as follows:

**a** launch the SAM21 EM

*The SAM21 EM GUI appears with the related shelf icons displayed.*

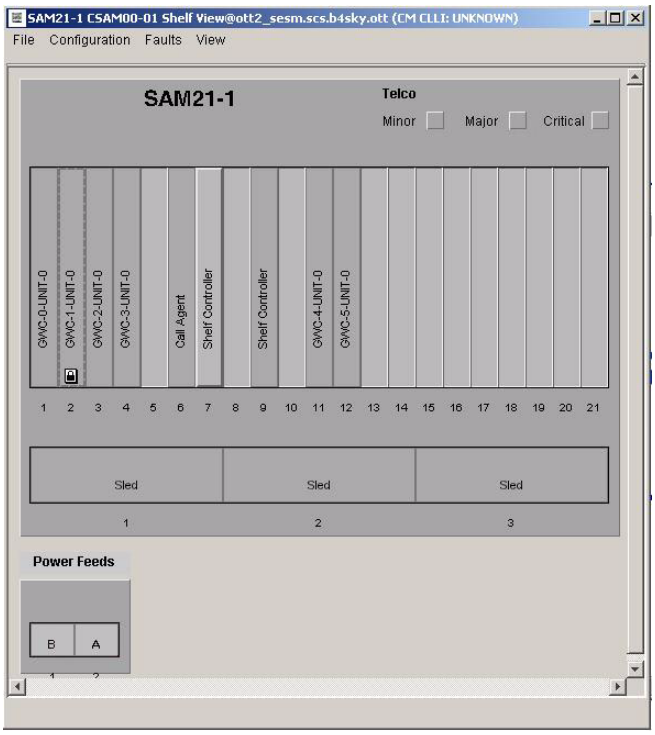



**b** use the cursor to select the shelf icon for the first SAM21 shelf displayed

**Example**
The first shelf in the figure above is SAM21-1 CSAM00-01

**c** double-click the selected shelf icon

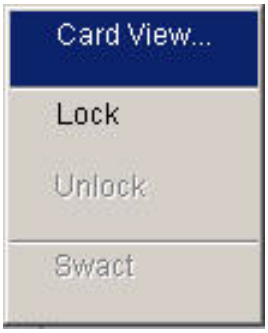
*The SAM21 EM shelf view for the selected shelf appears.*




**d** right-click on the icon for the SC blade associated with the inactive Passport 8600 Chassis

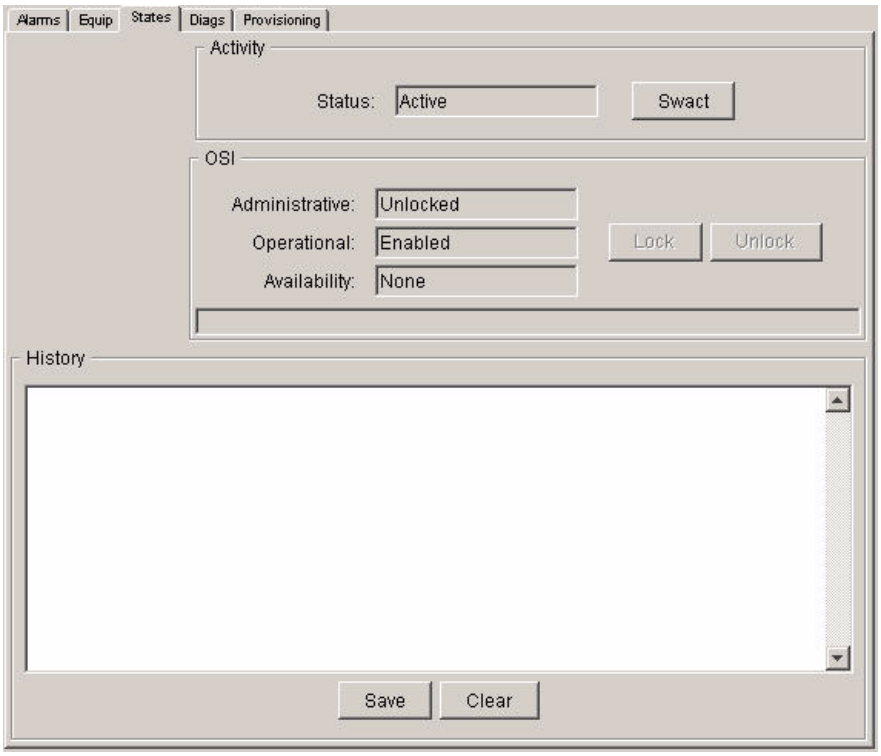
***Note:*** The SC blade in slot 7 subtends Passport 8600 Chassis 0, slot 9 subtends Chassis 1 (see note to step 59)

*A sub-window appears with the **Card View** and **Lock** selections enabled.*




**e** click **Card View**

*The SC Card View appears.*




**f** select the **State** tab and make sure the SC is inactive

*If the SC state is **Active**, press the **SWACT** button to change the activity status to **Inactive**.*

**g** close the **Card View**

*The **Shelf View** reappears.*

**h** right-click on the icon for the inactive SC blade

*A sub-window appears with the **Card View** and **Lock** selections enabled.*

**i** click **Lock**

*The inactive SC blade is locked.*

***Note:** This prevents an automatic change of activity from occurring. An automatic SWACT at this point could cause a system outage.*

**j** close the **Shelf View**

*The SAM21 EM view reappears.*

**k** select the next step as follows

| If the (inactive) SC cards are | Do |
|---|---|
| locked on all SAM21 shelves | step 61 |
| not all locked | select the next SAM21 Shelf and go to sub-step c |

***Note:*** Repeat sub-step c through sub-step j until the inactive SCs are all locked.

***Use the Passport 8600 CLI to make devices subtending Chassis X of Passport 8600 active (Chassis N devices inactive):***

**61** Recheck the address resolution protocol information by typing:

**sho ip arp info**

*The IP ARP file appears. Verify that active units subtend the Passport 8600 Chassis X (inactive units subtend Chassis N)*

***Note 1:*** *For more information IR ARP information, select option Documentation under Passport 8600 Routing Switch on the Nortel Networks website. Or contact your next level of support.*

***Note 2:*** *If any units do not meet this requirement, repeat step 26. If the problem persists, contact your next level of support.*

***Use the Passport 8600 CLI to restore the original software load on Passport 8600 Chassis N:***

**62** Select the next step as follows

| If your CS-LAN: | Do |
|---|---|
| is a dual CPU configuration | step 63 |
| is a single CPU configuration | step 68 |

**63**

**ATTENTION**

Refer to section Text conventions on page 1790 for brief definitions and examples of the software filenames used the following commands.

For a Passport 8600 with a dual-CPU configuration, TFTP the upgrade software to the flash on the master CPU. Then copy it to the standby CPU.

In the following sub-steps, both commands must be executed on the master CPU.

***Note:*** The Passport 8600 automatically copies files to the PCMCIA card using the same name as the current file. Therefore, it is not necessary to enter a new filename for the backup version of this file.

**a** TFTP the new software image file. Type:

**copy /pcmcia/<oldload> /flash/**

**copy peer:/pcmcia/<oldload> peer:/flash/**

where **<oldload>** is the original software image file

**b** TFTP the new boot monitor image file. Type:

**copy /pcmcia/<oldboot> /flash/**

**copy peer:/pcmcia/<oldboot> peer:/flash/**

where **<oldboot>** is the original bootmonitor image file

*The boot flash image and software image is backed up to the PCMCIA card on the Passport 8600 Chassis N.*

***Note 1:*** *If either file transfer fails, verify TFTP server IP address and connectivity with Passport 8600 Chassis N. Confirm Passport 8600 TFTP flag is set to true by typing:*
***config bootconfig flags info***

*If the **tftpd** flag is set to false, reset the flag to true by typing:*
***config bootconfig flags tftpd true***

*Confirm the flag is now set to true, then retry the transfer. If the problem persists, contact your next level of support.*

***Note 2:*** *If the transfer completes but the file is corrupted, verify original file and PCMCIA card and transfer the file again. If the problem persists, contact your next level of support.*

***Note 3:*** *Compare file parameters such as file size to check for possible corruption.*

**c** ***Only*** if Chassis N of Passport 8600 uses an ATM blade, TFTP the ATM Flash image to the Flash card on the Passport 8600 Chassis N by typing (otherwise go to step 64)

**copy /pcmcia/<oldatm> /flash/**

**copy peer:/pcmcia/<oldatm> peer:/flash/**

where **<oldatm>** is the name of the original ATM load file

***Note:*** Notes 1 and 2 from step 63, sub-step b apply.

**d** If the Passport 8600 uses DES, TFTP the file. Type:

**copy /pcmcia/<oldDES> /flash/**

**copy peer:/pcmcia/<oldDES> peer:/flash/**

where **<oldDES>** is the name of the original DES file

**e** If the Passport 8600 uses 3DES, TFTP the file. Type:

**copy /pcmcia/<old3DES> /flash**

**copy peer:/pcmcia/<old3DES> peer:/flash/**

where **<old3DES>** is the name of the original 3DES file

**64** Verify that the software has been copied to the master and standby CPUs.

**a** For the master CPU, type

**dir**

**b** For the standby CPU, at the prompt of the master CPU, type

**peer telnet**

**dir**

**65** Exit the standby CPU.

**exit**

**66** Prepare to boot both CPUs. Select the next sub-step as follows.

| If | Do |
|---|---|
| rolling back to a pre-3.7.0.0 software load | step 66a |
| rolling back to a 3.7.0.0 (or greater) software load | step 66b |

**a**

**WARNING**

Failure to observe this step can result in loss of configuration.

Disable the flag setting before saving the bootconfig file.

**config bootconfig flags ha-cpu false**

**b** **config bootconfig choice primary image-file /flash/<oldload>**

where **<oldload>** is the name of the current software image file

***Note:*** There is a mandatory space between **image-file** and **/flash** in the syntax this sub-step.

**c** save the bootconfig file by typing:

**sav bootconfig**

***Note:*** If the switch response does not show the file being saved to the standby CPU, copy the files to the standby CPU by typing:

**copy /flash/boot.cfg peer:/flash/boot.cfg**

*This prepares Passport 8600 Chassis N to reboot.*

**67**

**WARNING**

When booting the dual CPUs, do not wait for the standby CPU to complete the boot process before booting the master CPU. Waiting results in different images on each CPU. While in the high-availability (HA) mode, booting the master CPU and the standby CPU with different software images can crash the standby CPU.

Boot both CPUs in rapid sequential order, booting the standby CPU first and immediately booting the master CPU next.

**a** Boot the standby CPU. In the standby CPU session, type

**peer telnet**

**boot /flash/<oldboot> [config /pcmcia/<cfgbkup>]**

where **<oldboot>** is the name of the current boot monitor image file

**b**

**ATTENTION**

This command upgrades the primary-image file (including the ATM-image if present) and boot monitor at the same time.

**ATTENTION**

Do not interrupt the reboot process. The CPU card can be damaged if the reboot is interrupted incorrectly.

Immediately boot the master CPU. In the master CPU session, type

**boot /flash/<oldboot> [config /pcmcia/<cfgbkup>]**

Go to step 70.

**68** Prepare to reboot Passport 8600 Chassis N as follows:

**a** only if the original software has already been deleted from the Passport 8600, type:

**copy /pcmcia/<oldload> /flash/**

**b** only if the original boot monitor file has already been deleted from the Passport 8600, type:

**copy /pcmcia/<oldboot> /flash/**

**c** only if an ATM blade exists and the original ATM image file has already been deleted from the Passport 8600, type:

**copy /pcmcia/<oldatm> /flash/**

**d** If the Passport 8600 uses DES, TFTP the file. Type:

**copy /pcmcia/<oldDES> /flash/**

where **<oldDES>** is the name of the original DES file

**e** if the Passport 8600 uses 3DES, TFTP the file. Type:

**copy /pcmcia/<old3DES> /flash**

where **<old3DES>** is the name of the original 3DES file

**f** set the primary image file to the saved load by typing:

**config bootconfig choice primary image-file /flash/<oldload>**

***Note:*** There is a mandatory space between **image-file** and **/flash** in the syntax this sub-step.

**g** set the primary config file to the saved configuration by typing:

**config bootconfig choice primary config-file /pcmcia/<cfgbkup>**

***Note:*** Configure the primary config file to ensure that the original configuration was not changed during the upgrade process.

**h** save the bootconfig file by typing:

**sav bootconfig**



**69** Roll back Passport 8600 Chassis N software upgrade by typing:

**boot /flash/<oldboot>**

**ATTENTION**

This command automatically upgrades the primary-image file (including the ATM-image if present) and boot monitor at the same time.

*The Passport 8600 reboots loading the original software image. The reboot takes approximately 15 to 20 seconds. Serial connectivity is maintained during the reboot.*

***Note:*** *If the reboot is unsuccessful make sure the path is correct and try again. If the problem persists contact your next level of support.*

**70** Select the next step as follows.

| If | Do |
|---|---|
| the volumes on any STORM disk (for example, sd01) were mounted in DIRP | step 71 |
| the volumes on the STORM disk are not actively mounted in DIRP, or use a STORM IA configuration | step 73 |
| using an XA-Core shelf | step 73 |

**71** At the Core, return to service all disk volumes connected to the Passport 8600 chassis that was upgraded.

**>diskadm sdXX; rts all**

where:
XX=01 for iteration N=0
XX=00 for iteration N=1

**72** Individually remount all volumes in DIRP. (Ensure you are at the nodisp;mtc;iod;dirp level of the MAPCI for this step.)

**>mnt <subsystem> <volume> <variable>**

***Note 1:*** The **<variable>** parameter is not required when mounting and demounting regular DIRP volumes.

***Note 2:*** Nortel Networks recommends recording all subsystems, volume, and variable information for each volume demounted in this step.

***Use the Passport 8600 CLI to verify all hardware and software on the master Passport 8600:***

**73** Confirm master Passport 8600 is operating correctly as follows:

***Note:*** Refer to step 3 of Upgrading Passport 8600 software for the CS-LAN for more information

**a** check the log file by typing:

**sho log file**

*Review the info and correct any errors or problems reported.*

**b** check the configuration by typing:

**sho config**

*Output similar to the following appears.*

```
#<output date and time info>
#boxtype : Passport-8010
#software version : W.X.Y.Z
#monitor version : W.X.Y.Z/NNN
#<output continues>
```

*where W.X.Y.Z provides release information and the NNN can be ignored.*

*Review the configuration file (showing network topology and configuration) and correct any incorrect configurations.*

***Note:*** Software version is the load or image version. Monitor version is the bootflash version.

**c** check the address resolution protocol information by typing:

**sho ip arp info**

*Review the IP ARP file and correct any MAC address problems.*

***Use the SAM21 EM to unlock the inactive GWCs and SCs:***

**74** Launch the SAM21EM client.

*The SAM21 EM GUI appears.*

**75** Select the next step as follows:

| If the GWC software release is | Do |
|---|---|
| from lower than SN06 | step 76 |
| from SN06 or greater | step 77 |

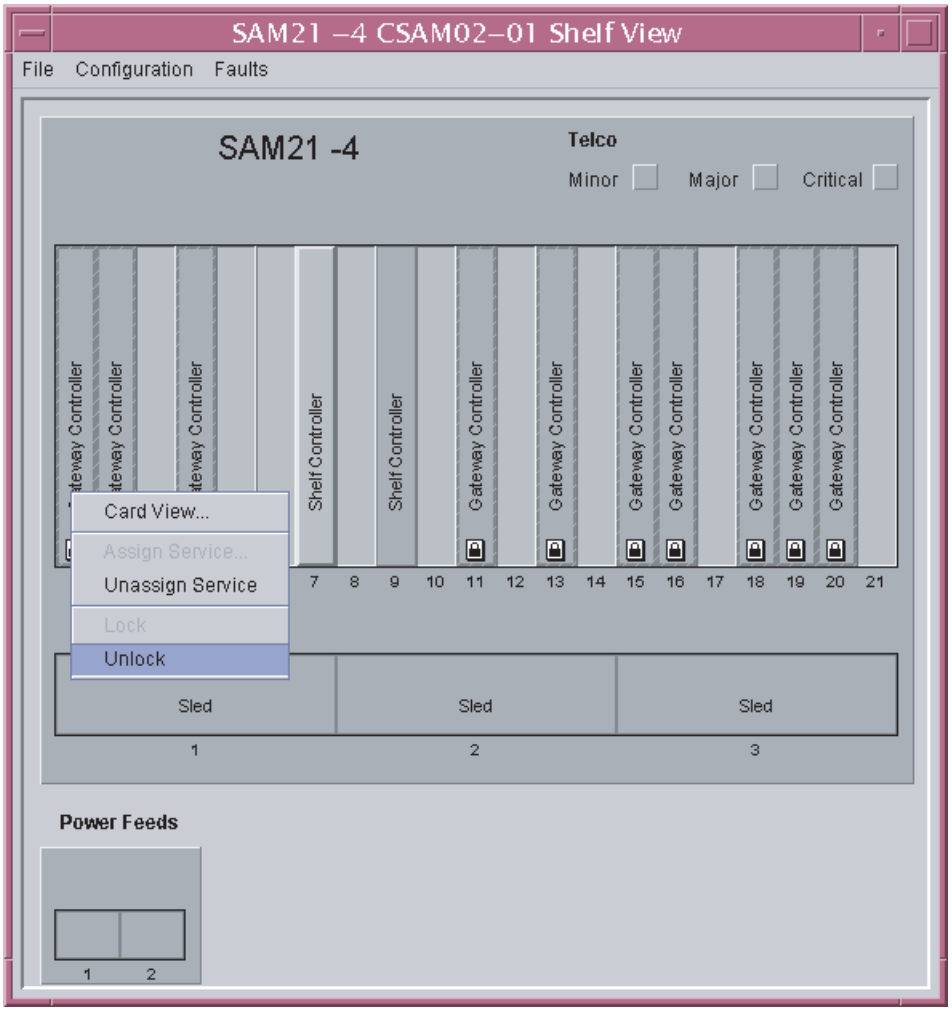
**76** Unlock each locked Gateway Controller unit as follows:

**a** right click on a locked Gateway Controller Unit

**b** select **Unlock** from the drop-down menu that appears

**c** repeat sub-step a and sub-step b until all units are unlocked.

***Note:*** A padlock icon identifies locked GWC units.



**77** Select the next step as follows:

| If rolling back with an | Do |
|---|---|
| ATM solution | step 78 |
| IP solution | step 80 |

***Use the SAM21 Element Manager to unlock the inactive SCs:***

**78** Launch the SAM21 Element Manager.

*The SAM21 EM GUI appears. Padlock icons identify locked SC blades.*

**79** From the SAM21 EM shelf view, right click on each of the locked SC blades in turn and do the following:

**a** Select **Unlock** from the drop-down menu that appears.

**b** Repeat sub-step a until all locked SC blades are unlocked.

**80** Select the next step as follows:

| If the USP Compact is: | Do |
|---|---|
| used | step 81 |
| not used | step 86 |

***Use the SAM21 EM to perform the following additional steps (for USP Compact only):***

**81** Unlock the slave USPc.

***Note:*** Unlocking the slave USPc from the SAM21 EM enables the USPc GUI.

***Use the USPc GUI to perform the following additional steps (for USP Compact only):***

**82** Unlock the slave USPc as follows:

**a** from the main menu, select System Management

**b** click on the USPc circuit card (blade)

**c** click Unlock

**83** Activate all paths on the slave USPc.

**84** Activate all links on the slave USPc.

**85** Uninhibit all links on the slave USPc.

**86** Select the next step as follows:

| If the Communication Server uses: | Do |
|---|---|
| an XA-Core | step 87 |
| a Compact chassis | step 89 |

***Use the XA-Core MAP terminal to enable the Ethernet link with Passport Chassis N***

**87** Access the ETHR level of the MAP display by typing:

**MAPCI;XAC;MTC;ETHR**

**88** Refer to the tables below and enable the Ethernet link between the XA-Core and Passport 8600 Chassis N by doing either sub-step a or sub-step b as appropriate.

**a** if the XA-Core uses HIOPs or HCMICs, type (otherwise do sub-step b):



**rts <slot> r link**

| HIOPs/HCMICs | N = 0 | N = 1 |
|---|---|---|
| **<slot>** | 5 | 14 |

go to step 89

**b** if the XA-Core uses IOPs with ETHR packlets, type:



**rts <slot1> r l link**

wait for the command to complete then type:

**rts <slot2> r l link**

| IOP with ETHRs | N = 0 | N = 1 |
|---|---|---|
| **<slot1>** | 5 | 6 |
| **<slot2>** | 13 | 14 |

***Use the Passport 8600 CLI to reset the VRRP priority settings and OSPF cost metrics and swap the Passport 8600 master/slave status:***

**89** Make sure Passport 8600 Chassis N is in service as follows:

**a** check the IP route information by typing:

**sho ip route info**

*The IP route information file appears. Review the file and verify that the route information is correct.*

**b** check the IP VRRP information by typing:

**sho ip vrrp info**

*The IP vrrp information file appears. Review the file and verify that the information is correct.*

**90** Reset the VRRP priority and OSPF metrics for Chassis N as follows:

**a** type:

**config vlan <vid> ip vrrp <vrid> prio <setting>**

***Note:*** See step 2 for <vid> and <vrid> values for Chassis N. The **PRIO** value for the Chassis N <setting> is also recorded step 3.

*The VRRP priority metric is reset to its operational value.*

**b** type:

**config vlan <vid> ip ospf metric <value>**

***Note:*** See step 3 for the OSPF metric for <value>.

*The OSPF metrics reset to their original value.*

**c** Save the new Passport 8600 configuration by typing:

**sav config**

*This updates the new Passport 8600 configuration so that VRRP settings are maintained after any subsequent reboot.*

**91** Swap the Passport 8600 master/slave status on Chassis X by typing:

**config vlan <vid> ip vrrp <vrid> priority <prio>**

where **<prio>** is priority information that determines which Passport 8600 is master and which one is slave.

***Note 1:*** Refer to step 2 for the applicable **<vid>**, **<vrid>**, and **<prio>** values.

***Note 2:*** The Passport 8600 **<prio>** is higher for the master Passport 8600 chassis than for slave.

*The master Passport 8600 becomes the new slave Passport 8600 (the old slave Passport 8600 becomes the new master).*

**92** Increment the iteration index (N = N+1) and select the next step as follows:

| If | Do |
|---|---|
| N = 1 | step 3(second pass) |
| N = 2 | step 93 |

***Note:*** In the second iteration (where N = 1), when repeating step 3 through step 92, use Chassis X in place of Chassis N. Passport 8600 Chassis 1 (identified as Chassis N) is the slave and Passport 8600 Chassis 0 (identified as Chassis X) is the master.

**93** The procedure is complete.

# Downgrading the CS 2000 Management Tools software

This section provides the information required to roll back a software upgrade and revert to the previous release of the software. Follow the link associated with the release you are downgrading to.

- Downgrading to (I)SN05 on page 1842
- Downgrading to (I)SN06 on page 1844
- Downgrading to (I)SN06.2 on page 1845

***Note:*** It is highly recommended that all console and telnet sessions used during rollbacks, be logged to a file to assist in any necessary troubleshooting.

## Downgrading to (I)SN05

Downgrading to (I)SN05 involves a rollback of the CS 2000 SAM21 Manager software, if present, to the CS 2000 Core Manager, and a rollback of the SSPFS and CS 2000 Management Tools software.

### Rollback of the CS 2000 SAM21 Manager to (I)SN05

Use the table below as a checklist during the rollback of the CS 2000 SAM21 Manager to (I)SN05. Place a check (√) in the √column as you complete each procedure.

**Downgrading the CS 2000 SAM21 Manager to (I)SN05**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Boot the core manager from the (I)SN05 backup tape. | | Refer to procedure “Performing a full restore of the software from S-tape” in the CS 2000 Core Manager Fault document, NN10082-911. |
| 2 | Migrate the SAM21 shelves back to the CS 2000 SAM21 Manager on the core manager. | | Refer to procedure Migrating the SAM21 network elements back to the CS 2000 SAM21 Manager on the core manager on page 1848 in this document. |

### Downgrading the CS 2000 SAM21 Manager to (I)SN05

| | Activities | √ | Procedures |
|---|---|---|---|
| 3 | Downgrade the shelf controllers to the (I)SN05 release for all shelves. | | Contact your next level of support if you already upgraded both SAM21 shelf controllers to (I)SN07 and want to downgrade them to (I)SN05.<br><br>or<br><br>Refer to procedure Rollback software on the SAM21 Shelf Controller on page 1853 in this document if you only upgraded one SAM21 shelf controller to (I)SN07 and want to downgrade it to (I)SN05. |
| 4 | Migrate the SAM21 Manager data back to the core manager. | | Refer to procedure Performing a rollback of the CS 2000 SAM21 Manager on page 1856 in this document. |

## Rollback of the SSPFS and CS 2000 Management Tools software to (I)SN05

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN05. Place a check (√) in the √column as you complete each procedure.

### Downgrading the SSPFS and CS 2000 Management Tools software to (I)SN05

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Install the previous version of SSPFS on the CS 2000 Management Tools server. | | Refer to procedure Reverting to the previous release of the SSPFS software on page 1858 in this document. |
| 2 | Restore the file systems from backup media. | | Refer to procedures Restoring root file systems - pre-(I)SN06.2 on page 1865 and Restoring non-root file systems on an SSPFS-based server pre-(I)SN06.2 on page 1868 in this document. |

### Downgrading the SSPFS and CS 2000 Management Tools software to (I)SN05

| | Activities | √ | Procedures |
|---|---|---|---|
| 3 | Restore the Oracle data from backup media. | | Refer to procedure Restoring application data to the Oracle database on an SSPFS-based server pre-(I)SN06.2 on page 1874 in this document. |
| 4 | Clear the Java ™ Web Start (JWS) cache on the client workstation. | | Refer to procedure Clearing the JWS cache on a client workstation on page 1892 in this document. |

***Note:*** Installing the previous version of SSPFS and restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN07.

## Downgrading to (I)SN06

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06. Place a check (√) in the √column as you complete each procedure.

### Downgrading the SSPFS and CS 2000 Management Tools software to (I)SN06

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Install the previous version of SSPFS on the CS 2000 Management Tools server. | | Refer to procedure Reverting to the previous release of the SSPFS software on page 1858 in this document. |
| 2 | Restore the file systems from backup media. | | Refer to procedures Restoring root file systems - pre-(I)SN06.2. and Restoring non-root file systems on an SSPFS-based server pre-(I)SN06.2 on page 1868 in this document. |
| 3 | Restore the Oracle data from backup media. | | Refer to procedure Restoring application data to the Oracle database on an SSPFS-based server pre-(I)SN06.2 on page 1874 in this document. |
| 4 | Clear the Java ™ Web Start (JWS) cache on the client workstation. | | Refer to procedure Clearing the JWS cache on a client workstation on page 1892 in this document. |

***Note:*** Installing the previous version of SSPFS and restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN07.

# Downgrading to (I)SN06.2

Follow the link according to your office configuration.

- Rollback on Sun Netra t1400 and Sun Netra 240 one-server configuration on page 1845
- Rollback on Sun Netra 240 two-server configuration on page 1846

## Rollback on Sun Netra t1400 and Sun Netra 240 one-server configuration

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06.2. Place a check (√) in the √column as you complete each procedure.

### Downgrading a Sun Netra t1400 or Sun Netra 240 (one-server configuration) to (I)SN06.2

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Restore the file systems and Oracle data from backup media. | | Refer to procedure Performing a full system restore on an SSPFS-based server (I)SN06.2 or greater on page 1885 in this document. |
| 2 | Clear the Java ™ Web Start (JWS) cache on the client workstation. | | Refer to procedure Clearing the JWS cache on a client workstation on page 1892 in this document. |

***Note:*** Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN07.

### Rollback on Sun Netra 240 two-server configuration

Follow the link according to whether only one server in the cluster was upgraded to (I)SN07, or both servers in the cluster were upgraded to (I)SN07.

- Downgrading the only upgraded server in the cluster on page 1846
- Downgrading both upgraded servers in the cluster on page 1847

### Downgrading the only upgraded server in the cluster

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06.2 on the only upgraded server. Place a check (√) in the √column as you complete each procedure.

### Downgrading the only upgraded server to (I)SN06.2

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Clone the image of the server with the (I)SN06.2 software onto the other (upgraded) server. | | Refer to procedure Cloning the image of one node in a cluster to the other node on page 734 in this document. |

***Note:*** Cloning the image of the (I)SN06.2 server onto the server that was upgraded, restores the server as it was before the upgrade to (I)SN07.

**Downgrading both upgraded servers in the cluster**

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06.2 on both upgraded servers. Place a check (√) in the √column as you complete each procedure.

**Downgrading both upgraded servers to (I)SN06.2**

| | Activities | √ | Procedures |
|---|---|---|---|
| 1 | Restore the file systems and Oracle data from backup media. | | Refer to procedure Performing a full system restore on an SSPFS-based server (I)SN06.2 or greater on page 1885 in this document. |
| 2 | Clone the image of the server you just downgraded to (I)SN06.2, onto the other server. | | Refer to procedure Cloning the image of one node in a cluster to the other node on page 734 in this document. |
| 3 | Clear the Java ™ Web Start (JWS) cache on the client workstation. | | Refer to procedure Clearing the JWS cache on a client workstation on page 1892 in this document. |

***Note:*** Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN07.

# Migrating the SAM21 network elements back to the CS 2000 SAM21 Manager on the core manager

## Application

Use this procedure to migrate the SAM21network element back to the CS 2000 SAM21 Manager on the core manager.

## Prerequisites

None

## Action

### Launch the CS 2000 SAM21 Manager client that resides on the core manager

***At the client workstation***

1 Log on the client workstation using the correct user ID and password. Do not log on as the root user.

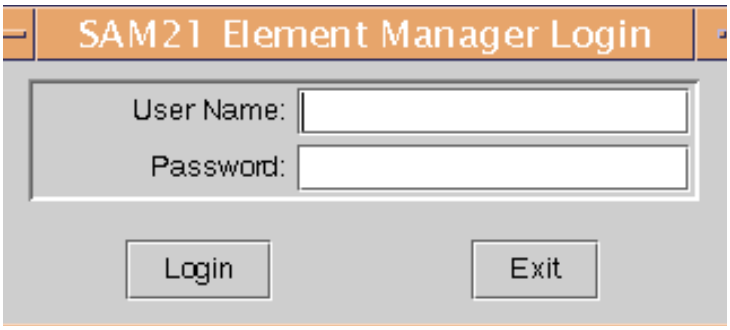
2 Launch the SAM21 Manager client application that resides on the core manager by typing

```
# /sdm/bin/sam21gui
```

and pressing the Enter key.

The user authentication window appears.

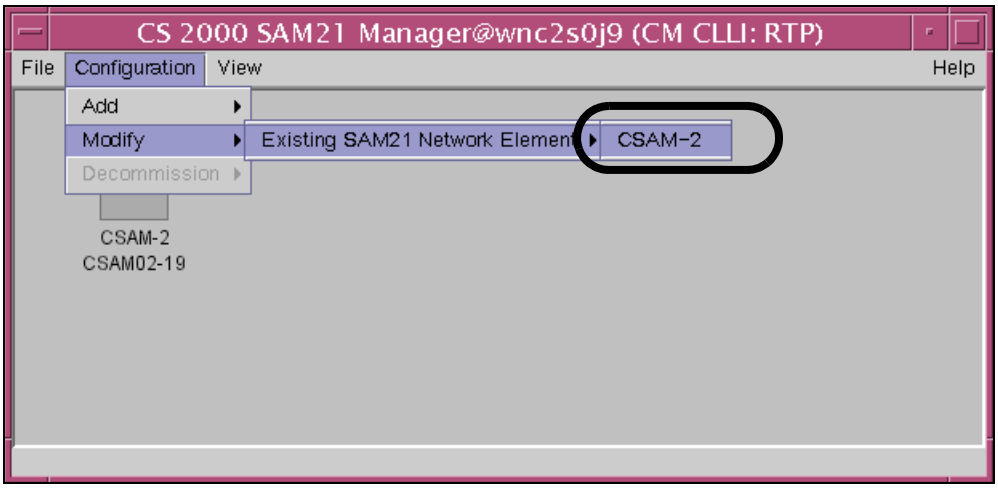
**User authentication window**




3 Enter a valid user name and password, and click the “Login” button.

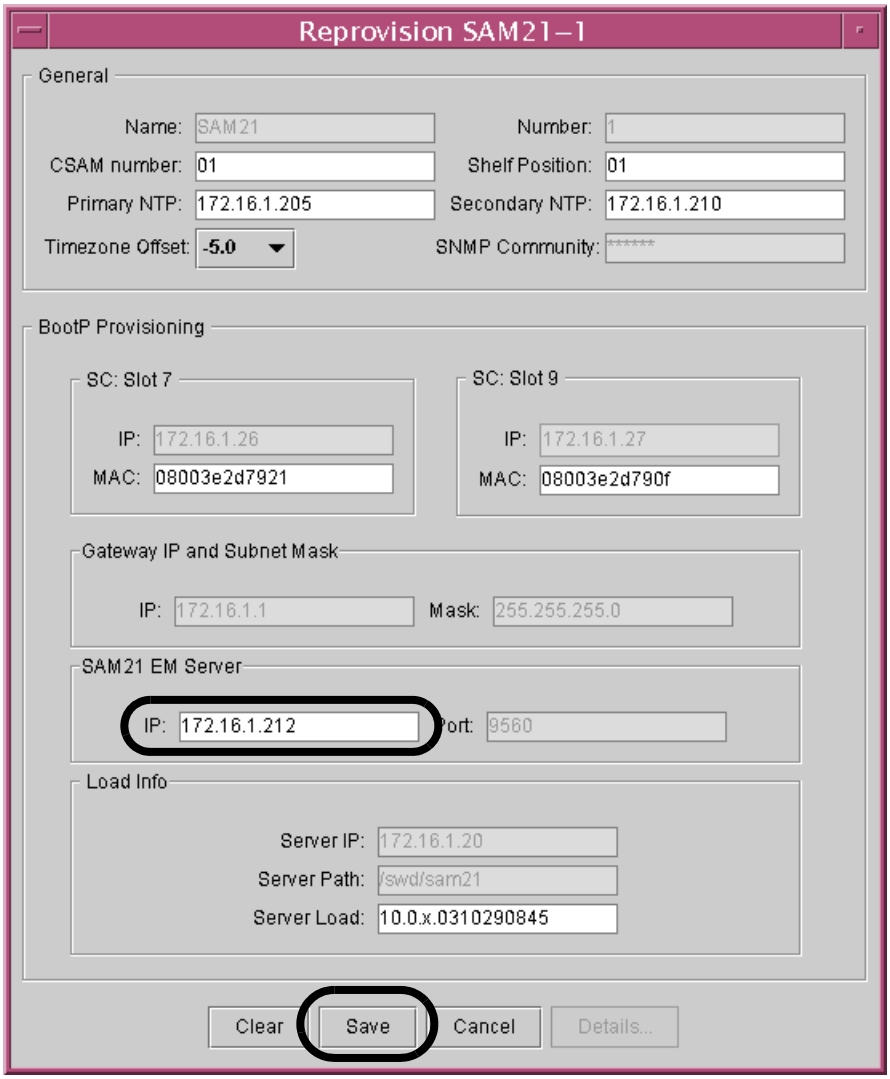
**4** Reprovision each SAM21 network element (NE) as follows:

**a** Use the Configuration menu to modify a SAM21 NE.




The Reprovision window for the SAM21NE you selected, opens.

**b** Replace the existing IP address with the IP address of the core manager, and click Save.




An SNMP message is sent to both SAM21 NEs with the IP and port of the core manager. Within approximately 1 minute, the SAM21 NE recovers from isolation on the CS 2000 SAM21 Manager that resides on the core manager. Within approximately 2 minutes, the SAM21 NE is isolated on the CS 2000 SAM21 Manager that resides on the CS 2000 Management Tools server.

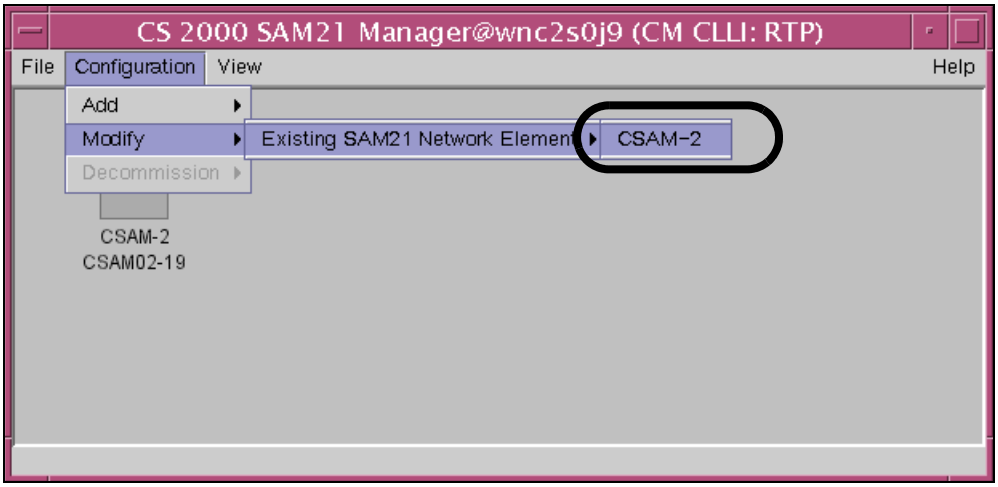
## Launch the CS 2000 SAM21 Manager client that resides on the CS 2000 Management Tools server

***At your workstation***

**1** Launch the SAM21 Manager client application that resides on the CS 2000 Management Tools server. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

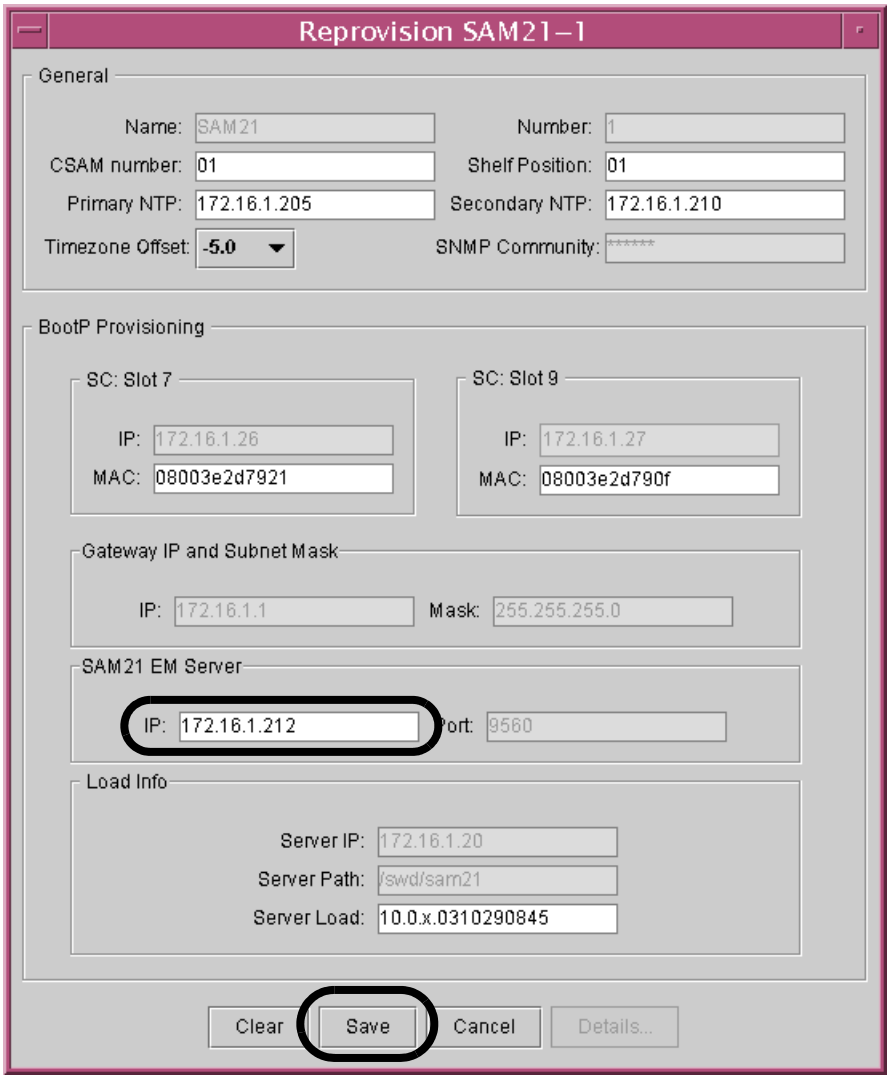
**2** Reprovision each SAM21 network element (NE) as follows:

**a** Use the Configuration menu to modify a SAM21 NE.




The Reprovision window for the SAM21NE you selected, opens.

**b** Replace the existing IP address with the IP address of the core manager, and click Save.




All non-isolated shelves are communicating with the CS 2000 SAM21 Manager on the core manager.

**3** You have completed this procedure.

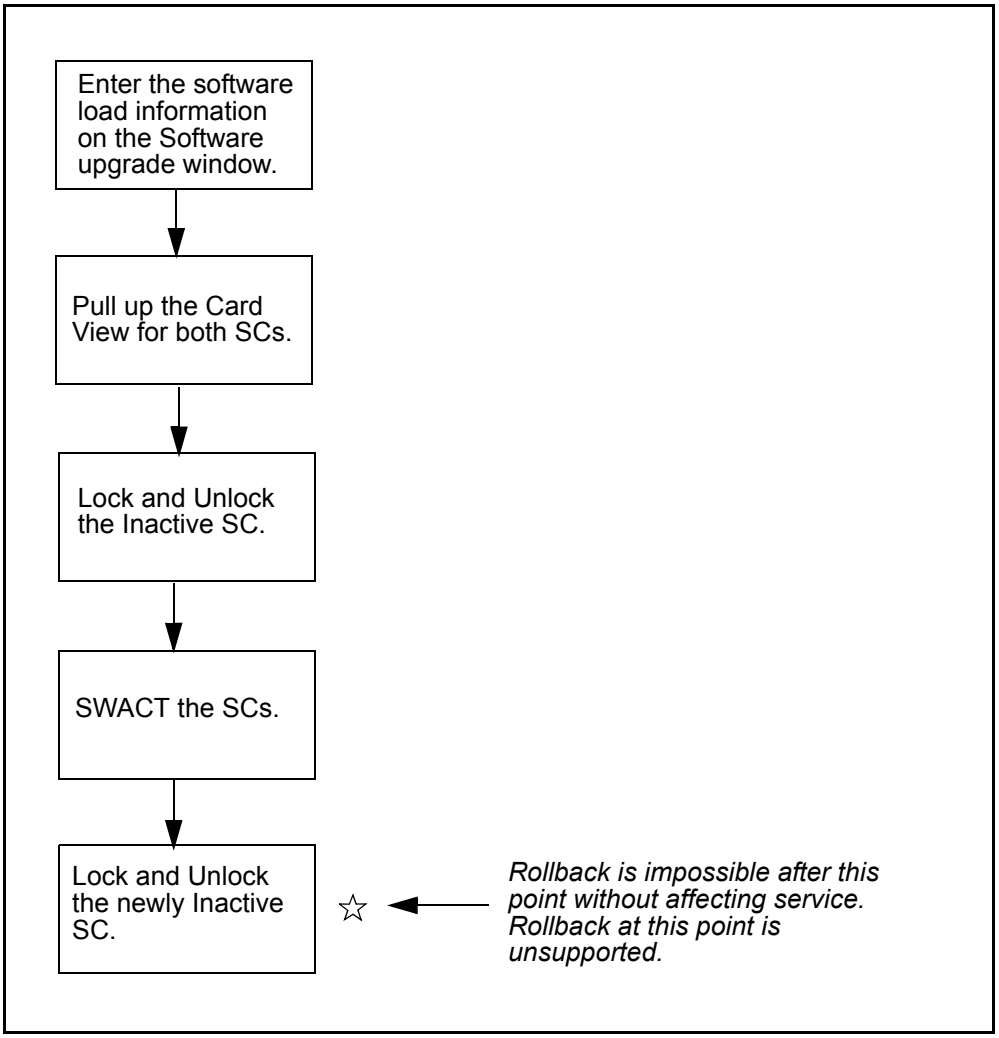
# Rollback software on the SAM21 Shelf Controller

If a rollback from SN07 to SN05 is required, ensure that the CS 2000 SAM21 Manager is running on the CS 2000 Core Manager.

**ATTENTION**

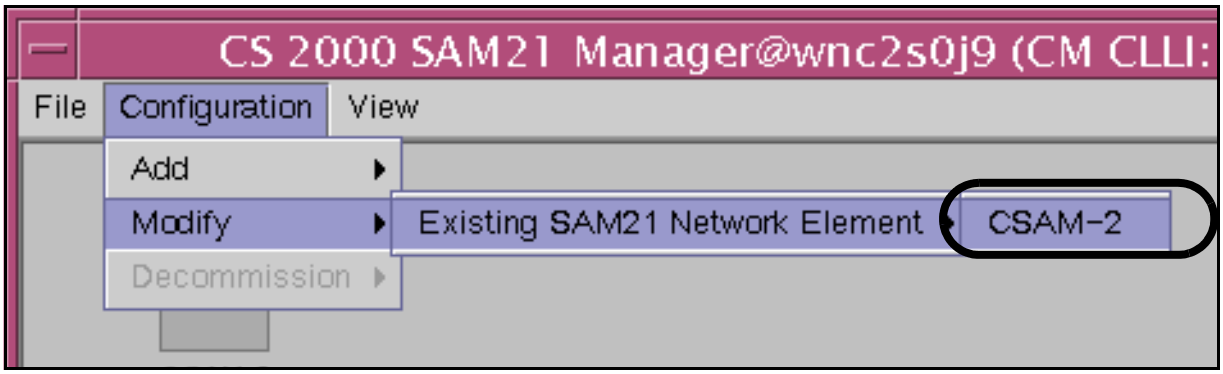
If the office is a CS 2000 - Compact, rollback the Call Agent software to SN06 before rolling back the SAM21 Shelf Controller software. Not rolling back the Call Agent software first may result in a reset loop on the next unlock or RExTst of the Call Agent.

The following figure summarizes the upgrade procedure. Rollback is available until the second SAM21 Shelf Controller is unlocked and upgraded to the new software load. This point is indicated with the star.

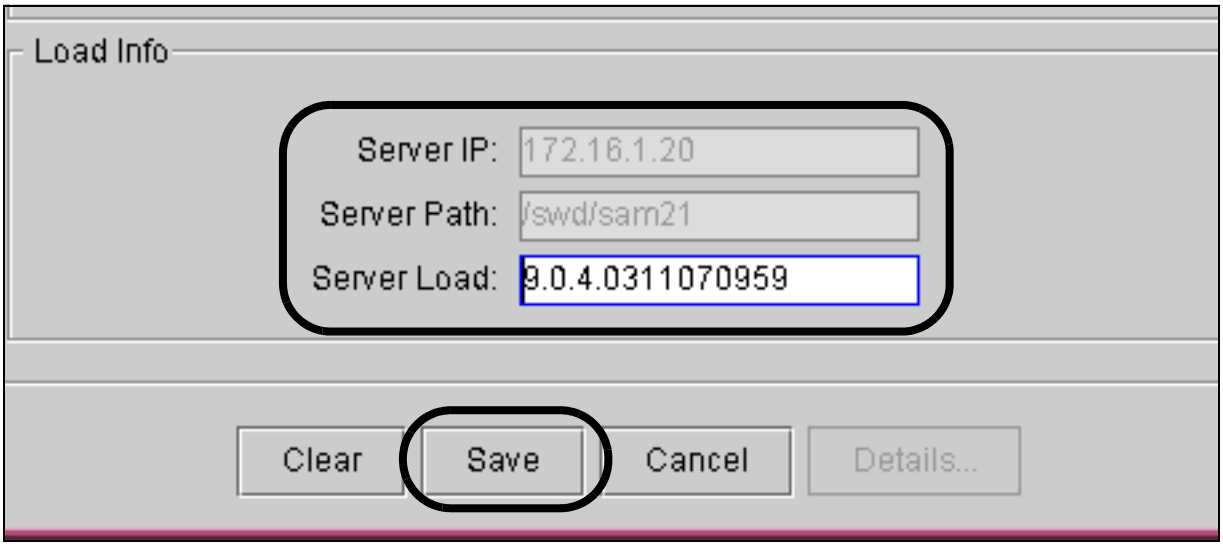


***At the CS 2000 SAM21 Manager client (Java Web Start client)***

**1** From the Subnet View, select Configuration, Modify and then the SAM21 shelf with the SAM21 Shelf Controllers to revert.




**2** Enter the software loadname of the old software load on the Reprovisioning window. For example, if the upgrade was from 9.0.4.0311070959 to 10.0.0.0301120523, enter 9.0.4.0311070959 to revert to the old software load.




**3** Click Save.

**4**

**ATTENTION**

If this was an SN05 to SN07 upgrade, perform steps 4 through 8 from the client that is served by the CS 2000 Core Manager and is started with the `/sdm/bin/sam21gui` command.

If the active SAM21 Shelf Controller is running SN07, right click on the card icon and select Swact from the card context menu. Wait for completion of SWACT.

From the Shelf View, right click on the inactive SAM21 Shelf Controller and select Lock from the card context menu.

***Note:*** This SAM21 Shelf Controller is the card that was loaded with the software upgrade and is being reverted to the previous software load.

**5** Wait for the lock icon to appear on the inactive SAM21 Shelf Controller.

**6** From the Shelf View, right click on the inactive SAM21 Shelf Controller and select Unlock from the card context menu.

**7** Wait for the hashed outline to disappear from the Inactive SAM21 Shelf Controller.

**8** This procedure is complete.

# Performing a rollback of the CS 2000 SAM21 Manager

## Application

Use this procedure to rollback the CS 2000 SAM21 Manager from the CS 2000 Management Tools server to the core manager.

**ATTENTION**
This procedure deletes all provisioned data for the CS 2000 SAM21 Manager from the database on the CS 2000 Management Tools server.

## Prerequisites

None

## Action

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

**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 hostname 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** Stop the SAM21 Manager server application by typing

```
# servstop SAM21EM
```

and pressing the Enter key.

**6** Change directory by typing

```
# cd /opt/nortel/sam21em/bin/migration
```

and pressing the Enter key.

**7** Run the SAM21 Manager rollback script by typing

```
# ./sam21emRollback.sh
```

and pressing the Enter key.

*Example response:*

```
SAM21 Element Manager Server Persistent Data
Migration Rollback
================================================
This script should only be executed to rollback
from the SSPFS SAM21 EM to the CS2E SAM21 EM.

WARNING: This script deletes all provisioned
data from the SAM21 EM database.

Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N")
```

**8** Confirm that you want to proceed with the rollback by typing

```
# y
```

and pressing the Enter key.

*Example response:*

```
Retrieving Oracle SAM21 EM Password...

Clearing the SAM21EM Database Tables...
SAM21 Element Manager Persistent data migration
rollback successful.
```

**9** You have completed this procedure.

# Reverting to the previous release of the SSPFS software

## Application

Use this procedure if you have upgraded the SSPFS software to the SN07 release and want to revert to the previous release, which can be one of the following:

- Reverting to SN05 on page 1859
- Reverting to SN06 on page 1862

## Prerequisites

You must have “SSPFS Disk 1” and “SSPFS Disk 2” for the release you are reverting to, as well as the following information:

- hostname and IP address for this system
- subnet mask for this network
- IP address for this network’s router
- timezone for this system
- IP address of the host database server
- Domain Name Service (DNS) domain name, IP address for DNS server(s), and DNS search domain(s)

***Note:*** DNS information is only required if DNS is used.

# Action

### Reverting to SN05

***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 Disk 1” into the CD ROM drive.

**4** Boot the system from the “SSPFS Disk 1” by typing

```
OK boot cdrom
```

and pressing the Enter key.

*Example response*

```
This CD contains software that under the terms
of your license agreement with Nortel Networks
is licensed for use only on Succession OAM&P.
Type “ok” to acknowledge this restriction on
your use of the software. Any other input will
halt the installation of this software.
```

**5** When prompted, acknowledge your use of the software by typing

```
ok
```

and pressing the Enter key.

**6** When prompted, enter the hostname for this system.

**7** When prompted, enter the IP address for this system.

**8** When prompted, enter the subnet mask for this network.

**9** When prompted, enter the IP address for this network’s router.

**10** When prompted, enter the timezone for this system.

***Note:*** Type **`Help`** or **`?`** for a list of timezones.

**11** When prompted, indicate whether this system will host a database. Entering “yes”, installs database services, and entering “no”, installs a database client.

Answer “yes” if the system is hosting one or more of the following applications:

- Audio Provisioning Server (APS)
- Network Patch Manager (NPM)
- CS 2000 Management Tools (SESM)

Answer “no” if the system is hosting one of the following applications:

- MG 9000 Manager Midtier (mg9kemmidtier)
- MG 9000 Manager OM Collector (mg9kemomcollector)
- MG 9000 Manager Server (mg9kemserver)

| If you enter | Do |
|---|---|
| yes (does host a database) | step 13 |
| no (does not host a database) | step 12 |

**12** When prompted, enter the IP address of the host database server.

**13** When prompted, indicate whether this system uses DNS (Domain Name Service).

| If you enter | Do |
|---|---|
| no (does not use DNS) | step 17 |
| yes (uses DNS) | step 14 |

**14** When prompted, enter the DNS domain name for this system.

**15** When prompted, enter the IP address of the DNS server(s).

***Note:*** You can enter a maximum of 5 IP addresses. If you have less than 5, enter a blank line to stop entry.

**16** When prompted, enter the DNS search domain(s).

***Note:*** You can enter a maximum of 5 DNS search domains. If you have less than 5, enter a blank line to stop entry.

**17** When prompted, review the current settings, and if correct, enter “ok” to accept them. Enter anything else to edit the settings.

The installation process begins, and takes approximately 65 minutes to complete. When complete, the system reboots, and prompts for the root password.

**18** When prompted, enter the root password.

**19** When prompted, enter the root password again.

The system ejects “SSPFS Disk 1” and prompts to insert “SSPFS Disk 2” to install all the platform common services.

**20** When prompted, remove “SSPFS Disk 1” from the drive, and insert “SSPFS Disk 2”.

**21** When ready, indicate you want to proceed by typing

```
ok
```

and pressing the Enter key.

The installation process takes approximately 40 minutes to complete. When complete, the system ejects “SSPFS Disk 2” and reboots. Once complete, the system presents the logon prompt.

**22** Log in using the root user ID and password.

***Note:*** At this point, the root password is “root”. The user-set root password will be restored once the root file system is restored, which follows.

**23** You have completed this procedure. Return to Downgrading to (I)SN05 on page 1842 in this document.

## Reverting to SN06

### *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 Disk 1” into the CD ROM drive.

4 Boot the system from the “SSPFS Disk 1” by typing

```
OK boot cdrom
```

and pressing the Enter key.

*Example response*

```
This CD contains software that under the terms
of your license agreement with Nortel Networks
is licensed for use only on Succession OAM&P.
Type “ok” to acknowledge this restriction on
your use of the software. Any other input will
halt the installation of this software.
```

5 When prompted, acknowledge your use of the software by typing

```
ok
```

and pressing the Enter key.

**6** When prompted, indicate whether this system will host a database. Entering “yes”, installs database services, and entering “no”, installs a database client.

Answer “yes” if the system is hosting one or more of the following applications:

- Audio Provisioning Server (APS)
- Network Patch Manager (NPM)
- CS 2000 Management Tools (SESM)
- CS 2000 SAM21 Manager (SAM21EM)

Answer “no” if the system is hosting one of the following applications:

- MG 9000 Manager Midtier (mg9kemmidtier)
- MG 9000 Manager OM Collector (mg9kemomcollector)
- MG 9000 Manager Server (mg9kemserver)

| If you enter | Do |
|---|---|
| yes (does host a database) | step 8 |
| no (does not host a database) | step 7 |

**7** When prompted, enter the IP address of the host database server.

**8** When prompted, review the current settings, and if correct, enter “ok” to accept them. Enter anything else to edit the settings.

The installation process begins, and takes approximately 65 minutes to complete. When complete, the system ejects “SSPFS Disk 1” and prompts to insert “SSPFS Disk 2” to install all the platform common services.

**9** When prompted, remove “SSPFS Disk 1” from the drive, and insert “SSPFS Disk 2”.

**10** When ready, indicate you want to proceed by typing

**ok**

and pressing the Enter key.

The installation process takes approximately 40 minutes to complete. When complete, the system ejects “SSPFS Disk 2” and reboots. Once complete, the system presents the logon prompt.

**11** Log in using the root user ID and password.

***Note:*** At this point, the root password is “root”. The user-set root password will be restored once the root file system is restored, which will follow.

**12** You have completed this procedure. Return to Downgrading to (I)SN06 on page 1844 in this document.

# 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 an SSPFS-based server (I)SN06.2 or greater on page 1885 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 on an SSPFS-based server pre-(I)SN06.2

## Application

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

***Note:*** For systems running the (I)SN06.2 or greater release of the SSPFS, use procedure Performing a full system restore on an SSPFS-based server (I)SN06.2 or greater on page 1885.

## 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<br>`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** When prompted, log on as root.

**9** Enter the following command to list the groups:

```
# groups oracle
```

| If the output is | Do |
|---|---|
| oinstall dba data | step 11 |
| oinstall data dba or oinstall dbs data | step 10 |

**10** Enter the following command to correct the oracle groups:

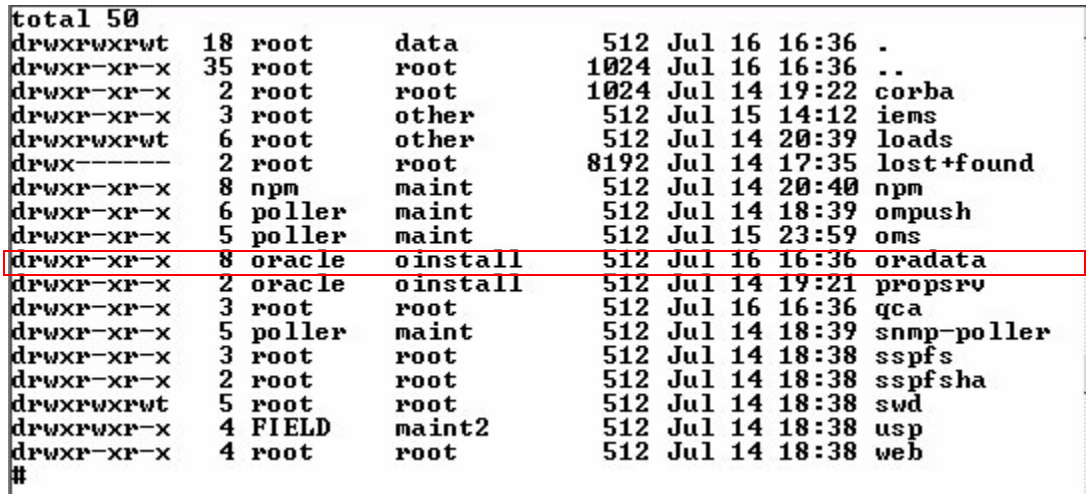
```
# usermod -g oinstall -G data,dba oracle
```

**11** Enter the following commands to ensure the ownership of the “oradata” directory is”oracle” user and “oinstall” group:

```
# cd /data

# ls -al
```

*Example response*



```
total 50
drwxrwxrwt  18 root     data          512 Jul 16 16:36 .
drwxr-xr-x  35 root     root         1024 Jul 16 16:36 ..
drwxr-xr-x   2 root     root         1024 Jul 14 19:22 corba
drwxr-xr-x   3 root     other         512 Jul 15 14:12 iems
drwxrwxrwt   6 root     other         512 Jul 14 20:39 loads
drwx------   2 root     root         8192 Jul 14 17:35 lost+found
drwxr-xr-x   8 npm      maint         512 Jul 14 20:40 npm
drwxr-xr-x   6 poller   maint         512 Jul 14 18:39 ompush
drwxr-xr-x   5 poller   maint         512 Jul 15 23:59 oms
drwxr-xr-x   8 oracle   oinstall      512 Jul 16 16:36 oradata
drwxr-xr-x   2 oracle   oinstall      512 Jul 14 19:21 propsrv
drwxr-xr-x   3 root     root          512 Jul 16 16:36 qca
drwxr-xr-x   5 poller   maint         512 Jul 14 18:39 snmp-poller
drwxr-xr-x   3 root     root          512 Jul 14 18:38 sspfs
drwxr-xr-x   2 root     root          512 Jul 14 18:38 sspfsha
drwxrwxrwt   5 root     root          512 Jul 14 18:38 swd
drwxrwxr-x   4 FIELD    maint2        512 Jul 14 18:38 usp
drwxr-xr-x   4 root     root          512 Jul 14 18:38 web
#
```

| If the ownership of the oradata directory is | Do |
|---|---|
| oracle and oinstall | step 13 |
| not oracle and oinstall | step 12 |

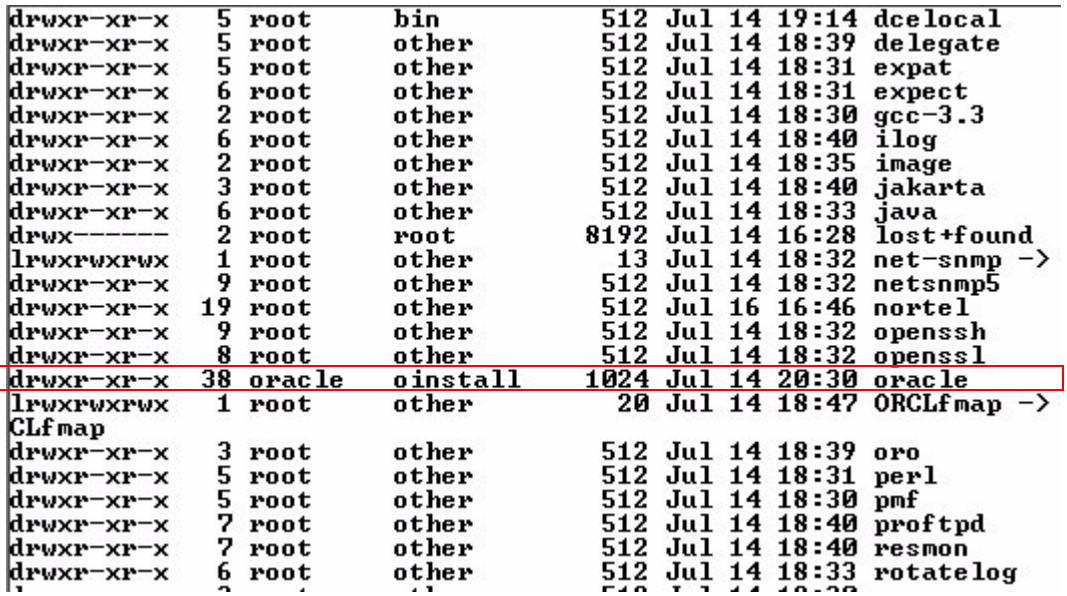
**12** Enter the following command to change the ownership to oracle and oinstall:

```
# chown oracle:oinstall oradata
```

**13** Enter the following commands to ensure the ownership of the "oracle" directory is"oracle" user and "oinstall" group :

```
# cd /opt
# ls -al
```

*Example response*



```
drwxr-xr-x   5 root     bin          512 Jul 14 19:14 dcelocal
drwxr-xr-x   5 root     other        512 Jul 14 18:39 delegate
drwxr-xr-x   5 root     other        512 Jul 14 18:31 expat
drwxr-xr-x   6 root     other        512 Jul 14 18:31 expect
drwxr-xr-x   2 root     other        512 Jul 14 18:30 gcc-3.3
drwxr-xr-x   6 root     other        512 Jul 14 18:40 ilog
drwxr-xr-x   2 root     other        512 Jul 14 18:35 image
drwxr-xr-x   3 root     other        512 Jul 14 18:40 jakarta
drwxr-xr-x   6 root     other        512 Jul 14 18:33 java
drwx------   2 root     root        8192 Jul 14 16:28 lost+found
lrwxrwxrwx   1 root     other         13 Jul 14 18:32 net-snmp ->
drwxr-xr-x   9 root     other        512 Jul 14 18:32 netsnmp5
drwxr-xr-x  19 root     other        512 Jul 16 16:46 nortel
drwxr-xr-x   9 root     other        512 Jul 14 18:32 openssh
drwxr-xr-x   8 root     other        512 Jul 14 18:32 openssl
drwxr-xr-x  38 oracle   oinstall    1024 Jul 14 20:30 oracle
lrwxrwxrwx   1 root     other         20 Jul 14 18:47 ORCLfmap ->
CLfmap
drwxr-xr-x   3 root     other        512 Jul 14 18:39 oro
drwxr-xr-x   5 root     other        512 Jul 14 18:31 perl
drwxr-xr-x   5 root     other        512 Jul 14 18:30 pmf
drwxr-xr-x   7 root     other        512 Jul 14 18:40 proftpd
drwxr-xr-x   7 root     other        512 Jul 14 18:40 resmon
drwxr-xr-x   6 root     other        512 Jul 14 18:33 rotatelog
```

| If the ownership of the opt directory is | Do |
|---|---|
| oracle and oinstall | step 15 |
| not oracle and oinstall | step 14 |

**14** Enter the following command to change the ownership to oracle and oinstall:

```
# chown oracle:oinstall oracle
```

**15** Enter the following commands to ensure the ownership of all the “oracle” subdirectories is”oracle” user and “oinstall” group:

```
# cd /opt/oracle
# ls -al
```

*Example response*

```
drwxr-xr-x  16 oracle   oinstall     512 Jul 14 18:46 ldap
drwxr-xr-x   3 oracle   oinstall    3584 Jul 14 21:36 lib
-rw-r--r--   1 oracle   oinstall     124 Jul 14 18:38 local.cshrc
-rw-r--r--   1 oracle   oinstall     607 Jul 14 18:38 local.login
-rw-r--r--   1 oracle   oinstall     582 Jul 14 18:38 local.profile
drwxr-xr-x   4 oracle   oinstall     512 Jul 14 18:47 md
drwxr-xr-x  13 oracle   oinstall     512 Jul 14 18:47 network
drwxr-xr-x   3 oracle   oinstall     512 Jul 14 18:47 ocommon
drwxr-xr-x   5 oracle   oinstall     512 Jul 14 18:47 oracore
drwxr-xr-x   6 oracle   oinstall     512 Jul 14 18:46 ORCLfmap
drwxr-xr-x  13 oracle   oinstall     512 Jul 14 18:47 ord
drwxr-xr-x   7 oracle   oinstall     512 Jul 14 18:47 otrace
drwxr-xr-x   4 oracle   oinstall     512 Jul 14 18:47 owm
drwxr-xr-x   7 oracle   oinstall     512 Jul 14 18:47 plsql
drwxr-xr-x   5 oracle   oinstall     512 Jul 14 18:47 precomp
drwxr-xr-x   2 oracle   oinstall     512 Jul 14 18:47 rcscripts
drwxr-xr-x  12 oracle   oinstall     512 Jul 14 18:47 rdbms
drwxr-xr-x   3 oracle   oinstall     512 Jul 14 18:47 relnotes
drwxr-xr-x   3 oracle   oinstall     512 Jul 14 18:47 slax
drwxr-xr-x   7 oracle   oinstall     512 Jul 14 18:47 sqlplus
drwxr-xr-x   3 oracle   oinstall     512 Jul 14 18:47 sysman
drwxr-xr-x   2 oracle   oinstall     512 Jul 14 18:46 USR
drwxr-xr-x   2 oracle   oinstall     512 Jul 14 18:46 VAR
drwxr-xr-x   3 oracle   oinstall     512 Jul 14 18:47 wwg
```

| If the ownership of all the oracle subdirectories is | Do |
|---|---|
| oracle and oinstall | step 17 |
| not oracle and oinstall | step 16 |

**16** Enter the following command to change the ownership to oracle and oinstall:

```
# chown oracle:oinstall <directory>
```

*where*

**directory**
is the name of any of the oracle subdirectories that do not have the correct ownership (oracle user and oinstall group)

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

You have completed this procedure.

# Restoring application data to the Oracle database on an SSPFS-based server pre-(I)SN06.2

## Application

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

***Note:*** For system running the (I)SN06.2 or greater release of the SSPFS, use Performing a data restore on an SSPFS-based server (I)SN06.2 or greater on page 1889 .

## Prerequisites

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

## Action

Perform the following steps to complete this procedure.

***At the server***

**1** Insert the backup tape into the drive.

***At your workstation***

**2** Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**
is the IP address or host name of the SSPFS-based server on which you are performing the data restore

**3** When prompted, enter your user ID and password.

**4** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 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 1877<br><br>Stopping the SAM21 Manager server application on page 1879<br><br>Stopping the NPM server application on page 1881 |
| MG 9000 Manager and mid-tier server applications | the MG9000 Security and Administration document, NN10162-611, if required |

7 Verify the permissions on the restore log directory (bkslog) by typing

```
# ls -alrt /var/opt/nortel
```

and pressing the Enter key.

*Example response*

```
total 22
lrwxrwxrwx   1 root     succssn       28 Dec 22  2003 gwc
-> /net/47.141.126.131//swd/gwc
drwxrwxr-x   4 root     other         512 Dec 22  2003 .
drwxr-xr-x   7 root     sys           512 Sep 10 12:41 ..
drwxr-xr-x   2 oracle   oinstall      512 Dec  8 15:58 db
drwxrwxrwt   2 root     other      6656 Dec 15 19:56 bkslog
```

| If the permissions of bkslog | Do |
|---|---|
| are drwxrwxrwt | step 9 |
| are not drwxrwxrwt | step 8 |

8 Change the permissions of bkslog by typing

```
# chmod 1777 /var/opt/nortel/bkslog
```

9 Change to the Oracle user by typing

```
# su - oracle
```

and pressing the Enter key.

10 Perform the restore command by typing

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

and pressing the Enter key.

11 Quit the Oracle user by typing

```
$ exit
```

and pressing the Enter key.

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

13 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 719<br><br>Starting the SAM21 Manager server application on page 722<br><br>Starting the NPM server application on page 1883 |
| MG 9000 Manager and mid-tier server applications | the MG9000 Security and Administration document, NN10162-611, if required |

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.

# 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.

# Performing a full system restore on an SSPFS-based server (I)SN06.2 or greater

## Application

Use this procedure to perform a full system restore from backup media on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240).

***Note:*** This procedure applies to systems restoring to the SN06.2 release of the SSPFS. For systems restoring to the SN05 or SN06 release of the SSPFS, use procedures Restoring root file systems - pre-(I)SN06.2 on page 1865 and Restoring non-root file systems on an SSPFS-based server pre-(I)SN06.2 on page 1868.

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

- Simplex configuration (one server) on page 1885
- High-availability configuration (two servers) on page 1887

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

## Prerequisites

This procedure has the following prerequisites:

- you need SSPFS CD disk#1 for the release you are reverting to
- you need the tape, CD or DVD on which you backup up the file systems
- you need the tape, CD or DVD on which you backup up the oracle data

## 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 drive.

| If restoring from | Do |
|---|---|
| tape | step 4 |
| CD/DVD | step 5 |

4 Insert the tape on which you backed up the file systems, into the drive.

5 At the OK prompt, restore the system by typing

```
OK boot cdrom - restore
```

and pressing the Enter key.

6 When prompted, accept the software license restrictions by typing

```
ok
```

and pressing the Enter key.

The system reboots.

***Note:*** If restoring from CD or DVD, you will be prompted to insert Volume 1 of the backup CD or DVD into the drive. Insert the CD or DVD on which you backed up the file systems. During the restore process, the system will prompt you for additional Volumes if more than one CD or DVD was used during the backup of file system.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

***Note:*** Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

7 Enter the following command to list the groups:

```
# groups oracle
```

| If the output is | Do |
|---|---|
| oinstall dba data | step 9 |
| oinstall data dba or oinstall dbs data | step 8 |

8 Enter the following command to correct the oracle groups:

```
# usermod -g oinstall -G data,dba oracle
```

9 Restore the data. If required, refer to procedure Performing a full system restore on an SSPFS-based server (I)SN06.2 or greater on page 1885.

***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 pressing the Enter key.

You have completed this procedure.

### High-availability configuration (two servers)

#### *At the console connected to the inactive node*

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

2 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

#### *At the console connected to the active node*

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

4 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

5 Insert SSPFS CD disk#1 into the drive.

6 At the OK prompt, restore the system by typing

```
OK boot cdrom - restore
```

and pressing the Enter key.

7 When prompted, accept the software license restrictions by typing

```
ok
```

and press the Enter key.

The system reboots.

8 When prompted, insert Volume 1 of the CD or DVD on which you backed up the file systems, into the drive.

***Note:*** During the restore process, the system will prompt you for additional Volumes if more than one CD or DVD was used during the backup file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

***Note:*** Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

9 Enter the following command to list the groups:

```
# groups oracle
```

| If the output is | Do |
|---|---|
| oinstall dba data | step 11 |
| oinstall data dba or oinstall dbs data | step 10 |

10 Enter the following command to correct the oracle groups:

```
# usermod -g oinstall -G data,dba oracle
```

11 Restore the data. If required, refer to procedure Performing a data restore on an SSPFS-based server (I)SN06.2 or greater on page 1889.

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

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

```
# init 6
```

and press the Enter key.

13 Reimage the inactive node using the active node's image. If required, refer to procedure Cloning the image of one node in a cluster to the other node on page 734.

You have completed this procedure.

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

## Application

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

***Note 1:*** For systems running the (I)SN05 or (I)SN06 release of the SSPFS, use procedure Restoring application data to the Oracle database on an SSPFS-based server pre-(I)SN06.2.

***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 server***

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

***At your workstation***

**2** Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**
is the IP address or host name of the SSPFS-based server on which you are performing the data restore

**3** When prompted, enter your user ID and password.

**4** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

**5** When prompted, enter the root password.

6 Verify the permissions on the restore log directory (bkslog) by typing

```
# ls -alrt /var/opt/nortel
```

and pressing the Enter key.

*Example response*

```
total 22
lrwxrwxrwx   1 root     succssn       28 Dec 22  2003 gwc
-> /net/47.141.126.131//swd/gwc
drwxrwxr-x   4 root     other         512 Dec 22  2003 .
drwxr-xr-x   7 root     sys           512 Sep 10 12:41 ..
drwxr-xr-x   2 oracle   oinstall      512 Dec  8 15:58 db
drwxrwxrwt   2 root     other      6656 Dec 15 19:56 bkslog
```

| If the permissions of bkslog | Do |
|---|---|
| are drwxrwxrwt | step 8 |
| are not drwxrwxrwt | step 7 |

7 Change the permissions of bkslog by typing

```
# chmod 1777 /var/opt/nortel/bkslog
```

8 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<br><br>Stopping the SAM21 Manager server application<br><br>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 |

9 Restore the database by typing

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

and pressing the Enter key.

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

11 Verify that the database restored properly.

12 Start the server applications that run on the server.

| For | Refer to |
|---|---|
| CS 2000 Management Tools server applications | Starting the SESM server application<br><br>Starting the SAM21 Manager server application<br><br>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 |

You have completed this procedure.

# Clearing the JWS cache on a client workstation

## Application

Use this procedure to clear the Java ™ Web Start (JWS) cache on a client workstation.

The JWS cache on a client workstation needs to be cleared after an HTTPS certificate is installed on an existing Sun server that was not previously using a certificate. Clearing the cache allows you to properly launch the CS 2000 Management Tools client applications from your workstation.

## Prerequisites

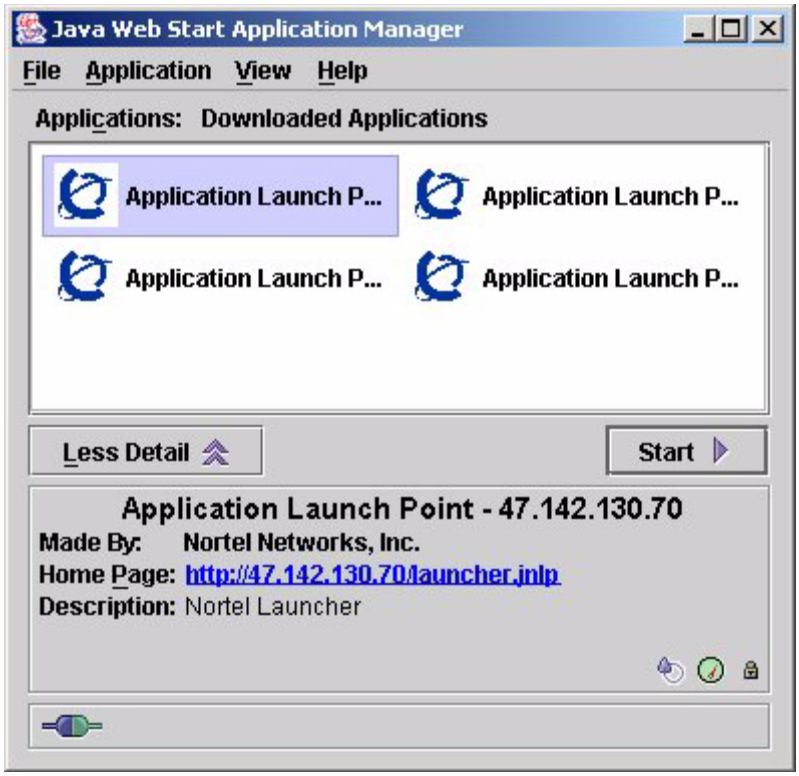
None

## Action

Perform the following steps to complete this procedure.

***At your workstation***

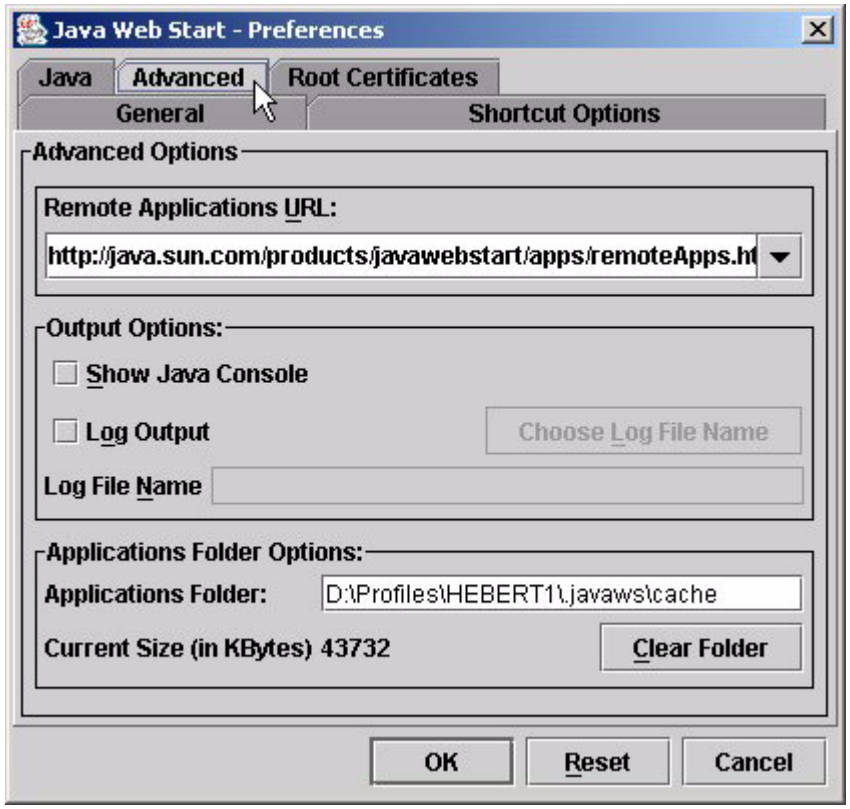
**1** Access the Java Web Start Application Manager.



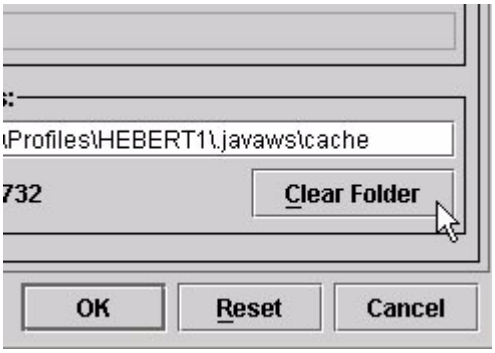
2 Access the Preferences panel by clicking **File->Preferences**.




3 Access the Advanced panel by clicking the **Advanced** tab.



4 Clear the cache by clicking **Clear Folder**.




5 Confirm you want to clear the cache (remove all downloaded resources) by clicking **Yes**.




6 You have completed this procedure.

# SAM21 Shelf Controller does not unlock

If the SAM21 Shelf Controller does not unlock and the lock icon persists on the SAM21 Shelf View, then the SAM21 Shelf Controller failed to boot.

### *At the CS 2000 SAM21 Manager client*

**1** Ensure that the SAM21 Shelf Controller has enough time to boot. A SAM21 Shelf Controller can take up to 4 minutes to boot on a slow network.

If the SAM21 Shelf Controller has enough time to boot and still has a lock icon and a hashed outline, continue with this procedure.

### *At the SAM21 frame*

**2** Verify that the SAM21 Shelf Controller is fully seated in the slot. Check the latches on the SAM21 Shelf Controller and the Hot Swap Controllers. The latch handles are perpendicular to the faceplate when the card is inserted properly and the latches are latched properly.

***Note:*** Do not push on the faceplate to seat the card; use the levers.

**3** Connect a VT100 terminal or a PC with terminal application software to the serial port labeled COM1 on the rear of the SAM21 shelf. If the SAM21 Shelf Controller in slot 7 does not boot, connect to slot 7. If the SAM21 Shelf Controller in slot 9 does not boot, connect to slot 9.

**a** To start the HyperTerminal application, click Start menu, click Programs, click Accessories, and click HyperTerminal.

**b** Double click the Hyperterm.exe icon to open a new connection.

The system displays the Connection Description box.

**c** Enter SC in the Name field and click OK.

The system displays the Phone Number box.

**d** Select Direct to COM1 from the “Connecting using:” list. Leave other entries in the box empty. Click OK.

**e** Open the COM1 Properties box and set the port settings to the following:

- Bits per second: 9600
- Data bits: 8

- Parity: None
- Flow control: Hardware

Click OK.

**f** Press the Enter key.

The system displays a new Hyperterm window with a login prompt.

**4** If the message `em respawning too fast` is displayed on the console, the latches are not latched properly.

Press the reset button on the faceplate while the console is connected and verify that the firmware revision is RM12 or the firmware revision indicated in the *SAM21 Platform Base Release Notes*.

```
Copyright Motorola Inc. 1988-2000, All Rights Reserved

PPC1 Debugger/Diagnostics Release Version 4.9 - 07/12/01 HA RM12
COLD Start

Local Memory Found=08000000 (&134217728)

MPU Clock Speed=367Mhz

BUS Clock Speed=67Mhz

WARNING: Keyboard Not Connected

Reset Vector Location   : ROM Bank B
Mezzanine Configuration : Single-MPU
Current 60X-Bus Master  : MPU0
Idle MPU(s)             : none

L2Cache                 : 1024KB, 147Mhz
System Memory           : 128MB, ECC Enabled (ECC-Memory Detected)


HA Mesquite Abbreviated Self-Tests about to Begin...
ISABRIDGE IRQ: Interrupt Request.....Running--->   PASSED

SelfTest/Boots about to Begin... Press <BREAK> at anytime to Abort ALL

NetBoot about to begin... Press <ESC> to Bypass, <SPC> to Continue
```

Firmware revision RM12

**5** Press the **Esc** key to bypass NetBoot and access the PPC-Bug prompt.

**6** Type **cnfg** at the PPC-Bug prompt and press Enter.

***Note:*** The MAC address of the SAM21 Shelf Controller card should be displayed. Verify that this is the address used in the CS 2000 SAM21 Manager client on the Reprovisioning window.

7 Type **niot** at the PPC-Bug prompt and press Enter.

8 The SAM21 Shelf Controller software provides a series of prompts. Accept the default values except the following options in bold. For the options in bold, enter the value indicated in the table.

***Note:*** If an error is entered, type **.** (period) and press Enter to quit. Restart niot by typing **niot** and pressing Enter.

| Prompt | Value |
|---|---|
| Controller LUN | 00 |
| Device LUN | 00 |
| Node Control Memory Address | 07F9E000 |
| **Client IP Address** | **0.0.0.0** |
| **Server IP Address** | **0.0.0.0** |
| Subnet IP Address Mask | 255.255.255.0 |
| Broadcast IP Address | 255.255.255.255 |
| **Gateway IP Address** | **0.0.0.0** |
| **Boot File Name** | NULL |
| Argument File Name | NULL |
| Boot File Load Address | 001F0000 |
| Boot File Execution Address | 001F0000 |
| Boot File Execution Delay | 00000000 |
| Boot File Length | 00000000 |
| Boot File Byte Offset | 00000000 |
| **BOOTP/RARP Request Retry** | **00** |
| **TFTP/ARP Request Retry** | **00** |
| **Hardware Error Retry Attempts** | **20** |
| Trace Character Buffer Address | 00000000 |

| Prompt | Value |
|---|---|
| **BOOTP/RARP Request Control** | **A** |
| **BOOTP/RARP Reply Update Control** | **N** |
| **Update Non-Volatile RAM** (only appears if a change has been made) | **Y** |

**9** Type **env** at the PPC-Bug prompt and press Enter.

**10** The SAM21 Shelf Controller software provides a series of prompts. Accept the default values except the following options in bold. For the options in bold, enter the value indicated in the table.

| Prompt | Value |
|---|---|
| Bug or System Environment | B |
| Field Service Menu Enable | N |
| Probe System for Supported I/O Controllers | Y |
| Auto-Initialize of NVRAM Header Enable | Y |
| **Network PReP-Boot Mode Enable** | **Y** |
| SCSI Bus Reset on Debugger Startup | N |
| Primary SCSI Bus Negotiations Type | A |
| Primary SCSI Data Bus Width | N |
| Secondary SCSI Identifier | 07 |
| NVRAM Boot List (GEV.fw-boot-path) Boot Enable | N |
| NVRAM Boot List (GEV.fw-boot-path) Boot at power-up only | N |
| NVRAM Boot List (GEV.fw-boot-path) Boot Abort Delay | 5 |
| Auto Boot Enable | N |
| Auto Boot at power-up only | N |
| Auto Boot Scan Enable | N |

| Prompt | Value |
|---|---|
| Auto Boot Scan Device Type List | FDISK/CDROM/TAPE/HDISK/ |
| Auto Boot Controller LUN | 00 |
| Auto Boot Device LUN | 00 |
| Auto Boot Partition Number | 00 |
| Auto Boot Abort Delay | 7 |
| Auto Boot Default String | NULL |
| ROM Boot Enable | N |
| ROM Boot at power-up only | Y |
| ROM Boot Abort Delay | 5 |
| ROM Boot Direct Starting Address | FFF00000 |
| ROM Boot Direct Ending Address | FFFFFFFC |
| **Network Auto Boot Enable** | **N** |
| Network Auto Boot at power-up only | N |
| Network Auto Boot Controller LUN | 00 |
| Network Auto Boot Device LUN | 00 |
| Network Auto Boot Abort Delay | 5 |
| Network Auto Boot Configuration Parameters Offset (NVRAM) | 00001000 |
| **Watchdog prior status ignored at autoboot** | **Y** |
| **Watchdog reset at board reset** | **Y** |
| **Reset Ethernet chip after file reception** | **Y** |
| Stop Auto Boot After Selftest Failure | N |
| Memory Size Enable | Y |
| Memory Size Starting Address | 00000000 |
| Memory Size Ending Address | 08000000 |

| Prompt | Value |
|---|---|
| DRAM Speed in NANO Seconds | 50 |
| ROM First Access Length (0-31) | 10 |
| ROM Next Access Length (0-15) | 0 |
| DRAM Parity Enable [On-Detection/Always/ Never - O/A/N] | O (letter O) |
| L2Cache Parity Enable [On-Detection/Always/Never - O/A/N] | O (letter O) |
| PCI Interrupts Route Control Registers (PIRQ0/1/2/3) | 0A050000 |
| Serial Startup Code Master Enable | N |
| Serial Startup Code LF Enable | N |
| Claim domain A | N |
| Claim domain B | N |
| Slot power control word | 00000000 |
| Ignore healthy control word | 00000000 |
| **Firmware Command Buffer Enabled** | **Y** |
| **Firmware Command Buffer Delay** | **20** |
| **Firmware Command Buffer** | **ma cboot**<Enter key><br>**pboot 14 0**<Enter key><br>**nbo**<Enter key><br><Enter key><br>**ma ;l**<Enter key> (letter L)<br>**cboot**<Enter key><br>**NULL** |
| **Update Non-Volatile RAM** (appears only when a change is made) | **Y** |
| Reset local system (CPU) | Y |

**11** The SAM21 Shelf Controller reboots.

**12** Optionally verify that calls can originate and complete.

**13** If this problem persists, contact Nortel Networks support personnel.

**14** This procedure is complete.

# Cleaning up old data in the NPM database

## Application

Use this procedure to clean up the old data in the Network Patch Manager (NPM) database following an upgrade.

**ATTENTION**

This procedure includes stopping and starting the NPM, which has the NPM re-discover the patches on the system when the NPM is brought back into service. This can take up to one hour depending on office configuration. Therefore, ensure patching tasks are not planned or scheduled in the timeframe you want to perform this procedure.

**ATTENTION**

This procedure purges any user-defined reports, tasks, sets, plans and alarms, disables any enabled plans such as AUTOAPPLY and AUTORESTART, releases any patches or devices on hold, and unconfigures the Patch File Receipt System (PFRS). Therefore, you will need to re-define any user-defined reports, tasks, sets, plans, and alarms, re-enable any plans such as AUTOAPPLY and AUTORESTART, place any desired patches or devices on hold, and re-configure PFRS following this procedure.

## Prerequisites

You must have root user privileges to perform this procedure.

## Action

Perform the following steps to complete this procedure.

***At your workstation***

1 Generate and save a patchlist report using the NPM CLUI or GUI.

***Note:*** The patchlist report may be useful in the event the apply time information is required at a later time.

| If using the | Do |
|---|---|
| CLUI | step 2 |
| GUI | step 3 |

2 Using the NPM CLUI, generate and save a patchlist as follows:

**a** 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 generate the report

**b** When prompted, enter your user ID and password.

**c** Generate the patchlist report by typing

***Note:*** You need write access to the directory that you execute the command from.

```
$ npm q patchlist output <current_date>.list
```

and pressing the Enter key.

where

**current_date**
is the date on which you are generating the report

**Example**

```
npm q patchlist output aug032004.list
```

Example response

```
Enter the NPM Succession user id and
password.
Login
```

**d** When prompted, enter the NPM user ID.

Example response

```
password
```

**e** When prompted, enter the NPM user password.

Example response

```
Redirecting output to: aug032004.list
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
Redirecting output to standard I/O
```

**f** Display the file by typing

```
$ ls
```

and pressing the Enter key.

Example response

```
aug032004.list
local.login
local.cshrc
local.profile
```

**g** Display the contents of the file by typing

```
$ cat <filename>
```

and pressing the Enter key.

where

**filename**
is the name of the file you generated earlier

**Example**
**cat aug032004.list**

Example response

```
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
```

**h** Proceed to step 6.

**3** Using the NPM GUI, generate and save a patchlist as follows:

**a** Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools client applications on page 1651 in this document.

**b** On the **Tasks** menu, click **Reports...**

**c** Click the **Report List** tab.

**d** Click on **PATCHLIST**, and click **Execute** to generate the report.

**e** Click **Save**, and specify the filename and location to save the report.

**4** 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

**5** When prompted, enter your user ID and password.

**6** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

**7** When prompted, enter the root password.

**8** Stop the NPM server application by typing

```
# servstop NPM
```

and pressing the Enter key.

**9** Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

*Example response*

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

 X - exit

select -
```

**10** Enter the number next to the “Configuration” option in the menu.

*Example response*

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit

Select -
```

**11** Enter the number next to the “Succession Element Configuration” option in the menu.

*Example response*

```
Succession Element Configuration
 1 - NPM Application Configuration
 2 - SAM21EM Application Configuration
 3 - PSE Application Configuration
 4 - OMPUSH Application Configuration


 X - exit

select -
```

**12** Enter the number next to the “NPM Application Configuration” option in the menu.

*Example response*

```
NPM Application Configuration
 1 - PFRS (Patch File Receipt System
     Configuration (PFRS))
 2 - CreateDB (Initialize or re-initialize the
     NPM database)
 3 - ConfigureNpm (Configure the Network Patch
     Manager)


 X - exit

select -
```

**13** Enter the number next to the “CreateDB” option in the menu.

**14** 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.

**15** Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

16 If any user-defined reports, tasks, sets, plans, or alarms existed prior to this procedure, re-define them using the corresponding procedure:

- for reports, use procedure Defining reports using the NPM on page 1745
- for tasks, use procedure Saving a task using the NPM on page 1735
- for sets, use procedure Defining sets using the NPM on page 1729
- for plans, use procedure Defining a plan using the NPM on page 1752
- for alarms, use procedure “Defining alarms using the NPM” in the ATM/IP solution-level Fault Management document, NN10408-900.

17 If any patches or devices were on hold prior to this procedure, place them back on hold using procedure Setting field values using the NPM on page 1740 in this document.

18 If any plans such as AUTOAPPLY and AUTORESTART, were enabled prior to this procedure, re-enable them using procedure Modifying a plan using the NPM on page 1759 in this document.

19 If PFRS was configured prior to this procedure, re-configure it using procedure Configuring NPM for automatic patch file delivery on page 1580 in this document.

20 You have completed this procedure.

***Note:*** If any users were logged in to the NPM GUI prior to this procedure, they must exit and re-launch the GUI. A re-connect to the NPM server from the GUI is not sufficient to clean up old data showing up in the GUI.

# 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.