Carrier Voice over IP Network Upgrade Overview

ATTENTION

All Media Server 2000 Series commissioned offices must also contain a commissioned Integrated Element Management System (IEMS) network application in order to complete an upgrade to software release SN08 or greater.

An IEMS can be commissioned on a stand alone server or on the same SSPFS-based server as the CS 2000 Management Tools and Clients (CMT) application.

Offices that do not contain an IEMS prior to the upgrade must schedule to commission an IEMS during the upgrade.

CAUTION

Performing an end-to-end Carrier Voice over IP network upgrade requires upgrading individual component software in a specific order. Failing to follow the required order may result in a service outage.

This document describes the upgrade order and corresponding procedures for the following configurations:

- ATM networks
- IP networks
- Tri-Modal networks

Tri-Modal configurations, introduced in the SN07 software release, allow UA-AAL1 and UA-IP configuration interworking in a multi-bearer network configuration.

This document describes the upgrade process from an existing Nortel Networks software release to a later software release. New installations and conversions are not considered as upgrades and do not pertain to the information available in this document.

Any conversions or installations of new Carrier Voice over IP components introduced in the solution cannot be performed until after the solution has been upgraded to the new software release.

How to use this document

This document includes details about supported solutions and the required component upgrade order. The upgrade order for each solution is provided in the table Component Upgrade Order on page 5. A more detailed upgrade order is provided in Component upgrade order on page 9. 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.

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 Carrier Voice over IP networks and new and changed hardware and software refer to the document *IP Solutions Basics*, NN10300-100 and *ATM Solutions Basics*, NN10320-100.

> ***Note:*** This document applies to both North American and International solutions and the prefix “i” in release numbers (for example, “(I)SN08” indicates that solutions that both market segments apply.

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

Electronically viewing this document

When viewing this document electronically, hyperlinks are provided to automatically view referenced sections. Navigating between hyperlinks is an Acrobat Reader function managed by Adobe.

Clicking on a hyperlink reference, which appears underlined and in blue, automatically navigates to the associated reference point in the document.

Returning back to the hyperlink reference may be accomplished by either of the following methods:

- on a keyboard, the hot-key combination of “Alt/arrow” navigates back and forth between hyperlinks. “Alt/left” and “Alt/right” toggle back and forth between the reference hyperlink page and the page where the hyperlink originated.
- on the screen bottom, the right and left arrow keys toggle back and forth between hyperlinks. A green arrow indicates that hyperlink activation has occurred and arrow navigation is available.

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-SN08 conversion details

SN08 Upgrade Paths

Each new software release supports an upgrade, based on dependencies, from up to two previous releases. The SN08 software release supports the following upgrade paths:

ATM Upgrade paths

The following upgrade paths to software release SN08 are supported:

- From SN06 to SN08
  - Packet Trunking - AAL1 (PT-AAL1 North American)
- From SN06.2 to SN08
  - Universal Access - AAL1 (UA-AAL1)
  - Packet Transit - AAL2 (PT-AAL2 International)
- From SN07 to SN08 - all are supported

Note: Hybrid configurations of the PT-AAL1 and UA-AAL1 solutions are also supported.

IP Upgrade paths

The following upgrade paths to SN08 are supported:

- From SN06.2 to SN08
  - Packet Transit - IP (PT-IP - International)
  - Packet Trunking - IP (PT-IP - North American)
  - Integrated Access - Wireline (IAW)
  - Integrated Access - Cable (IAC)
  - Carrier Hosted Services (CHS)
- From SN07 to SN08 - all are supported

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

Supported Tri-Modal Upgrade paths

Tri-Modal configurations were introduced in the SN07 software release therefore only upgrades from SN07 to SN08 are supported.

Carrier Hosted Services (CHS) is introduced to Tri-Modal applications in the SN08 software release, therefore no upgrades for CHS is available for a Tri-Modal application.

Component Upgrade order

This section summarizes the required component order to upgrade software to release SN08 for each all components in an upgrade path. The order applies to all solutions and applications. If a component is not part of a solution or application, the upgrade should follow the listed order for the next component that applies to the configured application.

Component Upgrade Order

	Component Name
Preparatory Upgrade	
1	Device Manager **ATTENTION: Perform this upgrade only if currently on SN06.2. An upgrade is not required if currently on SN07.**
2	Ethernet Routing Switch 8600 **ATTENTION: Perform this upgrade only if currently on SN06.2. An upgrade is not required if currently on SN07.**
Carrier Voice over IP Upgrade Order	
3	Multiservice Data Manager (MDM) • MDM • Solaris OS
4	CS 2000 Core Manager or Core and Billing Manager (CBM) 850 • SSPFS • CBM
5	Integrated Element Management System (IEMS) **ATTENTION: Perform this upgrade only if the IEMS resides on a standalone server.** **ATTENTION: If the IEMS is on the same server as the CS 2000 Management Tools (CMT) application, go directly to the CMT upgrade.** • SSPFS • IEMS

Component Upgrade Order

	Component Name
6	CS 2000 Management Tools and clients (CMT) **ATTENTION: Perform the IEMS upgrade at this time only if the IEMS is a co-resident application on the CMT server.** • SSPFS • IEMS • CS2M • APS • ABS
7	Multiservice Switch 15000
8	Peripheral Modules[1]
9	MG 9000 Manager • SSPFS • MG 9000 Manager
10	Session Server
11	SAM21 Shelf Controller
12	Gateway Controller (GWC)
13	Universal Audio Server (UAS) - no upgrade required for SN08
14	Media Server 2000 Series
15	MG 9000
16	Universal Signaling Point (USP) or USP Compact
17	Enhanced Network and Message Switch
18	CS 2000 - XA Core or CS 2000 Compact - Call Agent
19	Media Gateway 7400/15000/20000
20	Centrex IP Client Manager (CICM)[2]
21	Non-MG 15000 gateway managers and gateway[3]

Component Upgrade Order

	Component Name
22	MCS Management Server [4]
23	RTP Media Portal [4]

1.MG 4000, IW SPM ATM, IW SPM IP, and DPT SPM using PANTHER automated upgrade tool, plus legacy peripheral modules (LCM, DTC, DMS SPM, LPP, ABI XPM).
2. CHS was introduced to Tri-Modal in SN08, therefore a CICM upgrade not required for Tri-Modal networks.
3.Upgrade the element manager (EM) for one type of gateway and immediately upgrade all corresponding gateways of the same type before upgrading the next EM type.
4.Due to the complexity of the upgrade for the MCS Management Server and RTP Media Protal product, Nortel requires that all customers contact their Nortel Customer Service respresentative to engage the appropriate Nortel Software Delivery team to perform this upgrade.

Partial network upgrades

An upgrade may be necessary to introduce a maintenance release or major upgrade. These upgrades are referred to as regular maintenance release (RMR) upgrades. RMRs support upgrade or reload of individual components without affecting the rest of the components.

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 the Multiservice Data Manager, that make up a given solution.

When performing an RMR upgrade you must follow the solution upgrade order outlined in the Component Upgrade Order on page 5 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 Carrier Voice over IP network is solely within the Multiservice Data Manager 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 RMR upgrades are in-service upgrades, some components require additional hardware or special procedures for in-service upgrades.

Component upgrade order

This section provides reference tables for all components in a Carrier Voice over IP Network software upgrade. The components are listed in the required order to perform an entire end to end upgrade.

ATTENTION

This section provides the upgrade order for all components in an software upgrade. Site component configurations vary, therefore throughout this document, please disregard components not used in your configuration and move to the next applicable component in the upgrade order.

CAUTION

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

Upgrade component order summary tables

The following tables represent the components in a Carrier Voice over IP Network and are listed in the required upgrade order.

Multiservice Data Manager (MDM)

The following table contains relevant upgrade information for this component.

Multiservice Data Manager (MDM)		
Applicable Solutions	**Estimated times**	**Documentation**
ATTENTION Upgrading from SN06 (PT-AAL1 only), SN06.2, or SN07 to SN08 requires the following: • upgrade MDM 14.2 (SN06) or MDM 15.1 to MDM 15.2 • upgrade the operating system from Solaris 8 to Solaris 9		

Multiservice Data Manager (MDM)

SN06 (PT-AAL1 only), SN06.2, and SN07 to SN08

PT-AAL1 UA-AAL1 PT-IP UA-IP IAC - International CHS PT-AAL2 IAW	Up to 7 hours, longer if not performing the first two steps prior to the actual upgrade: • 30 minutes to gather software • variable time allowed to prepare OSS or IEMS • 30 minutes to apply MDM patch and MOP • 15 minutes for prechecks • 30 - 40 minutes to migrate active features • 15 minutes for post-checks • 1 hour to activate new features • 30 minutes to backup new configuration • upgrade Solaris OS — 3 hours without disk partitioning — 4 hours with disk partitioning	For upgrade procedures, refer to Multiservice Data Manager (MDM) on page 215 For rollback and other upgrade details about upgrading to SN08, refer to *Upgrading MDM*, NN10185-461

Service impacts

Upgrading the Solaris operating system requires a reboot which results in an approximate 10 minute service outage.

Comments

All times provided are estimates.

The upgrade steps to gather software and prepare the OSS or IEMS are not service affecting and my be performed prior to the actual upgrade.

The one hour allotted to activate new features represents a maximum time allowed if all features in an installed base require activation.

CS 2000 Core Manager

The following table contains relevant upgrade information for this component.

CS 2000 Core Manager		
Applicable Solutions	**Estimated times**	**Documentation**
	**Distributed Computing Environment (DCE) CAUTION** 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. 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. 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.	
	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.	

CS 2000 Core Manager		
PT-AAL1 UA-AAL1 PT-IP UA-IP IAC CHS PT-AAL2 IAW	Enhanced SDM upgrade: 2.5 hr Out-of-Service Mode: 55 min.	For upgrade procedures refer to CS 2000 Core Manager on page 303 For rollback and other upgrade details refer to *Upgrading the CS 2000 Core Manager*, NN10060-461

Service impacts

No CallP outage. OAM&P outage depends on the type of upgrade performed.

The choice of upgrade type depends on your preference between minimizing outage time or minimizing upgrade time.

Enhanced SDM upgrade service impacts

- During a SWACT the entire system will be out of service for 10 to 12 minutes.
- LMM/TMM provisioning will be OOS for up to 20 minutes.
- Billing backed up on core during the 10 to 12-minute OOS period.

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

No additional comments.

Core and Billing Manager (CBM) 850

The following table contains relevant upgrade information for this component.

Core and Billing Manager (CBM) 850		
Applicable Solutions	**Estimated times**	**Documentation**
ATTENTION Upgrading from SN07 to SN08 requires the following: • upgrade SSPFS platform — upgrade Solaris OS — upgrade SSPFS software • upgrade CBM 850 software — prepare CBM upgrade media — apply and patch the new CBM software The CBM upgrade automatically initiates during the SSPFS upgrade. Once you have upgraded the SSPFS, continue until you have upgraded all applications on that server. Failing to upgrade an application to the same release as the SSPFS will result in operational problems.		
UA-AAL1 PT-IP UA-IP IAC CHS PT-AAL2 IAW	**SSPFS** The SSPFS approximated upgrade times provided below can vary dramatically depending on the site configuration and the number of processes running: • Disk 1: 60 minutes • Disk 2: 30 minutes • Disk 3: 75 minutes	For upgrade procedures, refer to Core and Billing Manager (CBM) 850 on page 455 For rollback and other upgrade details refer to *Upgrading the Core and Billing Manager*, NN10347-461

Core and Billing Manager (CBM) 850	
	CBM Approximately 2 hours total, including • 10 - 15 minutes for prechecks • up to 1 hour to clone, SWACT, reboot • 30 minutes to install software • 10-15 minutes for post-checks
Service impacts No CallP or OAM&P outage. • The CBM 850 will be out of service for approximately 60 minutes. • Billing backed up on the core during the 60-minute OOS period.	
Comments No additional comments.	

Integrated Element Management System (IEMS)

The following table contains relevant upgrade information for this component.

Integrated Element Management System (IEMS)		
Applicable Solutions	**Estimated times**	**Documentation**

ATTENTION

All Media Server 2000 Series commissioned offices must also contain a commissioned IEMS network application in order to complete an upgrade to software release SN08 or greater.

An IEMS can be commissioned on a stand alone server or on the same SSPFS-based server (co-resident) as the CS 2000 Management Tools and Clients (CMT) application.

The IEMS Graphical User Interface (GUI) replaces the Media Server 2000 series Command Line User Interface (CLUI) used in SN07. An IEMS must be commissioned in the office and at an SN08 release before upgrading a Media Server 2000 node.

When upgrading from a release prior to SN08, perform the following procedures before beginning the network upgrade:

- Backing up Media Server 2000 Series files on page 77
- Updating the Media Server 2000 Series trusted manager table on page 80 (from SN07 only)

Once you have upgraded the SSPFS, continue until you have upgraded all applications on that server. Failing to upgrade an application to the same release as the SSPFS will result in operational problems.

STAND ALONE CONFIGURATION

For stand alone configurations; upgrade an existing server running the IEMS application or, if introducing IEMS into the office, commission IEMS at this time on a new SSPFS-based server installed prior to the upgrade.

CO-RESIDENT CONFIGURATION

For co-resident configurations, upgrade an existing IEMS application or commission a new IEMS application during the CS 2000 Management Tools and clients (CMT) on page 17 upgrade.

Integrated Element Management System (IEMS)

SN06.2 or SN07 to SN08 Commissioning (if required)

UA-AAL1
PT-IP
UA-IP
IAC
CHS
PT-AAL2
IAW

For simplex T1400 or N240:

- IEMS commission 2 hours

For dual N240 (HA)

- IEMS commission (with clone) 4 hours

SN07 to SN08 Upgrade

UA-AAL1
PT-IP
UA-IP
IAC
CHS
PT-AAL2
IAW

SSPFS

Estimated upgrade times for Sun Fire N240 cluster or simplex; or t1400 simplex configurations:

The SSPFS approximated upgrade times provided below can vary dramatically depending on the site configuration and the number of processes running:

- Disk 1: 60 minutes
- Disk 2: 30 minutes
- Disk 3: 75 minutes

For simplex T1400 or N240:

- IEMS upgrade 1.5 hours

For dual N240 (HA)

- IEMS upgrade (with clone) 3.5 hours

For upgrade procedures, refer to Integrated Element Management System (IEMS) on page 487

For downgrade and other upgrade details refer to *Upgrading the Integrated EMS*, NN10326-461

Service impacts

OAM and security services outage occurs for the combined SSPFS and IEMS upgrade times.

For HA configurations, during the switch of activity (SWACT) between active and inactive components a network loss of visibility occurs for an estimated 10 to 15 minutes.

CS 2000 Management Tools and clients (CMT)

The following table contains relevant upgrade information for this component.

CS 2000 Management Tools and clients (CMT)		
Applicable Solutions	**Estimated times**	**Documentation**
ATTENTION All Media Server 2000 Series commissioned offices must also contain a commissioned IEMS network application in order to complete an upgrade to software release SN08 or greater. For IEMS co-resident configurations, upgrade an existing IEMS application or commission a new IEMS application during the CMT upgrade. The IEMS Graphical User Interface (GUI) replaces the Media Server 2000 series Command Line User Interface (CLUI) used in SN07. An IEMS must be commissioned in the office and at an SN08 release before upgrading a Media Server 2000 node. When upgrading from a release prior to SN08, perform the following procedures before beginning the network upgrade if a Media Server 2000 Series is present in the network: • Backing up Media Server 2000 Series files on page 77 • Updating the Media Server 2000 Series trusted manager table on page 80 (from SN07 only) Once you have upgraded the SSPFS, continue until you have upgraded all applications on that server. Failing to upgrade an application to the same release as the SSPFS will result in operational problems.		

CS 2000 Management Tools and clients (CMT)

CAUTION

For the SSPFS upgrade, new logs and alarms are not processed during the required reboot however those alarm and log statuses are re synchronized after the reboot to ensure accurate status.

UA-AAL1
PT-IP
UA-IP
IAC
CHS
PT-AAL2
IAW

SSPFS

Estimated upgrade times for Sun Fire N240 cluster or simplex; or t1400 simplex configurations:

The SSPFS approximated upgrade times provided below can vary dramatically depending on the site configuration and the number of processes running:

- Disk 1: 60 minutes
- Disk 2: 30 minutes
- Disk 3: 75 minutes

If IEMS commissioning required:

For simplex T1400 or N240:

- IEMS commission 1 hour

For upgrade procedures, refer to CS 2000 Management Tools and Clients (CMT) on page 523

For rollback procedures refer to *ATM/IP Solution-level Fault Management*, NN10408-900

Service impacts

During the SWACT between active and inactive components a network loss of visibility occurs for an estimated 10 to 15 minutes.

Comments

Includes CS 2000 GWC Manager, LMM, TMM, and SAM21 clients.

APS and CS2M upgrades include upgrade of SSPFS.

SSPFS supports both t1400 and N240.

IEMS co-resident on a t1400 simplex server requires 4gb of RAM.

Multiservice Switch 15000

The following table contains relevant upgrade information for this component.

Multiservice Switch 15000		
Applicable Solutions	**Estimated times**	**Documentation**

Multiservice Switch 15000		
PT-AAL1 UA-AAL1 PT-IP UA-IP PT-AAL2	1.5 hours to 2 hours	For upgrade procedures refer to Multiservice Switch (MSS) 15000/20000 on page 820 For rollback and other upgrade details refer to *Upgrading Nortel Networks Multiservice Switch 15000 in Succession Networks PT-AAL1/UA-AAL1*, NN10070-461

Multiservice Switch 15000

Service Impacts

Loss of redundancy for a period of time:

- Call processing redundancy loss for 50 minutes
- Loss of MDM connectivity upon call processing switchover

Stable two-port calls are unaffected. Other call types are impacted for up to 10 seconds.

In MSS 15000/20000, ATM networks, ATM SPVP and SPVC connections fail to transmit traffic at relay points after PNNI links bounce in the network. This problem only impacts customers having a reroute subcomponent provisioned under the ATM UNI, and having LAPS protected PNNI Relay points. This issue can be seen PCR 6.1.1, SPCR 6.1.1, PCR6.2, PCR7.1 and PCR7.2. This issue is service affecting and there are no alarms issued indicating the ATM connection is impacted.

The problem can be cleared by issuing the command:

>lock Atmif/100 Vcc/0.54 src

followed by

>unlock Atmif/100 Vcc/0.54 src

Or

>Switchover lp/2

where

shelf card/2 Spserv standbyStatus = providingService

Note: Issuing the switchover lp/x command will result in service disruptions for any unprotected ports on the card.

A MSS 15000 patch is available for PCR 6.1.1 under patch ID baseFT1409A, it can be picked up by the software baseline MSS15k05w47A_CF01S1E or later, and should be applied on customer networks as soon as possible. Patches for SPCR6.1.1, PCR 6.2 , PCR 7.1 and PCR 7.2 are currently under development. Patches for the MSS 7000 are not required as this issue relates to LAPS which is only supported on the MSS 15000. There are no workarounds to prevent this issue from occurring.

Note: To recover from the problem, either lock or unlock the problem ATM source VPC or VCC or identify the Relay Point where cells are not passing and perform a card switchover.

Comments

Multiservice Switch MSS only

Peripheral Modules

The following table contains relevant upgrade information for this component.

Peripheral Modules
ATTENTION Peripheral module upgrades use the PANTHER automated upgrade tool. For SPM-based equipment, PANTHER can concurrently mate load up to 64 RMs across 8 SPMs in the current upgrade set. Peripheral modules can consist of the following components: • Legacy Peripheral Modules: — LCM — XPM — DMS SPM (PT-AAL1) — LPP/FLPP • IW SPM IP (IAC - North America only and PT-IP) • IW SPM ATM (PT-AAL1 and UA-AAL1) • MG 4000 (PT-AAL1 and UA-AAL1) • DPT SPM (PT-AAL1 and UA-AAL1)

Peripheral Modules		
Applicable Solutions	**Estimated times**	**Documentation**
PT-AAL1 UA-AAL1 PT-IP UA-IP IAC - North America	Estimated upgrade times using the PANTHER tool are. • Legacy Peripheral Modules, refer to appropriate documentation: • IW SPM IP - 1 hour for concurrent upgrade up to 8 • IW SPM ATM - 1 hour for concurrent upgrade up to 8 • MG 4000 - 3 hours for concurrent upgrade up to 8 • DPT SPM - 3 hours for concurrent upgrade up to 8	For PANTHER upgrade procedures refer to Peripheral Modules on page 1065. For legacy PMS, refer to the *Peripheral Module Release Document*, 297-9051-599 (intl) or 297-2663-599 (NA) in your SN07 Helmsman DMS collection For rollback and other upgrade details refer to: • *Upgrading the MG 4000*, NN10054-461 • *Upgrading the IW SPM ATM*, NN10055-461 • *Upgrading the IW SPM IP*, NN10056-461 • *Upgrading the DPT SPM*, NN10058-461

Service impacts

The inactive/spare card that is being upgraded is out of service for up to 15 minutes per card.

No loss of CallP, Billing or Customer visibility to the switch as the traffic is loadshared with redundant components.

For legacy PMS, refer to peripheral module documentation.

Comments

For DMS SPM and IW SPM nodes only, the Sync Resource Module (SRM) does not provide sparing therefore offices that use SRM in those nodes must manually upgrade those SRMs prior to using the PANTHER tool. Those SRMs can be located in the SYNCLK table

MG 9000 Manager

The following table contains relevant upgrade information for this component.

MG 9000 Manager	
	**CAUTION** 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** For the SSPFS upgrade, new logs and alarms are not processed during the required reboot however those alarm and log statuses are re synchronized after the reboot to ensure accurate status. 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.

MG 9000 Manager		
Applicable Solutions	**Estimated times**	**Documentation**
UA-AAL1 UA-IP	**SSPFS** The SSPFS approximated upgrade times provided below can vary dramatically depending on the site configuration and the number of processes running: • Disk 1: 60 minutes • Disk 2: 30 minutes • Disk 3: 75 minutes **MG 9000 Manager** 1 hour for an MG 9000 Manager supporting 4 MG 9000s with 16,000 lines	For upgrade procedures refer to Media Gateway (MG) 9000 Manager on page 1103. For rollback and other upgrade details refer to *Upgrading the MG 9000*, NN10048-461
Service impacts During the SWACT between active and inactive components a network loss of visibility occurs for an estimated 10 to 15 minutes. No loss of CallP or Billing for MG 9000. Once you have upgraded the SSPFS, continue until you have upgraded all applications on that server. Failing to upgrade an application to the same release as the SSPFS will result in operational problems. ***Note:*** Refer to *Upgrading the MG 9000*, NN10048-461 for detailed service impacts and estimated upgrade times.		

Session Server

The following table contains relevant upgrade information for this component.

Session Server		
Applicable Solutions	**Estimated times**	**Documentation**
PT-IP	Approximately 2.5 hours plus soak time after the SWACT before upgrading the redundant Session Server.	For upgrade procedures refer to Session Server on page 1158 For rollback and other upgrade details refer to *Upgrading the Session Server*, NN10349-461
Service impacts No CallP or OAM&P outage.		
Comments No additional comments.		

SAM21 Shelf Controller

The following table contains relevant upgrade information for this component.

SAM21 Shelf Controller		
Applicable Solutions	**Estimated times**	**Documentation**
UA-AAL1 PT-IP UA-IP IAC CHS PT-AAL2 IAW	10 minutes for SAM21 Manager 25 minutes for SAM21 Shelf Controller	For upgrade procedures refer to SAM21 Shelf Controller on page 1280. For rollback and other upgrade details refer to *Upgrading the SAM21 Shelf Controller*, NN10067-461
Service impacts None		
ATTENTION Make sure all ATM connections are established before performing the upgrade SWACT. **Comments** If after upgrading, the SAM21 Shelf Controller fails to boot; that is it does not unlock and the lock icon persists on the SAM21 Shelf View, then refer to the procedure "SAM21 Shelf Controller does not unlock" in Upgrading the SAM21 Shelf Controller, NN10067-461.		

Gateway Controller (GWC)

The following table contains relevant upgrade information for this component.

Gateway Controller (GWC)		
Applicable Solutions	**Estimated times**	**Documentation**
UA-AAL1 PT-IP UA-IP IAC CHS IAW	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 upgrade procedures refer to Gateway Controller on page 1330. For rollback and other upgrade details refer to *Upgrading the Gateway Controller*, NN10196-461
Service impacts Stable two-port calls survive GWC SWACT. Calls in setup mode during SWACT are dropped.		
Monitoring the alarm banner on the USP for "transition to disabled" alarms, M3UA path failure or AS Isolation alarms as indications that a card has failed. The customer should wait until each of these alarms has cleared before proceeding with next GWC Swact.		
Monitoring the status of the IPS7 application-server-process-path (ASP) states. From the USP GUI, open the "configuration->IPS7->Application-server-process-path" screen. Select the "search" tab and click "retrieve". This will display the list of all IPS7 paths on the USP. Before performing a GWC swact ensure that all paths are in service (Path state shows as "up"). To refresh the screen between GWC Swacts, click the refresh button.		

Gateway Controller (GWC)

Differing GWC types are upgraded in the following order:

Non-AAL1 GWC upgrade order (includes RMRs)

- AC
- VRDN
- NGSS (applies to RMR only)
- SIP-T
- Trunks
- H.323
- V5.2 trunks
- Lines (includes CICM and large- and small-line GWCs)

UA-AAL1 GWC upgrade order (includes RMRs)

- AC
- BICC
- LInes

Gateway Controller (GWC)

Tri-Modal GWC RMR upgrade order

- AC
- BICC
- VRDN
- NGSS
- SIP-T
- Trunks
- H.323
- V5.2 trunks
- Lines (includes CICM and large- and small-line GWCs)

Note: If you have a series of calls servers serviced by one Session Server, the minimum release for all the supported call servers must be SN06.2.

Comments

Starting in the SN08 software release, parallel CS 2000 GWC upgrades are supported using the Upgrade Automation Tool.

Note: 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

Media Server 2000 Series

The following table contains relevant upgrade information for this component.

Media Server 2000 Series

ATTENTION

The SN08 software release introduces an IEMS Graphical User Interface (GUI) Media Server 2000 series configuration interface that replaces the Command Line User Interface (CLUI) used in SN07. An IEMS must be commissioned in the office and at an SN08 release before upgrading a Media Server 2000 node.

When upgrading from a release prior to SN08, perform the following procedures before beginning the network upgrade:

- Backing up Media Server 2000 Series files on page 77
- Updating the Media Server 2000 Series trusted manager table on page 80 (from SN07 only)

Applicable Solutions	Estimated times	Documentation
UA-AAL1 PT-IP UA-IP IAC CHS IAW PT-AAL2	*Software upgrade*: 2 minutes *Download of audio announcements (if applicable)*: up to 5 minutes	For upgrade procedures refer to Media Server 2000 Series on page 1413. For full upgrade details, refer to *Upgrading the MS 2000 Series*, NN10335-461

Service impacts

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.

Comments

IP applications use Media Server 2010 and ATM applications use Media Server 2020. The ATM Media Server 2020 was introduced in the SN07 software release.

MG 9000

The following table contains relevant upgrade information for this component.

MG 9000		
Applicable Solutions	**Estimated times**	**Documentation**
UA-AAL1 UA-IP	1 to 3 hours depending on the size of the MG 9000	For upgrade procedures refer to Media Gateway (MG) 9000 on page 1440 For rollback and other upgrade details refer to *Upgrading the MG 9000*, NN10048-461
Service impacts 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.		

Universal Signaling Point (USP) or USP Compact

The following table contains relevant upgrade information for this component.

Universal Signaling Point (USP) or USP Compact		
Applicable Solutions	**Estimated times**	**Documentation**
UA-AAL1 UA-IP PT-IP IAC IAW PT-AAL2	**USP** 3 hours for a 1-shelf system 6 hours for a 2-shelf system **USP compact** 1 hour ***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 upgrade procedures refer to Universal Signaling Point on page 1490 For USP rollback and other upgrade details refer to *Upgrading the USP*, NN10045-461 For USPc rollback and other upgrade details refer to *Upgrading the USP Compact*, NN10046-461
Service impacts 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 Nortel Networks recommends that you upgrade the USP in the following order: • Upgrade the USP PC GUI to SN08. • Upgrade the USP using the USP PC GUI. • Make sure that the USP is stable. • Install the USP JAVA GUI on the SSPFS. • Migrate the alternate boot server (ABS) from the PC to the SSPFS. • Disable ABS on the PC.		

Enhanced Network and Message Switch

The following table contains relevant upgrade information for this component.

Enhanced Network and Message Switch		
Applicable Solutions	**Estimated times**	**Documentation**
PT-AAL1 UA-AAL1 UA-IP PT-IP IAC CHS IAW PT-AAL2	Refer to TDM standards	*For upgrade information refer to* Enhanced Network and Message Switch on page 1636
Service impacts Refer to TDM standards		

CS 2000 - XA Core

The following table contains relevant upgrade information for this component.

CS 2000 - XA Core		
Applicable Solutions	**Estimated times**	**Documentation**
XA-Core		
PT-AAL1 UA-AAL1 PT-IP UA-IP IAC CHS IAW PT-AAL2	CS 2000 Core: 4 hours IOP to HIOP: 10 minutes	*For upgrade information refer to* XA-Core - CS 2000 on page 1638 *XA-Core Maintenance Manual* (297-8991-510), in the Helmsman DMS collection *Global Software Delivery One Night Process Software Delivery Procedures*, 297-8991-303, in the Helmsman DMS collection *DMS Peripheral Module Software Release Document*, 297-9051-599 (intl) or 297-2663-599 (NA) in the Helmsman DMS collection
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 The Atlas PE is supported in SN08. Any 2+1 Rhino configuration must be upgraded to 3+1 Rhino prior to the SN08 upgrade. Rhino-to-Atlas network upgrades for networks using Carrier Voice over IP 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: All SN08 upgrades require new customer-specific parameters related to the solution fabric. The parameters are normally provided through bulletins in the FEATDATA file. Contact Nortel Networks technical support if you require more information.		

CS 2000 Compact - Call Agent

The following table contains relevant upgrade information for this component.

CS 2000 Compact - Call Agent		
Applicable Solutions	**Estimated times**	Documentation
PT-IP UA-IP IAC CHS IAW PT-AAL2	CS 2000 Compact: Platform and PCL upgrade (ONP): 1.5 hours (+ additional customer test acceptance time, if required).	For upgrade information refer to Call Agent - CS 2000 Compact on page 1639. 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.		

Media Gateway 7400/15000/20000

The following table contains relevant upgrade information for this component.

Media Gateway 7400/15000/20000		
Applicable Solutions	**Estimated times**	Documentation
MG 15000: PT-IP UA-IP IAC CHS IAW MG 15000 and MSS 15000 combo: UA-IP only	**In-service Med 5.2 upgrade** 20 minutes to 3.5 hours, depending on the number of calls and components that have been provisioned on the MG 15000 **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) **PLUS** time required to rts all links (20 seconds per link) **Out-of-service MG 15000 upgrade** 20 minutes to 3.5 hours, depending on the number of calls and components that have been provisioned on the MG 15000 **PLUS** time required to deactivate all V5 interfaces on the MG 15000 (1 minute per interface)	For upgrade information refer to Media Gateway 7400/15000/20000 on page 1769. For rollbacks and other upgrade details refer to *Upgrading Multiservice Switch 15000/Media Gateway 15000/20000 in Succession IP Solutions (UA-IP)*, NN10419-461

Media Gateway 7400/15000/20000

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)

Supported PCR upgrades to SN08

The following MG 15000 upgrade scenarios are supported:

- PCR 5.2 to PCR 6.1.2
- PCR 6.1 to PCR 6.1.2

Service impacts

SN06.2 to SN08 Upgrades

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

Service interruptions (for new calls) during an upgrade from SN06.2 (PCR 5.2) to SN08 will vary depending on whether VRAP capabilities are enabled, however an estimate of 5-7 seconds can be expected as the 4pGigE FP did not become carrier grade enabled until the SN08 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.

SN07 to SN08 Upgrades

No service interruptions.

HSM Supported upgrades

The following indicates which upgrades support HSM.

PCR Upgrade to PCR 6.1.2	HSM supported
5.2 or 6.1 ASPEN/H.248 with 4port OC-3	YES
5.2 or 6.1 ASPEN/H.248 with VSP3 GigE	NO
5.2 or 6.1 ASPEN/H.248 non 4port OC-3	NO

VoIP networks

Change from ASPEN to H.248 occurs during the upgrade and also is supported after the upgrade to PCR 6.1.2. 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 6.1.2 and then have H.248 enabled on a node-by-node basis.

Centrex IP Client Manager (CICM)

The following table contains relevant upgrade information for this component.

Centrex IP Client Manager (CICM)		
Applicable Solutions	**Estimated times**	Documentation
PT-IP UA-IP IAC CHS	Sequence 1 - Split CICM: 35 minutes Sequence 2 - New CICM RTS: 20 minutes Sequence 3 - Transferring Control: 55 minutes	For upgrade information refer to Centrex IP Client Manager (CICM) on page 1771. For rollback and other upgrade details, refer to *Upgrading CICM*, NN10230-461

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

Direct upgrades from SN06.2 to SN08 are not supported. Upgrading to SN08 from SN06.2 requires the following two upgrades: must be SN06.2 to SN07, then finally to SN08The SN06.2 CICM release is 6.12.

- SN06.2 to SN07
- SN07 to SN08

The CICM 6.12 release is only supported on a 5370 card mounted on a SAM16 chassis, therefore upgrading from SN06.2 to SN08 requires a hardware upgrade to a 5385 card mounted on a SAM21 chassis. The following list summarizes the Carrier Voice over IP releases to the CICM releases and supported hardware.

Release	CICM Release	Card/Chassis support
SN06.2	6.1	5370/SAM16
SN07	7.1	5385/SAM21
SN08	8.0	5385/SAM21

Non-MG 15000 gateway managers and gateway

The following table contains relevant upgrade information for this component.

Non-MG 15000 gateway managers and gateways		
Applicable Solutions	**Estimated times**	Documentation
CHS IAC IAW	For estimated upgrade times, refer to OEM/third-party media gateway upgrade documentation	For upgrade information refer to Original Equipment Manufacturer (OEM) gateways and gateway managers on page 1833 Refer to OEM/third-party media gateway upgrade documentation.
Service impacts Refer to the appropriate component upgrade documentation.		
Comments Either CS 2000 or MCS can upgrade independently. However, MCS must be upgraded prior to the CS 2000. 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. 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.		

MCS Management Server

The following table contains relevant upgrade information for this component.

MCS Management Server		
ATTENTION Due to the complexity of the upgrade for the MCS Management Server and RTP Media Portal product, Nortel requires that all customers contact their Nortel Customer Service representative to engage the appropriate Nortel Software Delivery team to perform this upgrade. There will be no service charges incurred for this activity.		
Applicable Solutions	**Estimated times**	**Documentation**
CHS IAW	60 minutes Install Oracle to disk. 15 minutes install 3.0 pool onto the MgmtSv 15 minutes back up the database 10 minutes to stop the System Manager and Database (RTP Media Portal remains in service) 5 minutes to stop the SysMgr processes 190 minutes to execute the Solaris upgrade CD 120 minutes to update the database 10 minutes to undeploy the Mgmtsvr and redeploy it with the new load 5 minutes to enter the license key	For upgrade procedures refer to MCS Management Server upgrade on page 1835 For rollback and other upgrade details, refer to *RTP Media Portal Basics NN10367-111* ***Note:*** MCS Management Server SN08 upgrade procedures were not available for publication. The procedures in this book are the same procedures that were available in SN07.

MCS Management Server
Service impacts The Solaris upgrade requires a service interrupting system reboot that requires approximately 10 minutes.
Comments Once the System Manager and Database are upgraded and brought back into service, each of the RTP Media Portals can be upgraded in turn.

RTP Media Portal

The following table contains relevant upgrade information for this component.

RTP Media Portal		
ATTENTION Due to the complexity of the upgrade for the MCS Management Server and RTP Media Portal product, Nortel requires that all customers contact their Nortel Customer Service representative to engage the appropriate Nortel Software Delivery team to perform this upgrade. There will be no service charges incurred for this activity.		
Applicable Solutions	**Estimated times**	Documentation
IAW CHS	7 hours 15 minutes ***Note:*** The following MCS components upgrade to SN08 (from MCS 2.0 to MCS 3.0) during this step: • RTP Media Portal • Database Module • System Management Console	For upgrade procedures refer to RTP Media Portal upgrade on page 1838. For rollback and other upgrade details, refer to *RTP Media Portal Basics*, NN10367-111 ***Note:*** Hardware upgrades from SUN Fire t1400 to SUN Netra 240 can only be done after the network is at SN08 and MCS 3.0. The hardware upgrade is documented separately. Refer to *RTP Media Portal Element Manager Hardware Upgrade (Sun T1400 to Sun N240)*, SSIP 0430

RTP Media Portal

Service Impacts

CAUTION

Upgrading all RTP Media Portals concurrently will cause a service outage.

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.

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 SN08 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.

Preparing for a Carrier Voice over IP Network 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 Required pre-upgrade procedures on page 47 before starting the end-to-end upgrade. Nortel Networks recommends that these pre-checks be performed as soon as an upgrade is scheduled.

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

ATTENTION

All Media Server 2000 Series commissioned offices must also contain a commissioned Integrated Element Management System (IEMS) network application in order to complete an upgrade to software release SN08 or greater.

An IEMS can be commissioned on a stand alone server or on the same SSPFS-based server as the CS 2000 Management Tools and Clients (CMT) application.

Offices that do not contain an IEMS prior to the upgrade must schedule to commission an IEMS during the upgrade.

CAUTION

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

CAUTION

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

Pre-upgrade procedures

A series of procedures are required before beginning a component network upgrade. The following table contains a summary of required pre-upgrade procedures. For additional information, refer to Preparing for a Carrier Voice over IP Network upgrade on page 46.

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: 1. Go to nortelnetworks.com and select **Technical Documentation**. 2. Under Other Resources, select **Search for Technical Bulletins**. 3. Enter your search criteria (for example, “RMRs”) and click **Search**. ***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	See above for information for finding RMR technical bulletins.

Table 1 Required pre-upgrade procedures

Requirement	Applicable Solutions	Documentation
3. Complete the Device Manager for Ethernet Routing Switch 8600 upgrade	All	Refer to Device Manager on page 86.
4. Complete the Ethernet Routing Switch 8600 (CS-LAN) upgrade	All	Refer to Ethernet Routing Switch 8600 on page 94.
5. Ensure all components are patch current	All	Refer to Carrier Voice over IP Network patching on page 1850. ***Note:*** Use the Regional Patch Selector (RPS) tool from nortelnetworks.com to determine which patches you require. Refer to Ensuring patch currency on page 50.
6. Ensure all patches for are available	All	Refer to Carrier Voice over IP Network patching on page 1850. ***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 50.
7. Complete all upgrade software delivery, planning and provisioning requirements	All	Refer to Software delivery overview on page 52.
9. Verify your lab or network against the hardware baseline for a release	All	Contact your Nortel customer support representative.

Table 1 Required pre-upgrade procedures

Requirement	Applicable Solutions	Documentation
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. Refer to Modifying a plan using the NPM on page 1985.
11. Complete the network and component backups	All	*Global ATM/IP Administration and Security*, NN10402-600
12. If adding a stand alone IEMS to the office install the server hardware prior to the upgrade	All except PT-AAL1	*Sun Netra 240 Physical Installation,* Installation Method –26-0598 ***Note:*** Commission the IEMS software during the office upgrade when instructed in the upgrade procedure.

OAM guidelines

Nortel Networks recommends that redundant Multiservice Data Managers (MDMs) be installed to ensure maintenance view of the Multiservice Switch element is maintained even when the element manager is being upgraded.

Parallel GWC upgrades are not recommended or supported. While it is possible to save time by loading all GWCs of a given GWC type and performing all the SWACTs at the same time, doing so is not recommended or supported for live office upgrades.

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.

Ensuring patch currency

How to check for the latest patches

Ensure that the baseline software is patch current and then that you have any required patches prior to starting the upgrade.

1) Go to http://www.nortel.com.

2) Click "Support & Training".

3) Click "Software Downloads".

4) Click "Communication Servers".

5) Click "Communication Server 2000".

6) Click "Tools".

To query for patches

1) Click "Pre Upgrade Patch Calculator".

2) Click "Pre Upgrade Patch Calculator Readme[readme]" for instructions.

Also refer to Carrier Voice over IP Network patching on page 1850

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 and procedures

Refer to Carrier Voice over IP Network patching on page 1850.

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 checks

Contact your Nortel customer support representative for the hardware baseline for your solution.

Software delivery overview

Introduction

In order to plan adequately for a Carrier Voice over IP software upgrade, the operating company must be aware of the total upgrade process, from the initial quote and order to the final delivery of the software. This section provides an overview of the software delivery processes. For more detailed information, contact your next level of support.

Status of current load

When considering an upgrade, and up to the time that the upgrade is implemented, customers must ensure that their current software load is up-to-date with respect to patches and maintenance releases. All components of the Carrier Voice over IP network must be patch current, and at the latest maintenance release prior to starting the end-to-end upgrade of the network.

When necessary, patches and maintenance releases are issued throughout the lifetime of the solution or component software load. Patches and maintenance releases are typically also included with a new software load. For details, refer to the sections Pre-production activities on page 54 and Patching and maintenance release activities on page 55.

Quoting and ordering

The operating company first requests a preliminary cost estimate, or a Request for Quote (RFQ). The Nortel regional sales group generates the quote using existing office data and information on feature packages and materials required.

After receiving the quote, the operating company can then order a new software load through a letter of intent with an accompanying purchase order.

For outside equipment manufacturer (OEM) components (for example, Cable MTA/CMTS, Mediatrix ISD) customers must order directly from original equipment manufacturers. This process is not covered in this document. However, Nortel provides definitive lists of the required materials.

Note: Where ordering falls within the remit of the operating company, Nortel must be made aware of lead times as these upgrades can impact other parts of the project.

Provisioning

Scheduling

The Nortel group develops and manages customer schedules based on both hardware and software parameters through the Nortel ordering system. First, a Request for Schedule (RFS) is generated that identifies several critical dates for events that must be performed at specific times to achieve successful software delivery. The RFS packages the product for both hardware and software to provide the customer with the total scheduling picture.

Carrier Voice over IP Solution Release gating hardware

Carrier Voice over IP Solution Release required hardware includes any hardware required in the Carrier Voice over IP office prior to the software delivery date. The three types of Carrier Voice over IP Solution Release required hardware are as follows:

- Release Gating - Hardware that is required on the component in question to allow the software upgrade to take place.
- Solution Gating - Hardware that is required on a component in order to make that component compatible with other components after they are upgraded.
- Feature Gating - Hardware that is required to support feature functionality. Although the absence of feature gating hardware will not affect the Carrier Voice over IP Solution Release load, it will affect the specific software feature, which will not work as expected.

All Carrier Voice over IP Solution Release gating hardware must be ordered (either on an S Suborder or customer provided), shipped, and installed prior to the application date for the new software to allow for sufficient hardware testing prior to the application and a sufficient interval to verify new hardware reliability.

Note: Refer to the relevant Carrier Voice over IP documents and upgrade support personnel for soak periods and ensure that these are observed. Ensure that all hardware soak periods are observed before software upgrades.

Operating company schedule acceptance

Once the software delivery dates have been confirmed through Nortel regional scheduling primes, the Regional Customer Service representative notifies the operating company of the schedule, usually by telephone. After a verbal acceptance of the scheduled dates, the regional representative sends to the operating company a confirmation letter identifying the dates and the scheduled sequence of events.

As a final acceptance, the authorized operating company representative signs the schedule and returns it to the Nortel group. This ensures that both the Nortel group and the operating company have an agreed schedule in writing.

Carrier Voice over IP Solution Release Polling

Each office scheduled for a new Carrier Voice over IP Solution Release load is polled at approximately seven weeks prior to the software delivery date, or sooner if the order is received earlier. The Carrier Voice over IP Solution Release Polling group first contacts the customer to request permission to poll the office, the correct user information and passwords, and then dials into the appropriate Carrier Voice over IP component to begin the session (note that IP addresses are required for all relevant components). Memory usage and correct Carrier Voice over IP Solution Release levels are verified on the switch. The results of the seven week polling session are submitted to the Regional Nortel Databases. This information is used by various software production and delivery groups who build and deliver the new software loads.

Note: At this time, all pertinent information for the whole suite of Carrier Voice over IP components is gathered, both in terms of hardware and software.

Order changes

Operating company changes to the software order must be included in an authorization letter to the Nortel group detailing the change. In general, the customer is allowed to make changes to the software order until the commencement of the upgrade process. However, as changes are made closer to the actual upgrade, the delivery schedule can be impacted to accommodate processing and ordering changes.

Pre-production activities

Pre-production activities are tasks performed immediately prior to cutting and dispatching the new software load. The following activities are required:

- Confirm the purchase order.
- Verify the job feature database (JFDB).
- Place the software order in the Software Load Information Database (SOLID) and set the production flag.

In addition to the preceding activities, which relate to producing the load, the following software delivery activities occur during the same time frame:

- Ship preliminary software media and documents to the site.
- Perform patching activities.

Preliminary tape and document shipment

Preliminary tapes and documents are shipped from Nortel at approximately 35 days before the scheduled insertion date. The following items are included:

- the full documentation suite on CD-ROM, which includes:
  - peripheral software release documents (regular peripheral module [PM] and extended multi-processor system based peripheral module [XPM])
  - software delivery ONP procedures guide for the CS 2000
  - individual component upgrade documents
- the full suite of SSR loads and associated maintenance releases including, solution component NCL tapes or CDs, solution component patch tapes or CDs, Non-res NCL tape
- software transmittal listings (hardcopy inventory listing of shipment, quantity of tapes and documents)
- software portfolio on Helmsman CD-ROM

Patching and maintenance release activities

Patches are software rewrites to existing software loads. Patches change only a small portion of a software package or piece of data in the switch as opposed to a software upgrade which changes all the system software. The following two types of patches exist:

- CC patches are written for software in the central control
- XPM patches are written for the software in the XPMs

An XPM Patch tape is included in the preliminary tape and documentation shipment. Loading the new PM and XPM software loads and patching the new XPM software loads must be completed by the operating company before the pre-application procedure (typically five days before the software application).

Certain components have Maintenance Releases associated with them. These releases are included in the initial dispatch of software for the components in question. If further Maintenance Releases subsequently become available, these will be shipped separately.

Normally, an Carrier Voice over IP office site is scheduled for patch downloading every 28 or 14 days, depending on the Carrier Voice over IP Solution Release level in the office and varying between the components of the office. If the office is scheduled to receive a new software load, it is taken off the Patching/Maintenance Release queue before the commencement of the software upgrades. All Patches and Maintenance Releases that are released after dispatch of the initial software shipment are handled by the regional software upgrade teams on an individual basis.

Patching activities

All released patches for the CS 2000 and applicable component loads are bound into the software load before the loadtape is cut and dispatched. An informlist is sent to the regional Nortel primes according to the patches present on the no-data load. Any additional patches required are handled on an individual basis over the upgrade.

Software delivery

The total solution-level upgrade covers multiple maintenance windows. Components are upgraded in a prescribed order with the core CS 2000 upgrade using the One Night Process (ONP). Various pre-application engineering and precheck activities are preformed as described in the sections that follow.

Pre-application engineering

At regular intervals, and also at various pre-defined points in the procedure, conference calls are held to ensure that an office is ready for a software upgrade. Through the pre-application procedure, various problems and issues that can prevent or impact the upgrade are identified and resolved. Unresolved problems are handed to the Nortel region for resolution.

The automated checks consist of programs run on the switch to perform the following activities:

- Verify the software and hardware.
- Load program files and modules required for the software upgrade.
- Check office data and tables.
- Negotiate a start time for the upgrade.
- Review office site tasks and responsibilities.

The day before the upgrade the final component review is conducted by the pre-application engineer. All issues and problems identified during previous prechecks must be resolved by the final office review.

Prechecks

Prechecks are performed on each component at the time of initial polling (for example, as soon as an order has been scheduled). The purpose of these prechecks is to highlight any current problems with the software or hardware.

A subsequent precheck is performed on each component the day before it is due to be upgraded to ensure that any issues highlighted by the previous precheck have been resolved. Furthermore, the final precheck brings to light any new faults that have appeared.

Responsibility for running prechecks lies with the group responsible for preforming the upgrade. Contact your software operations prime for a list of prechecks to run on each component.

Direct messaging

The USP to GWC messaging path is set to core bounce (CB) by default. From release SN07 onwards, direct messaging (DM) is the preferred configuration for IP solutions. ATM solutions (AAL1 and AAL2) continue to use core bounce.

Therefore for IP solutions, a CB to DM cutover must be carried out. The cutover must be performed in the following circumstances:

- in a new Carrier Voice over IP network with USP
- in an old Carrier Voice over IP network (04, 05, 06) upgraded to SN07
- in a network where a Fiberized Link Peripheral Processor (FLPP) is replaced by a USP

Impact of a software upgrade

In order to plan successfully for a Carrier Voice over IP software upgrade, the operating company must be aware of the impact of the upgrade on the existing condition of the office and its daily operations. This section describes the impact in the following areas:

- hardware
- service
- operations
- network
- workforce

Hardware impact

Hardware impact refers to the existing hardware in the Carrier Voice over IP office and any additional hardware that is needed in order to upgrade the office to a new software load. It also includes any hardware tests that are part of the software delivery process.

Identifying gating hardware

Carrier Voice over IP Solution Release required hardware includes any hardware required in the Carrier Voice over IP office prior to the software delivery date. The three types of Carrier Voice over IP Solution Release required hardware are as follows:

- Release Gating - Hardware that is required on the component in question to allow the software upgrade to take place.
- Solution Gating - Hardware that is required on a component in order to make that component compatible with other components after they are upgraded.
- Feature Gating - Hardware that is required to support feature functionality. Although the absence of feature gating hardware will not affect the Carrier Voice over IP Solution Release load, it will affect the specific software feature, which will not work as expected.

All Carrier Voice over IP Solution Release gating hardware must be ordered (either on an S Suborder or customer provided), shipped, and installed prior to the application date for the new software to allow for sufficient hardware testing prior to the application and a sufficient interval to verify new hardware reliability.

Installing gating hardware

If gating hardware is required for the software order, the operating company must liaise with its account team to ensure that the required orders have been placed.

> ***Note:*** Even where the customer is ordering hardware from sources other than Nortel, it is essential that Nortel is made aware of expected delivery times.

Once the orders have been placed and delivery dates have been confirmed, the customer must schedule personnel to install the new hardware. Nortel installation personnel can assume this task as a professional service, if the customer requests it.

All gating hardware must be installed before the scheduled software upgrade date. The customer must refer to the relevant hardware documentation to ensure that any recommended soak periods are complied with. During the soak period the new hardware must be monitored to ensure that no faults are present.

These conditions decrease the likelihood that the software upgrade will be impacted due to faulty or unstable hardware in the office. Operating companies must direct any question or deviation from these considerations to their Nortel regional support.

Restrictions on hardware changes

All non-upgrade related memory, network and peripheral module (PM) extensions/re-grades must be complete prior to the ordering of the software upgrade: no commissioning activities are supported after this event because of the complexity of the planned software upgrades. Any hardware change activity must be planned to complete prior to commencing the software upgrades or after the Carrier Voice over IP office has been upgraded in its entirety.

Switch maintenance

Normal switch maintenance is the operating company's responsibility. An office planning a software upgrade must have no system faults. Unresolved hardware faults can complicate and possibly prevent a successful Carrier Voice over IP Solution Release application.

Further to the basic switch maintenance activities, a review of monthly/yearly maintenance tasks must also be initiated and any outstanding items actioned accordingly.

Additional requirements

Operational site connections

Two operational connections are required for the CS 2000 switch. The connections must be foreign exchange lines into IOC 0 and IOC 1. If the connections are noisy, a backup connection line can be used. Operational connections allow access to the switch for the following purposes:

- polling to obtain memory "in use" and "total" counts, and inform lists
- Carrier Voice over IP Solution Release pre-application office check
- Carrier Voice over IP Solution Release software application

In addition, IP connectivity must be available for any other components that Nortel has been requested to upgrade as a professional service.

Note: Without a suitable level of connectivity to these components, Nortel is unable to carry out the upgrade of these components.

Foreign exchange voice lines

One voice foreign exchange line to the office must be equipped for communications between operating company personnel and the Carrier Voice over IP Solution Release application engineer during all software upgrades.

Service impact

Service impact refers to the switch activities that impact customer service during the software delivery process.

Call processing

During the application phase of the software delivery process, call processing is briefly suspended during the switch of activity (SWACT) from the old software load to the new software load. Since Automatic Message Accounting (AMA) recording also does not occur for 2 to 3 minutes after the SWACT, the SWACT is performed in the early hours of the morning, typically a low traffic period.

All 2-port stable calls (those calls already connected through the switch) are kept up, but 3-port calls are dropped. The number of calls kept up can be determined by observing the PSVD (preserved) field in the CPSYS maintenance administration position (MAP) level. Call processing for new call originations ceases at the start of the SWACT, and begins again 2 to 3 minutes after SWACT.

The customer is directed to explore the call processing implications to other components in the suite by referring to the end-to-end upgrade documents.

Hardware states

The new software load maintains the hardware status from the old load. Affected hardware includes peripheral modules (PM), signaling terminals (ST), inter-peripheral message link (IPML), carrier, network, link and junctor, input/output controller, console, magnetic tape drive, and disk drive units. Hardware units in the manual busy (MANB) state or system busy (SYSB) state are returned to service (RTS) or off-line (OFFL) by the applicator before the SWACT to the new software load. Hardware status discrepancies are checked between the old and new software loads.

Trunk states

Trunk states on the old software load are carried over to the new software load. Installation busy (INB), make busy (MB), and restricted idle (RES) trunks are restored to the same states on the new software load. A trunk in the lock-out state on the old software load are in an idle state until a trunk audit is run, which puts the trunk in a lock-out state on the new load.

Operations impact

Operations impact refers to the operating modes necessary for a software upgrade that normally are not encountered during day-to-day switch operation. Primarily, this is the time interval when the switch is out of sync (simplex mode) to accommodate software delivery procedures and tests.

Administrative activities

The operating company must notify the following operational, administrative, and maintenance centers connected to the Carrier Voice over IP office of an upcoming software upgrade:

- Network Operations Center (NOC)/Switching Control Center
- operator services
- engineering and administrative data acquisition system
- billing collection center
- any other support and special service centers
- emergency services (for example, police, ambulance)
- high profile customers

On scheduling of the software upgrades, offices with centralized automatic message accounting (CAMA) or local automatic message accounting (LAMA) must arrange with the site billing center for AMA validation tests.

Before the SWACT, during the upgrade of the CS 2000, the billing device independent recording package (DIRP) subsystem is rotated. Files are copied to disk volumes on either the IOP or the core manager, which ever is the preferred backup device. After the SWACT, the billing center polls the switch and verifies the format of the new billing. It is imperative that records of the tests made before the software upgrades are available to provide a comparison with the new records. For a more detailed review of billing activities, refer to the CS 2000 upgrade modules and the billing documents.

Call testing

At the time when the software upgrades are ordered, the customer must compile a list of all call scenarios supported by the switch. Furthermore, a test call plan must be created on a component basis for all those components involved in call processing. This call plan must include all critical call scenarios for the component in question and forms the basis for acceptance testing after the upgrade of that component.

It is imperative that the test call plan is validated on the day of the upgrade in order to validate that all call scenarios are currently operational.

Site access

Where site access is controlled (for example, by security personnel), the customer must ensure that the necessary authorizations have been obtained and arrangements made to ensure that visiting engineers can access the site.

Network impact

When a switch in a switching network is scheduled for a software upgrade, its arrangement and compatibility with other components in the network must be examined. Compatibility of the new Carrier Voice over IP Solution Release load with existing software levels in the other components is essential. If an incompatibility exists, each component must be upgraded in the proper order to avoid impacting the total network.

For example, in an Operator Centralization (OC) arrangement including both host and remote OCs, the host OC must be upgraded before the remote OC. If a remote OC is being scheduled for a software upgrade, the scheduling analyst must ensure that the host OC receives the upgrade first.

Workforce impact

Workforce impact refers to any changes to the customer workforce's normal duties caused by the upgrade-related tasks, for example, familiarizing with the relevant documentation, understanding when and where they are required on site.

Site preparation

On scheduling the software upgrades, Nortel sends a full suite of software loads and documents.

Nortel requests that the customer perform the following tasks prior to the software application date:

- Review the appropriate upgrade documents.
- Review any Product Notification Bulletins raised against the new software loads.
- Review the precheck document.
- Perform the prechecks for each component.
- Highlight resources required to perform the upgrade of each component.
- Understand where and when personnel are required on site.
- Draw up a schedule for the upgrade of each component.

Planning for a software upgrade

Introduction

This section provides advance planning information for operating companies with Carrier Voice over IP networks scheduled for conventional software upgrades. Information is intended to assist operating company managers, engineers, and planners in preparing for a Carrier Voice over IP software upgrade. Switch activities before, during, and after the upgrade are described.

Planning information is provided for the following areas:

- patching
- dump and restore
- pre-application procedures for all components
- software application (performed by Nortel or operating company)
- post-application activities for all components

Software delivery methods

For conventional software upgrades, the operating company is responsible for installing the new software load with the exception of the core, which remains a Nortel responsibility. As an additional service, Nortel can assume responsibility for upgrading certain components, providing that the relevant prechecks have been carried out satisfactorily. Both software delivery options use the same processes to install the software load.

The main difference between the two options is the performance of the pre-application and software application procedures. In an operating company-administered upgrade, the company performs both the pre-application procedure and the software application. In a Nortel-administered upgrade, a Carrier Voice over IP Solution Release Pre-Application Engineer performs the pre-application procedure in conjunction with a customer representative. A Carrier Voice over IP Solution Release Application Engineer performs the software application.

Operating company-administered software upgrades

For operating company-administered applications, the scheduling, provisioning, and production phases of software delivery remain primarily the same as the Nortel-administered software applications.

Technical support is provided by Nortel during the precheck and application phases of the job. A hotline number available to the operating company is answered by the same Nortel personnel who perform software applications. For a list of technical support contacts and telephone numbers, refer to your Nortel account team.

Note: For any emergency issues, the same process of contacting the Emergency Recovery team applies.

Scheduling requirements

When the operating company places an order for new software, it must decide who is to apply the software. No matter who performs the upgrade, Nortel schedules the application of the new software load. If the upgrade is Nortel-administered, application time slots are reserved on the schedule; however, for an operating company-administered upgrade, an application time slot is not reserved.

Note: Because of the various interdependencies of the different components and the diverse ownership, planning an overall upgrade requires both Nortel and the operating company to hold an initial review to ensure a plan within the boundaries of support that both parties can resource.

Documentation requirements

Operating companies must use the relevant documents to perform the Carrier Voice over IP Solution Release pre-application and application procedures. For a full list of documents, refer to *Carrier Voice over IP Quick Reference Guide*, NN10262-001.

The Nortel Software Delivery Bulletin System provides information to various user groups (both Nortel and operating company) concerning changes, alerts, additional information related to software delivery that has not yet be released or published in any documentation. The operating company must review any bulletins that impact the pre-application or application processes.

Training and certification requirements

Before the operating company begins application of software loads, company personnel must be certified by Nortel. This process involves training on the software pre-application and application procedures for the switch. The certification process involves the following activities for operating company personnel:

- observing the software application process as Nortel software application engineers apply software loads to in-service switches
- participating in a software application training seminar conducted by Nortel
- performing software applications while an Nortel application engineer observes

In addition to certification by Nortel, personnel must have Carrier Voice over IP switch training and hands-on switch experience.

Patching requirements

Any patches/maintenance releases are delivered with the software loads for each component.

Nortel-administered software upgrades

For a Nortel-administered software application, a Nortel application engineer dials into the switch on the application night. The applicator uses two dial-up data links: one for each side of the central control. In addition, a voice link with on-site operating company personnel is maintained to discuss progress of the application and to coordinate specific tasks necessary for the application.

The pre-application procedure and software delivery phases of the process are performed by Nortel.

Preliminary processes

Carrier Voice over IP Solution Release polling

As soon as the upgrades are scheduled, the Carrier Voice over IP Solution Release Polling group requests permission from the operating company to dial into the switch. In the polling session, Carrier Voice over IP Solution Release polling groups obtain the following information on the customer's switch:

- core information
  - inform list
  - office tables
  - DS and PS areas
  - DS and PS tables
  - Hardware Baseline
- components information
  - memory information (on various components - core manager, SAM21, CS 2000 Management Tools, UAS, APS, CS 2000)
  - hardware baseline information
  - software levels
  - initial checks also include log checks where appropriate, and an overview of current faults raised with Nortel (for example, Clarify Cases)

After the upgrade, the Carrier Voice over IP Solution Release Polling group requests permission from the operating company to perform a post-insertion polling session in order to obtain switch information on the new Carrier Voice over IP Solution Release. The post-polling session follows the same process, and records the same type of switch information as that used in previous polling sessions. Because of the addition of new feature packages, the new Carrier Voice over IP Solution Release information can differ greatly from that of the old Carrier Voice over IP Solution Release. Changes from the old Carrier Voice over IP Solution Release load to the new Carrier Voice over IP Solution Release load impact memory usage and the inform list.

Note: This happens several times as different components are completed and can coincide with pre-application sanity checks on other components.

The results of both polling sessions are recorded in the Regional Nortel database for use by other Nortel groups in the Carrier Voice over IP Solution Release process.

Pre-application procedure

The pre-application procedure is performed by the Nortel pre-application engineering group with an operating company contact. It consists of a series of verbal and automated verifications with site personnel and the operating company switch to ensure readiness for the software application.

The pre-application procedure starts with a kickoff call, and weekly meetings are held to chart progress. Any additional calls deemed necessary over intensive periods of activity, (such as the CS 2000 upgrade), must be agreed according to the accepted upgrade schedule.

Prior to the pre-application procedure, the operating company loads into the switch any program files and modules not resident in the old Carrier Voice over IP Solution Release load that are needed for the pre-application and application procedures. These are loaded from the Carrier Voice over IP Solution Release tools tape included in the preliminary tape and documentation shipment.

During the kick off meeting, the following details are finalized:

- methods of access to each individual component
- access protocol (for example, notifications to customer and security)
- schedule of works
- matters arising from hardware audit and prechecks

Final component reviews

The final phase of the pre-application procedure for any given component is the final component review. At one day prior to the software application, this review is conducted by the pre-application engineer in conjunction with the customer to determine if the component is ready to proceed with a Carrier Voice over IP Solution Release software application.

All issues and problems identified in the pre-application check must be resolved at the final component review. For example, any hardware highlighted by the initial prechecks as being required is reviewed. Any hardware that has not been installed or has a fault, will gate the component upgrade.

The conditions checked in the final component review can vary from one component to another. A typical review includes the following activities:

- Perform datafill sanity checks.
- Review logs.
- Verify that journal files have been handled according to procedures.
- Confirm the application start time.
- Ensure all problems are corrected and issues resolved.
- Review hardware.

After the final component review, the pre-application engineer completes parts of a pre-application report, supplying important information necessary for the Carrier Voice over IP Solution Release application. The pre-application report is forwarded to the assigned application engineer for the software application.

Post-software application activities

Monitor

Monitor refers to the phase of the software delivery during which the operating company observes logs and switch performance. This phase begins when the software insertion is complete. If technical assistance is needed, the customer must contact the next level of support.

Clarify Cases

Clarify Cases identify problems detected in the Carrier Voice over IP switch. The operating company must retest Clarify Cases opened on the previous software load. If the problem documented by the Clarify Case still exists in the new software load, the Clarify Case must be reopened on the new load within two weeks of the software application date. If the problem no longer exists on the new software load, the Clarify Case is closed.

Contingency plans

Contingency plans are used when an unexpected event occurs that prevents or has a potential negative impact on a successful software application. Contingency plans are used in only a small number of software jobs. The following definitions are used by Nortel to describe unsuccessful software upgrade procedures:

- Abort: Condition in which a software application is terminated after sync was dropped due to an unrecoverable error or malfunction, or when directed by the operating company. In a service-affecting abort, normal telephone operations are interrupted.
- Fail: Condition of a software application in which the customer or any of its subscribers experience any type of service degradation as a result of the software application.
- Re-schedule: Condition in which a scheduled software application is cancelled due to an unexpected problem or issue that has an impact on the success of the software application. This condition occurs after the production flag is set for the loadbuild process but before sync is dropped. The software application is then re-scheduled.

The following list includes some of the situations that can cause a software order to be re-scheduled:

- gating hardware not installed prior to making image tape
- insufficient memory installed or provisioned
- Distributed Processing Peripheral (DPP) firmware and software not updated
- journal file mishandled
- hardware extensions added after making image tape
- data changes during frozen image interval through unsupported means
- unexpected technical and maintenance problems in the office
- shipping problems with tapes and documents

The abort recovery procedure varies depending on how far the software application has progressed (for example, if the decision to abort occurs before or after the switch of activity). For detailed abort procedures, refer to the relevant documents.

Carrier Voice over IP Solution Release technical support (problem escalation and resolution)

Nortel has established a problem escalation procedure involving Carrier Voice over IP Solution Release technical support, to resolve any problems that can occur during a software application. Nortel senior engineers, specially trained in software delivery and experienced in dealing with software application problems, are present to support the Nortel application engineers during all software applications. The Carrier Voice over IP Solution Release technical support is provided in addition to the Nortel Technical Assistance Support (TAS) and Emergency Recovery groups.

The problem escalation procedure ensures problem resolution in a timely manner, while maintaining the highest level of service that is possible under a problem condition.

If a problem occurs during an application, execute the steps that follow to resolve the problem:

1 Identify the problem and determine if it is an E1 or E2 problem. (E1 problems result in system degradation or outage; E2 problems have the potential for system degradation or outage.)

If	Do
the problem is considered an E1 or E2 problem	step 8
otherwise	step 2

2 Contact Carrier Voice over IP Solution Release technical support for assistance.

3 Use the table that follows to determine your next step.

If	Do
a recovery strategy is available to resolve the problem within 10 minutes	step 4
otherwise	step 5

4 Use the table that follows to determine your next step.

If	Do
the problem is resolved within 10 minutes	no further action as the problem is resolved The steps taken to correct the problem are documented and all involved parties, operating company and Nortel personnel, are notified that the problem is resolved.
otherwise	step 5

5 Contact the next level of support for assistance.

6 Use the table that follows to determine your next step.

If	Do
the problem is resolved within the next 10 minutes	no further action as the problem is resolved The steps taken to correct the problem are documented and all involved parties, operating company and Nortel personnel, are notified that the problem is resolved.
otherwise	step 7

7 Escalate the problem to the Nortel duty manager and Carrier Voice over IP Solution Release Manager for further escalation. For all E1 conditions lasting more than 10 minutes, the Carrier Voice over IP Solution Release manager notifies the Carrier Voice over IP Solution Release production manager, Carrier Voice over IP Solution Release operations manager, Carrier Voice over IP Solution Release support manager, Nortel regional contact, and Director of Software Operations, for resolution and assistance from additional resources.

You have completed this procedure.

8 Escalate the E1 or E2 problem immediately to Carrier Voice over IP Solution Release technical support, and in addition, contact the Nortel Emergency Recovery group.

Emergency Recovery directs the problem resolution strategy, with the assistance of Carrier Voice over IP Solution Release technical support personnel. The Emergency Recovery personnel and operating company site personnel generate a customer service report (CSR) on the problem. The Carrier Voice over IP Solution Release operations manager is also notified of the problem.

Emergency Recovery personnel, Carrier Voice over IP Solution Release technical support, and operating company site personnel work together to resolve the problem.

You have completed this procedure.

Note: For E1 and E2 problems, recovery action by Nortel is immediate and continuous until the service level is restored to the pre-incident operation.

Tasks and timings

Planning and scheduling

The following list provides a task breakdown and estimated times for planning and scheduling an upgrade:

- Allow approximately 5 days to obtain network configuration and agree on timings with software fulfilment.
- Allow approximately 3 days to assign resources.
- Allow approximately 2 days to perform site readiness checks.
- Allow approximately 5 days to identify gating hardware.
- Order and install gating hardware, which varies in time depending on availability.
- Order and install third-party gating hardware, which varies in time depending on availability.
- Allow approximately 5 days to request software (CVoIP, Data, Enterprise Solution)

Upgrade tasks and timings

Section Component upgrade order on page 9 contains upgrade order tables with task summaries and estimated upgrade times for all the network components.

Customer acceptance tests

Allow approximately 8 days to run customer acceptance test suite.

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 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 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 CDROMs and documentation to the site
- Site polling by Nortel 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 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.

Monitor logs

CAUTION
Possible loss of service
Check the logs for CCA, SAM21 EM and Ethernet Routing Switch 8600 to make sure links are stable. Continue to monitor the logs until the day of SWACT.

Perform this activity according to site operating procedures.

SITE — At the ACTIVECM window

1 Enter the BCS update level.

```
> BCSUPDATE
```

2 Check the logs.

```
> LOGCHECK
```

3

ATTENTION
Do not proceed until all log activity is explained.

This procedure is complete.

Backing up Media Server 2000 Series files

When upgrading to software release SN08 or higher from a software release prior to SN08, perform a file backup prior to upgrading the Media Server 2000 Series node.

Before starting this procedure, review any documentation included with the software. The documentation included with the software may override or supplement this procedure.

CAUTION

Backing up the current load files must be performed prior to upgrading the server. These steps use the CLUI interface that is not available once the server is upgraded.

For increased security, the CS 2000 Management Tool, and SDM logins, are equipped with login timeouts. If at any point in the procedure 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.

Backing up Media Server 2000 files

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 this procedure until the ping commands indicate successful connections.

2 Log in 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

3 When prompted, enter your user ID and password.

4 Back up the files in the /data/loads/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 a user name and password that have been configured with emsadm authorization.

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 action retrieves a current copy of the INI file for each Media Server 2000 configured in the network.

Note: Each .ini file is backed up in a directory with the ip address of its associated Media Server 2010 node as the directory name. Only the last five backed up .ini files for the node are kept in this directory. Note the date of each .ini file to determine which file is the most recent. Also note the name of the most recent .ini file for use later in this procedure, for example, 2005-02-02_13:03:06.Board.ini.

5 Press “x” to exit the Media Server 2000 Series CLUI.

6 Enter the following on the command line.

```
cd /data/loads/ams
```

7 Create a backup directory with a descriptive name that includes the current date and the current release version (prior to the upgrade).

mkdir ams_bku_<today's date>_<release>

Example
mkdir ams_bku_20031031_7.0

8 Back up the files by entering the following commands.

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.

9 Each Media Server 2000 node has a directory containing a copy of its INI file. The directory name is the IP address of the Media Server 2000 node. Make a backup copy of each Media Server 2000 directory by repeating the following command at the command line for each Media Server 2000 node.

cp -pr <MS 2010 ip address> ams_bku_<today's date>_<release>

where <release> is the current release (prior to the upgrade)

Example
cp -pr 172.17.40.230 ams_bku_20040501_6.2

cp -pr 172.17.40.230 ams_bku_20040501_7.0

10 Access the backup directory you created in step 7 and verify that the files and directory are present.

Updating the Media Server 2000 Series trusted manager table

This procedure describes the process required to update the Media Server 2000 trusted manager table if an SN07 Media Server 2000 node existed in the network prior to the SESM upgrade. The trusted managers table was introduced in SN07, therefore this procedure is not required for releases prior to SN07.

CAUTION

Complete the pre-migration section of this document prior to upgrading the server. These steps use the CLUI interface that is no longer available after the server upgrade.

CAUTION

Deleting or adding the wrong entries in the trusted manager table can cause a communication loss to the Media Server 2000 node. Read this entire procedure before making any trusted manager table changes.

If communication with the node is lost during this procedure, but the node remains in service, then one of the following occurred:

- the machine used to access the Media Server 2000 node is not in the node's trusted manager list
- an SNMP community string mismatch exists

In either case, reload the node to resolve this problem as follows:

1. access the Media Server web interface
2. perform an INI file backup
3. edit and correct the trusted managers and/or snmp community strings

   Note: Set the community strings in the INI file to match those used for the Media Server 2000 CLUI or the IEMS (IEMS) Media Server 2000 Maintenance and Configuration Tool.

The community strings in the INI file must match those used by the Media Server 2000 CLUI or the IEMS Media Server 2000 Maintenance and Configuration Tool.

Updating the Media Server 2000 trusted manager table

At the Windows desktop interface

1 Log in to the CS 2000 Management Tools server using the root user ID and password.

2 Record the IP address on which the SESM application is running.

Example

```
# getpip.ksh
47.20.10.1
```

3

CAUTION

If deleting all entries from the trusted managers table, then delete the SESM IP as the last entry deleted from the table.

Record the IP address on which the IEMS application is running.

Note: The IEMS application frequently runs on a virtual IP, therefore the IEMS application may not be running on the physical external IP address.

```
# getpip.ksh iems
47.142.100.15
```

4 Launch the Media Server 2000 CLUI from the SESM node and list the trusted managers table.

```
# /opt/nortel/NTsesm/bin/ms2000.sh
**********************************************
Nortel Media Server 2000 Series Configuration Tool
**                version 2.05                **
**********************************************
```

5 Enter the user name and password when prompted.

```
Enter user name > iemslab
```

```
Enter password  >
```

The Media Server 2000 Series CLUI Main menu displays.

```
ORBWrapper orb initialized
*** 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)
>
```

6 Enter 2 to select the Node Maintenance and Configuration menu.

7 When prompted, enter the Media Server 2000 node IP address.

The maintenance and configuration Main Menu displays.

Note: The maintenance and configuration Main Menu shows the type of Media Server type based on the IP address entered in this step. This example uses an IP address for a Media Server 2010, rather than a Media Server 2020.

```
*** Main Menu for MS2010 at 47.142.134.127 ***
1) Maintenance Menu
2) Configuration Menu
x) EXIT
Enter Selection (1 - 2, x)
>
```

8 Enter 2 to select the Configuration menu.

The Main Configuration Menu displays.

```
***** Main Configuration Menu for MS2010 at
47.142.134.127 *****
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)
>
```

9 Enter 4 to select SNMP configuration and security.

The SNMP Configuration and Password Management Menu displays.

```
*** SNMP Configuration and Password Management
Menu for MS2010 at 47.142.134.127 ***
1) Setup Trusted SNMP Managers
2) Configuring SNMP Trap Destinations
3) Change SNMP Community String password
4) Change File Upload and Download user and
password
?) Help
x) EXIT
Enter Selection (1 - 4, ?, x)
>
```

10 Enter 1 to select Setup Trusted SNMP Managers.

The Trusted Mangers Configuration Menu displays.

```
*** Trusted Mangers Configuration Menu for
MS2010 at 47.142.134.127 ***
1) List configured trusted managers
2) Add a trusted manager
3) Delete a trusted manager
?) Help
x) EXIT
Enter Selection (1 - 3, ?, x)
>
```

11 Enter 1 to list the trusted managers.

A list of the trusted managers displays.

```
List of Trusted Managers
========================
IP = 47.142.10.1
```

```
IP = 47.142.100.15
IP = 47.140.4.0
```

Note: If there are no trusted managers, the following message displays.

```
There are no Trusted Managers defined
Press <enter> to continue
```

If the trusted manager table	Do
contains entries but does not contain the IEMS IP address	step 12
contains entries including the IEMS IP address	step 14
is empty	step 14

12 Add the IEMS application IP address to the trusted managers table.

Note: Another option, though not recommended, is to delete all entries in the trusted managers table and go to step 14. If choosing this option the SESM application MUST be deleted LAST.

13 Go to the IEMS application and launch the Media Server 2000 Configuration and Maintenance tool.

If the Media Server 2000 Configuration and Maintenance tool communicates with the device then the trusted manager table contains the correct IEMS IP address

14 This procedure is complete.

Upgrading Carrier Voice over IP Network Components

ATTENTION

The following sections contain upgrade procedures only. Conversions and installations are documented in Installation Methods. Software roll backs (downgrades) are documented in the component upgrade documents.

This document includes software procedures for possible components in a Carrier Voice over IP Network. Please disregard information about components that do not apply to your network.

Device Manager

The Device Manager is the first component operation performed in a network upgrade.

After upgrading the Device Manager

Perform the next required upgrade as follows:

Network	Device Manager applies to:	Next Upgrade
ATM	PT-AAL1, UA-AAL1, and PT-AAL2	Ethernet Routing Switch 8600 on page 94
IP	PT-IP, UA-IP, IAW, IAC, and CHS[a]	Ethernet Routing Switch 8600 on page 94
Tri-Modal	all applications	Ethernet Routing Switch 8600 on page 94

a.Includes IP International: CHS, IAC, PT-IP, and UA-IP

About the Device Manager

The Device Manager monitors and configures the Ethernet Routing Switch 8600.

Device Manager for Ethernet Routing Switch 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

Upgrading the Device Manager software is only required if currently on SN06.2. An upgrade is not required if currently on SN07.

Device Manager documentation

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

where:
X = current version of document

Technical document *Installing and Using Device Manager* also is available online from Technical Support on the Nortel 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

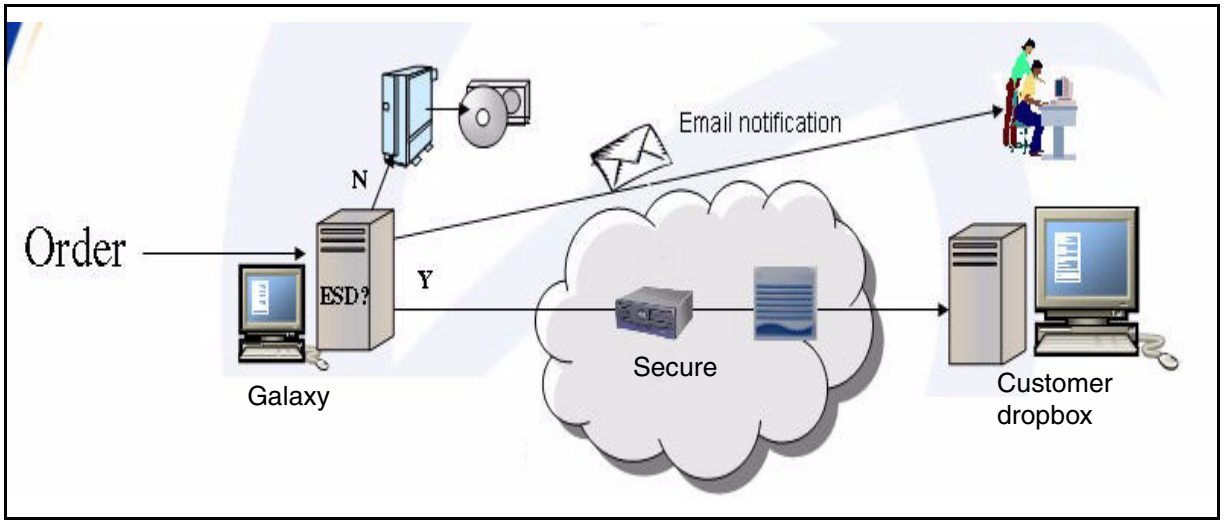
Software delivery methods

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.

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 Ethernet Routing Switch 8600 load for the CS-LAN. An example of the vaulted software load file for the Ethernet Routing Switch 8600 follows.

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

where

P86S00X0.X refers to the ordering code for the Ethernet Routing Switch 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.

Preparing the ESD version of the Device Manager software for an upgrade

At the workstation

1 Select the first step as follows:

If your core manager is	Do
an SDM/CS 2000 Core Manager	step 2
a CBM	step 5

2 Verify that the correct directory path, as shown in the following command, exists on the SDM/CS 2000 Core Manager:

>cd /swd/sdm/esd

If the above path	Do
does not exist and the response “not found” displays	step 3
exists	step 5

3 Create the directory path.

a Access the storage level from the SDM/CS 2000 Core Manager.

 # sdmmtc storage

b Add a logical volume in which to store the ESD file.

> esdadd

The system prompts you to enter a logical volume to be converted to the /swd/sdm/esd standard.

Note: Refer to procedure *Preparing the CS 2000 Core Manager for file transfer from the repository server* in the CS 2000 Core Manager section of this NTP for details on setting up a logical volume for conversion.

4 Ensure that the correct directory path has been accessed.

>cd /swd/sdm/esd

5 Use trivial file transfer protocol (TFTP) or file transfer protocol (FTP) to transfer the software load file as a binary file to the directory appropriate to the core manager platform.

- /swd/sdm/esd (SDM/CS 2000 Core Manager)
- /swd (CBM)

Note: Accessing the /swd link using the CBM is equivalent to accessing the /data/swd path.

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

cd /<directory>

where:
<directory> is /swd/sdm/esd for the SDM/CS 2000 Core Manager, or /data/swd for the CBM

7 Uncompress the software load file.

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

8 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 Ethernet Routing Switch 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

9 Access the new directory that contains the individual files.

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

10 Rename and move the Device Manager file for it to be recognizable for uncompression into the directory.

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

11 Reaccess the directory on the core manager that contains the Device Manager software file.

cd /swd

12 Uncompress the Device Manager file.

gzip -d device_mgr_XXXX.tar.gz

13 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.

14 The procedure is complete.

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

- all files in the original directory on the appropriate 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.

Preparing the CD version of the Device Manager software for an upgrade

At the workstation

1 Enter the following commands as the root user 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 TFTP or 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.

Ethernet Routing Switch 8600

Before upgrading the Ethernet Routing Switch 8600

Perform the required prerequisite upgrade as follows:

Note 1: For rollback procedures refer to *ATM/IP Solution-level Fault Management*, NN10408-900

Note 2: Prior to the SN08 software release, the Ethernet Routing Switch 8600 was known as Passport 8600.

Note 3: Upgrading the Device Manager is only required if currently on SN06.2. An upgrade is not required if currently on SN07.

Network	Ethernet Routing Switch 8600 applies to:	Previous Upgrade
ATM	PT-AAL1, UA-AAL1, and PT-AAL2	Device Manager on page 86
IP	PT-IP, UA-IP, IAW, IAC, and CHS[a]	Device Manager on page 86
Tri-Modal	all applications	Device Manager on page 86

a.Includes IP International: CHS, IAC, PT-IP, and UA-IP

After upgrading the Ethernet Routing Switch 8600

Perform the next required upgrade as follows:

Network	Ethernet Routing Switch 8600 applies to:	Next Upgrade
ATM	PT-AAL1, UA-AAL1, and PT-AAL2	Multiservice Data Manager (MDM) on page 215
IP	IAC- International, CHS - International, IAW, PT-IP and UA-IP[a]	Multiservice Data Manager (MDM) on page 215

Network	Ethernet Routing Switch 8600 applies to:	Next Upgrade
	IAC - North America and CHS - North America	Depending on configuration: CS 2000 Core Manager on page 303 Core and Billing Manager (CBM) 850 on page 455 (only if upgrading from SN07)
Tri-Modal	all applications	Multiservice Data Manager (MDM) on page 215

a.Includes IP International: PPT-IP and UA-IP

About the Ethernet Routing Switch 8600

The Ethernet Routing Switch provides optical Ethernet Virtual Private Networking (VPN) services to the network in a virtual router redundancy protocol (VRRP) configuration. The software upgrades are for routers that support the Succession Communication Server LAN (CS-LAN)

Upgrading the Ethernet Routing Switch 8600 Software for the CS-LAN

Introduction

This procedure upgrades Ethernet Routing Switch 8600 (formerly known as “Passport 8600") software on routers that support the Carrier Voice over IP (VoIP) Communication Server LAN (CS-LAN).

This procedure is only required if currently on SN06.2. An upgrade is not required if currently on SN07.

ATTENTION

Nortel urges users of this component upgrade to read thoroughly this Introduction, especially Important upgrade considerations, *before* attempting procedure Upgrading Ethernet Routing Switch 8600 software for the CS-LAN.

What’s new in this release

This section highlights the functionality introduced in this release.

- Beginning with release (I)SN08, the following branding conventions appear in this procedure:
  - — “Ethernet Routing Switch 8600" replaces “Passport 8600."
  - — “Carrier VoIP” replaces “Succession.”
- Moved procedure “Rolling Back the Ethernet Routing Switch 8600 Software for the CS-LAN” into NTP “ATM/IP Solution-level Fault Management,” NN10408-900.
- Added new steps when addressing the Universal Signalling Point Compact (USPc).
- Added Geographic Survivability impacts involving MS 2000 Series node, Call Agent, and STORM servers.
- Added steps addressing the RTP Media Portal, whereby the portal must be shut down gracefully to prevent it from accepting service requests during an Ethernet Routing Switch 8600 upgrade.

When to use this procedure

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

If the software upgrade must be reversed, use the procedure titled Rolling Back the Ethernet Routing Switch 8600 Software for the

CS-LAN to restore the original software load. Refer to NTP “ATM/IP Solution-level Fault Management,” NN10408-900.

Prerequisites

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

Important upgrade considerations

Ensure that you read thoroughly and understand the following points *prior* to beginning this software upgrade procedure.

- Note any existing alarms before executing this procedure. Once the upgrade is completed, verify that no additional alarms have been raised.
- 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).
- Beginning with SN07, this upgrade procedure addresses Ethernet Routing Switch 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).

- The Universal Signaling Point-Compact (USP-Compact) is addressed in this upgrade and the corresponding “Rolling Back the Ethernet Routing Switch 8600 Software for the CS-LAN”

procedures. However, no specific steps addressing the Universal Signaling Point (USP) are required in these procedures.

- For the procedure on rolling back software for the Ethernet Routing Switch 8600, refer to NTP “ATM/IP Solution-level Fault Management,” NN10408-900.

CAUTION
Potential network services disruption
To avoid network services disruption when upgrading the call processing unit (CPU) memory of an Ethernet Routing Switch 8600, perform the memory upgrade only when indicated in step 131. At this point, all traffic has been migrated to the other Ethernet Routing Switch 8600 chassis before the CPU is powered down for the memory upgrade.

Software upgrade strategy

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

Ethernet Routing Switch 8600 Router – Chassis 8010co Front View

In the VRRP configuration, one Ethernet Routing Switch 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 Ethernet Routing Switch 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 Ethernet Routing Switch 8600 software possible. Phased upgrades begin by upgrading the software on the slave router. Next, a switch of activity (SWACT) 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.

Supported solutions

The Ethernet Routing Switch 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 Ethernet Routing Switch 8600 does not carry call processing traffic. The PT-AAL1 solution includes the use of just the following Carrier VoIP components:

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

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

- step 1 to step 11
- step 119 to step 129
- step 183i and step 184

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, p80b3722)

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, p80a3722)

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 Ethernet Routing Switch 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, p80a3721)

<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:

<Ethernet_Routing_Switch_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

DNS entries

Due to the implementation of domain name service (DNS), the peer command option is not available unless you add the peer IP address in a new file called flash/etc/hosts.

You must create this file. No default file exists. Use a simple text editor to create it, similar to the text editor provided by the Ethernet Routing Switch 8600.

The following figure shows a sample of flash/etc/hosts file.

Sample flash/etc/hosts file of CPU in slot 5

```
198.202.188.44 inthp04.labpc.ernet.in labpc
206.236.134.194 inthp04.labpc1.ernet.in lacpc
198.202.188.174 ipksun05.accelar.wall.com ipksun05
198.202.188.34 dhcp.accelar.wall.com dhcpserver
127.0.0.6 peer cpuslot6
```

In the figure, the peer address corresponds to 127.0.0.6 for the CPU in slot 5. For the CPU in slot 6, the peer address would correspond to 127.0.0.5.

Note: To swap the CPU from slot 5 to slot 6, manually modify the address in the file.

Acquiring Ethernet Routing Switch 8600 software for the CS-LAN

Beginning with SN07, software for the Carrier VoIP Ethernet Routing Switch 8600 is stored in the Nortel 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 Ethernet Routing Switch 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.

ESD loads are compressed into a tar.gz file for delivery. Before transferring the load to the SuperNode Data Manager (SDM)/CS 2000 Core Manager or the Core and Billing Manager (CBM), the load files must be uncompressed.

Preparing the software file for an upgrade

Before starting an upgrade on the Ethernet Routing Switch 8600, perform the following software preparative measures:

- Move the Ethernet Routing Switch 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.

ATTENTION
The file must be copied to the /flash/ directory in lower case.

The following two procedures show how to prepare the Ethernet Routing Switch 8600 software for an upgrade:

- Use the first procedure when retrieving the Ethernet Routing Switch 8600 software from an ESD delivery.
- Use the second procedure when the Ethernet Routing Switch 8600 software is delivered on a CD.

Preparing the ESD version of the Ethernet Routing Switch 8600 software for an upgrade

At the workstation

1 Select the first step as follows:

If your core manager is	Do
an SDM/CS 2000 Core Manager	step 2
a CBM	step 5

2 Verify that the correct directory path, as shown in the following command, exists on the SDM/CS 2000 Core Manager.

```
> cd /swd/sdm/esd
```

If the above path	Do
does not exist and the response “not found” displays	step 3
exists	step 5

3 Create the directory path.

a Access the storage level from the SDM/CS 2000 Core Manager.

```
# sdmmtc storage
```

b Add a logical volume in which to store the ESD file.

```
> esdadd
```

The system prompts you to enter a logical volume to be converted to the /swd/sdm/esd standard.

Note: Refer to procedure *Preparing the CS 2000 Core Manager for file transfer from the repository server,* in the CS 2000 Core Manager section of this NTP for details on setting up a logical volume for conversion.

4 Ensure that the correct directory path has been accessed.

```
> cd /swd/sdm/esd
```

5 Use trivial file transfer protocol (TFTP) or file transfer protocol (FTP) to transfer the software load files to the directory appropriate to the core manager platform.

- /swd/sdm/esd (SDM/CS 2000 Core Manager)
- /swd (CBM)

Note: Accessing the /swd link on the CBM is equivalent to accessing the /data/swd path.

6 The procedure is complete. Continue to procedure Checking connectivity between the XA-Core and EIOP/HIOP and the Ethernet Routing Switch 8600.

Preparing the CD version of the Ethernet Routing Switch 8600 software for an upgrade

At the workstation

1 Enter the following commands as the root user to set up the directory structures on the core manager into which the Ethernet Routing Switch 8600 files are to reside.

```
cd /swd
mkdir pp8600
chmod 755 pp8600
cd pp8600
mkdir XXXX
```

where

XXXX
matches the new release of the Ethernet Routing Switch 8600 software (e.g., 3721)

```
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 Ethernet Routing Switch 8600 software files from the CD into the /swd/pp8600/XXXX directory of the CBM.

```
copy <filename> /swd/pp8600/XXXX/<new_filename>
```

where

filename
is the name of the file to copy

new_filename
is the name of the copied file in lower case

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 Ethernet Routing Switch 8600 software files from the CD into a temporary location on the CS 2000 Management Tools server.

```
cp <filename> /tmp/<filename>
```

8 Eject the CD.

```
eject cdrom
```

9 Use TFTP or FTP to transfer each of Ethernet Routing Switch 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 Ethernet Routing Switch 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 Checking connectivity between the XA-Core and EIOP/HIOP and the Ethernet Routing Switch 8600.

Note: It is important to check that the IOP, HIOP, or HCMICs connections are wired properly to the Ethernet Routing Switch 8600s because disabling the wrong links could isolate the Communication Server.

Checking connectivity between the XA-Core and EIOP/HIOP and the Ethernet Routing Switch 8600

At the workstation

1 Login to the CBM/SDM server (using telnet) and access the Core by typing.

`telnet CM`

2 Open table CMIPADDR by typing

`table CMIPADDR`

3 Display all fields in the table by typing

`range`

4 Display all tuples in the table by typing

`lis all`

A sample output of the CMIPADDR table follows.

```
TOP
KEY DATA
--------
GATEWAY 0 GW (192 168 0 1) 0
CMHOST 0 HOST (192 168 2 28) 22 0
CMHOST 1 HOST (192 168 2 29) 22 0
ETHRLNK 1 ETHR 15 REAR NONE (192 168 2 25) 22 (192 168 2 31) 22
(192 168 0 2) 0
ETHRLNK 4 ETHR 4 REAR NONE (192 168 2 24) 22 (192 168 2 30) 22 (192 168 0 3)
0
BOTTOM
```

5 Record the Physical IP address of each Ethernet connection.

- IOPs have four entries - ETHR 5 REAR, ETHR 6 REAR, ETHR 13 REAR, and ETHR 14 REAR
- HIOPs/HCMICs have two entries - ETHR 5 REAR and ETHR 14 REAR.

Each entry has two Physical IP addresses and one Gateway address. The Gateway address is the last column in table CMIPADDR.

Use the following table to record the Physical IP addresses.

XA-Core Ethernet Connection				
Slot (such as ETHR 5)	**First IP address**	**Second IP address**	**Connected to which 8600 (N=0 or N=1)**	**Third IP address**

6 Log into Ethernet Routing Switch 8600, chassis 0 and execute the following commands for the first row entries from the table in step 5:

```
ping <First_IP_address>
ping <Second_IP_address>
show ip arp info <First_IP_address>
show ip arp info <Second_IP_address>
```

If these IP addresses cannot be found in the ARP table, contact your next level of support for help in identifying the connections.

A sample output from the ARP table follows.

```
CSLAN-00:6# show ip arp info 192.168.2.25

================================================================================
                                    Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL(10 Sec)
--------------------------------------------------------------------------------
192.168.2.25    00:60:38:87:ff:b9    10    4/1   DYNAMIC  401

1 out of 265 ARP entries displayed

CSLAN-00:6# show ip arp info 192.168.2.31

================================================================================
                                    Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL(10 Sec)
--------------------------------------------------------------------------------
192.168.2.31    00:60:38:87:ff:b9    10    4/1   DYNAMIC  2160

1 out of 265 ARP entries displayed

CSLAN-00:6# show ip arp info 192.168.2.24

================================================================================
                                    Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL(10 Sec)
--------------------------------------------------------------------------------
192.168.2.24    00:11:f9:e7:10:fc    10   MLT 1   DYNAMIC 1065

1 out of 244 ARP entries displayed

CSLAN-00:6# show ip arp info 192.168.2.30

================================================================================
                                    Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL(10 Sec)
--------------------------------------------------------------------------------
192.168.2.30    00:11:f9:e7:10:fc    10   MLT 1   DYNAMIC 2160

1 out of 245 ARP entries displayed
```

Check the PORT column of the command output above to see if it lists a specific port (for example, 2/1) or shows “MLT”. Entries with a specific port value are directly connected to this chassis (chassis 0). Entries with “MLT” in the PORT column are connected to Ethernet Routing Switch 8600, chassis 1. In the

table in step 5, record which Ethernet Routing Switch 8600 chassis each IP address is connected to.

7 Repeat step 6 for each row in the table in step 5.

8 Execute the following command on each Ethernet Routing Switch 8600 chassis:

show vlan info ip

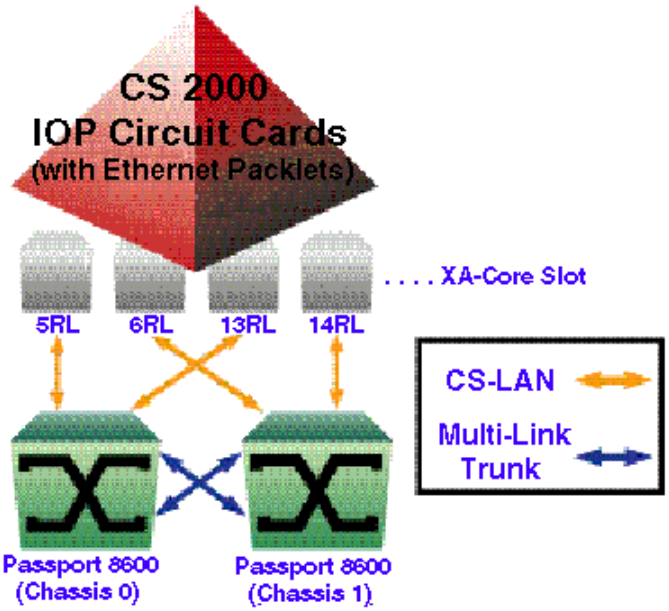
The third IP address in each row of the table in the step 5 should be a VLAN IP address in the output of this command. Also, each third IP address should reside on the same chassis as the first and second IP addresses on the same table row. If either of these conditions is not met, contact your next level of support.

A sample output of the show vlan info ip command follows.

```
================================================================================
                                    Vlan Ip
================================================================================
VLAN IP               NET              BCASTADDR REASM    ADVERTISE  DIRECTED
ID   ADDRESS          MASK             FORMAT    MAXSIZE  WHEN_DOWN  BROADCAST
--------------------------------------------------------------------------------
4    47.142.116.66    255.255.255.0    ones      1500     disable    enable
10   192.168.0.2      255.255.252.0    ones      1500     disable    enable
11   192.168.7.2      255.255.255.0    ones      1500     disable    enable
12   192.168.8.2      255.255.255.0    ones      1500     disable    enable
13   192.168.9.2      255.255.255.0    ones      1500     disable    enable
14   192.168.10.2     255.255.255.224  ones      1500     disable    enable
```

9 Verify the connections are wired according to the requirements stated below for the IOP and HIOPs/HCMICs

- An EIOP configuration can have a maximum of four connections; two to each Ethernet Routing Switch 8600 in any combination as shown in the following figure and table.



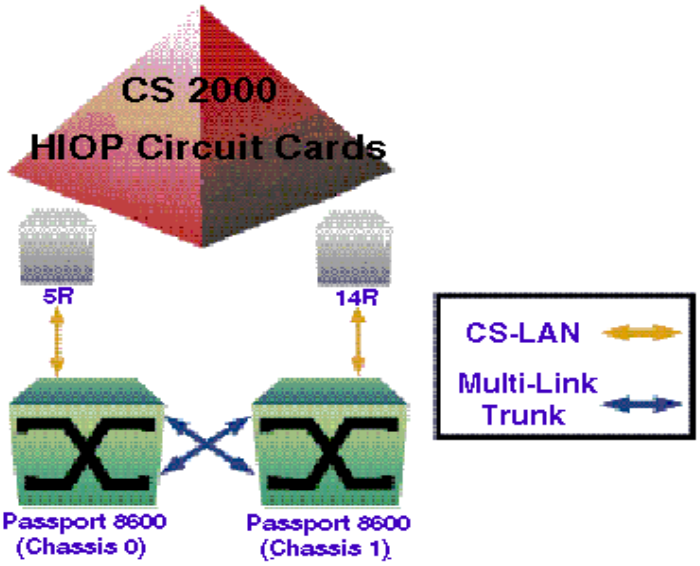
IOP with ETHRs	N = 0	N = 1
<slot1>	5	6
<slot2>	13	14

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 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

- An HIOP configuration has one HIOP connected to each Ethernet Routing Switch 8600 as shown in the following figure.



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

10 Proceed to Instructions on page 115 to upgrade the Ethernet Routing Switch 8600 software for the CS-LAN.

Instructions

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

The stepwise Upgrading Ethernet Routing Switch 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 SWACT. When this change of activity completes, the slave Ethernet Routing Switch 8600 takes on the master Ethernet Routing Switch 8600 function (the previous master Ethernet Routing Switch 8600 becomes the slave). The procedure then cycles back to the first set of steps to repeat the software upgrade process on the second Ethernet Routing Switch 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 recommends that all network element unit 0's subtend Ethernet Routing Switch 8600 Chassis 0. Likewise, all network elements unit 1's must subtend Chassis 1. The Upgrading Ethernet Routing Switch 8600 software for the CS-LAN procedure assumes the topology of your CS-LAN conforms to this recommendation.

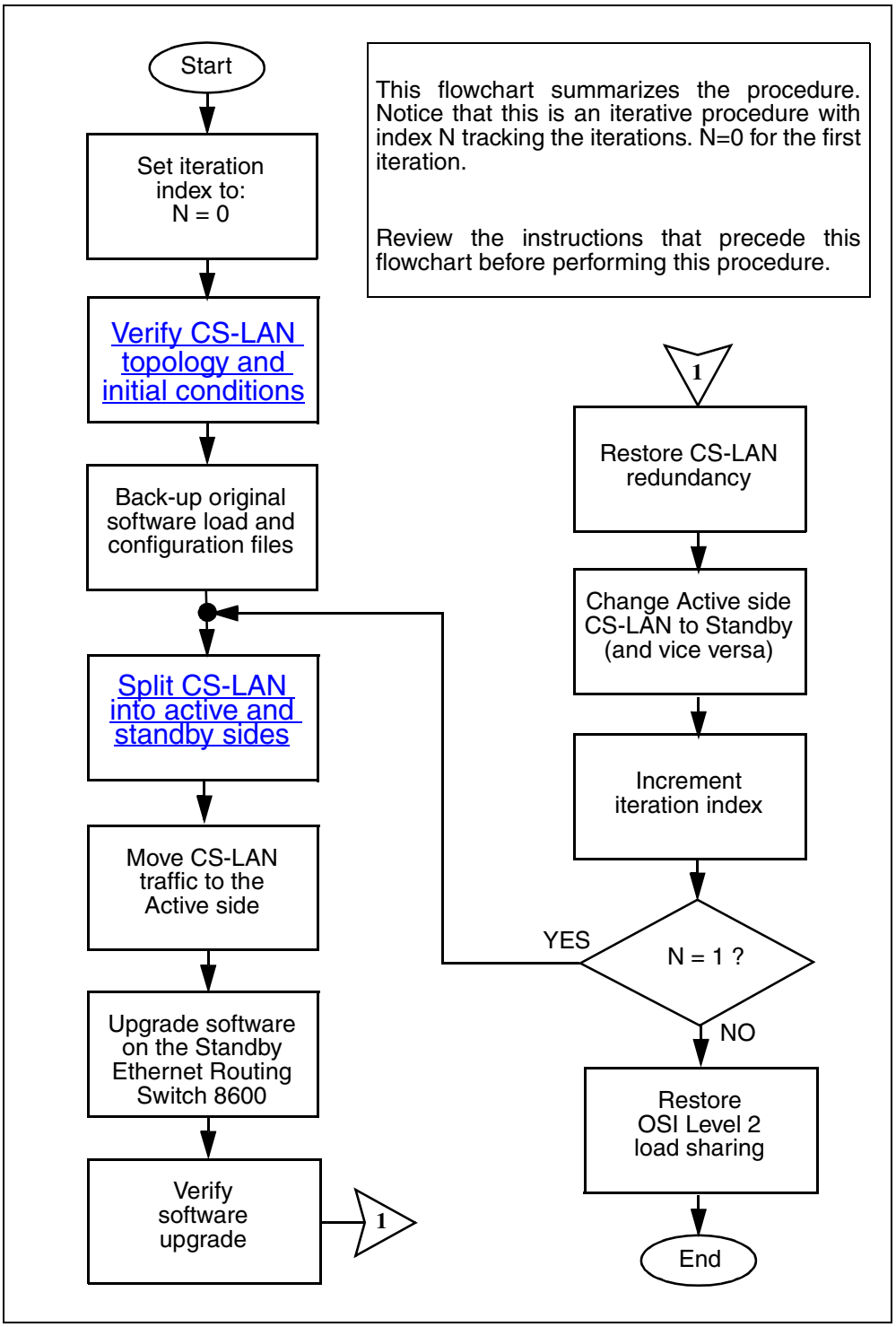
Note 1: If the topology of your CS-LAN does not conform to this recommendation, take this variation into account as you perform this procedure.

Note 2: If your solution includes Media Gateway 15000/7400[1], offload traffic from the slave to the master Ethernet Routing Switch 8600 before upgrading the slave software (see procedure Upgrading Ethernet Routing Switch 8600 software for the CS-LAN -- step 18 to step 33).

[1] Formerly known as Passport Packet Voice Gateways (PVG)

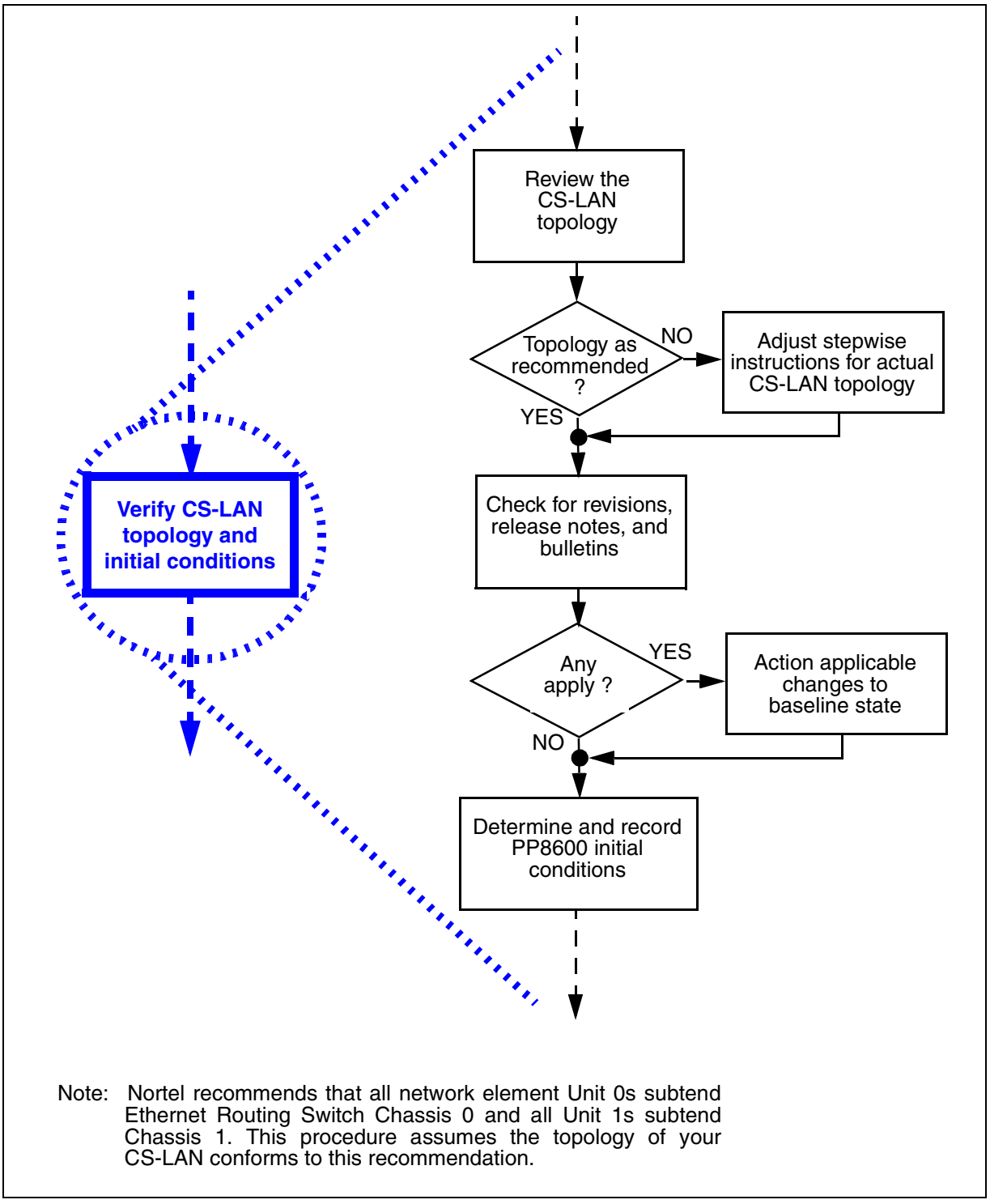
The following flowchart summarizes the overall software upgrade procedure.

Upgrading Ethernet Routing Switch 8600 software for the CS-LAN



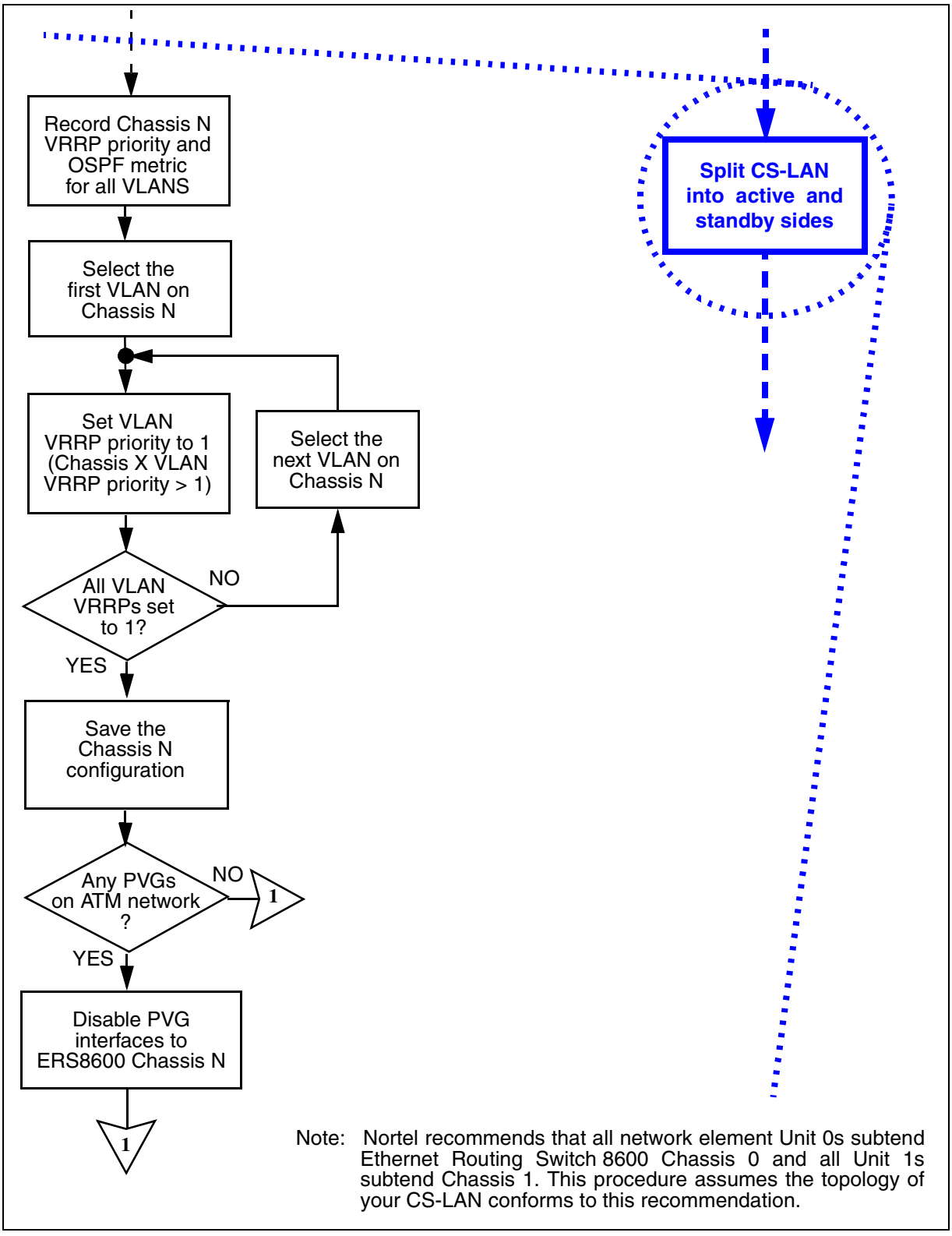
The following flowcharts provide additional detail to the Upgrading Ethernet Routing Switch 8600 software for the CS-LAN flowchart.

Verify CS-LAN topology and initial conditions



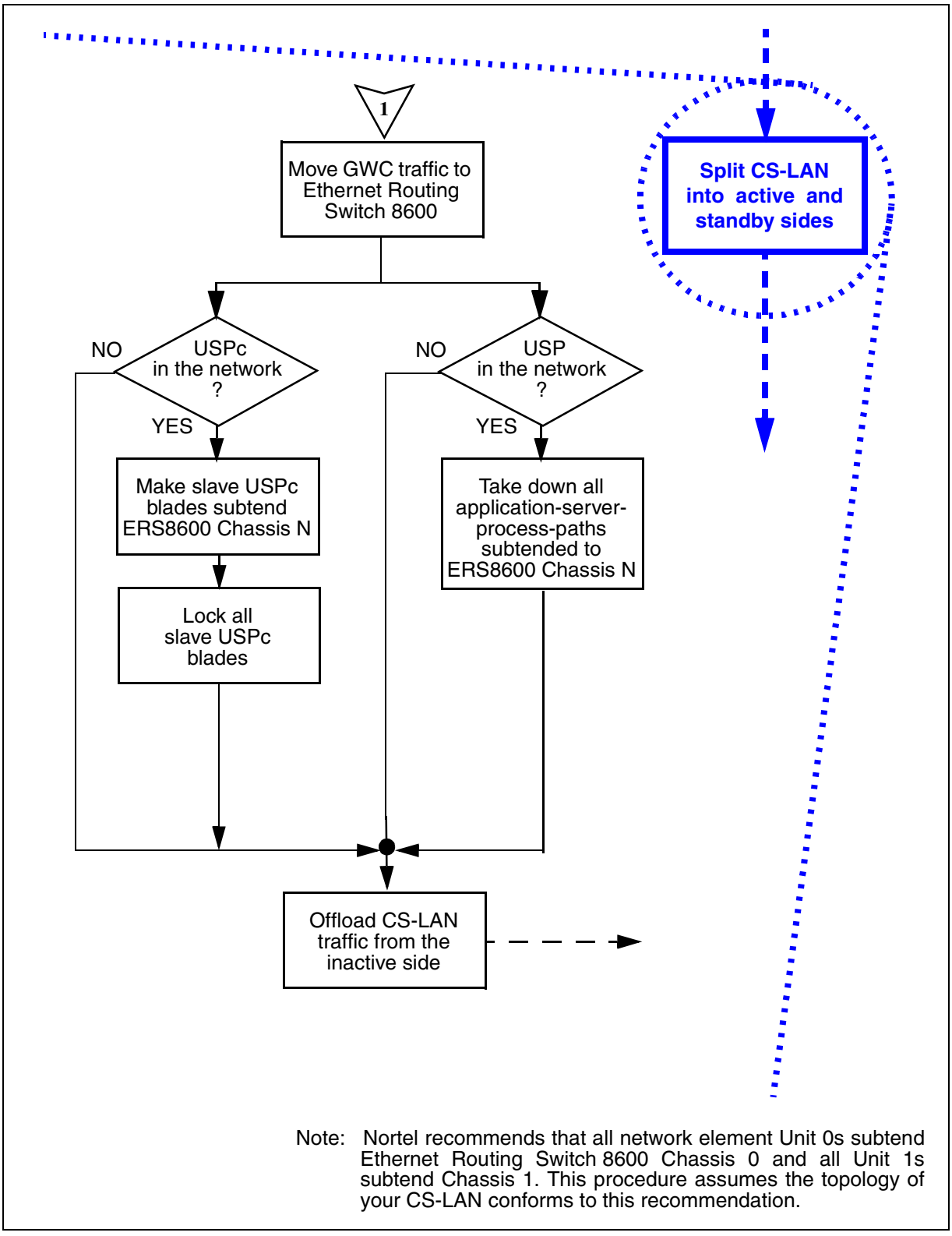
Note: Nortel recommends that all network element Unit 0s subtend Ethernet Routing Switch Chassis 0 and all Unit 1s subtend Chassis 1. This procedure assumes the topology of your CS-LAN conforms to this recommendation.

Split CS-LAN into active and standby sides



Note: Nortel recommends that all network element Unit 0s subtend Ethernet Routing Switch 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 (cont'd)



Note: Nortel recommends that all network element Unit 0s subtend Ethernet Routing Switch 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 Ethernet Routing Switch 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 website.

ATTENTION

The GUI/HMI graphics that support this procedure are current as of (I)SN08. 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 Ethernet Routing Switch 8600 software for the CS-LAN. The iterations (passes) proceed as follows:

- step 1 to step 11 establish initial conditions for the iterative procedure *to be completed on both CS-LAN routers*
- first pass (N=0) includes step 12 to step 184
- second pass (N=1) includes step 12 to step 186

Upgrading Ethernet Routing Switch 8600 software for the CS-LAN

ATTENTION

Ensure that you complete step 1 through step 11 on *both* routers before continuing to step 12.

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 Ethernet Routing Switch 8600s are in-service and use VRRP configuration.

b all network element Unit 0s subtend Ethernet Routing Switch 8600 chassis 0 and all Unit 1s subtend Ethernet Routing Switch 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 Ethernet Routing Switch 8600 master/slave conventions for this procedure.

Iteration	Slave Ethernet Routing Switch 8600	Master Ethernet Routing Switch 8600
First Pass	Chassis N = 0	Chassis X = 1
Second Pass	Chassis N = 1	Chassis X = 0

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

Use the Ethernet Routing Switch 8600 CLI to verify Ethernet Routing Switch 8600 initial conditions:

3 Verify the correct operation of the Ethernet Routing Switch 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 “Carrier VoIP 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
```

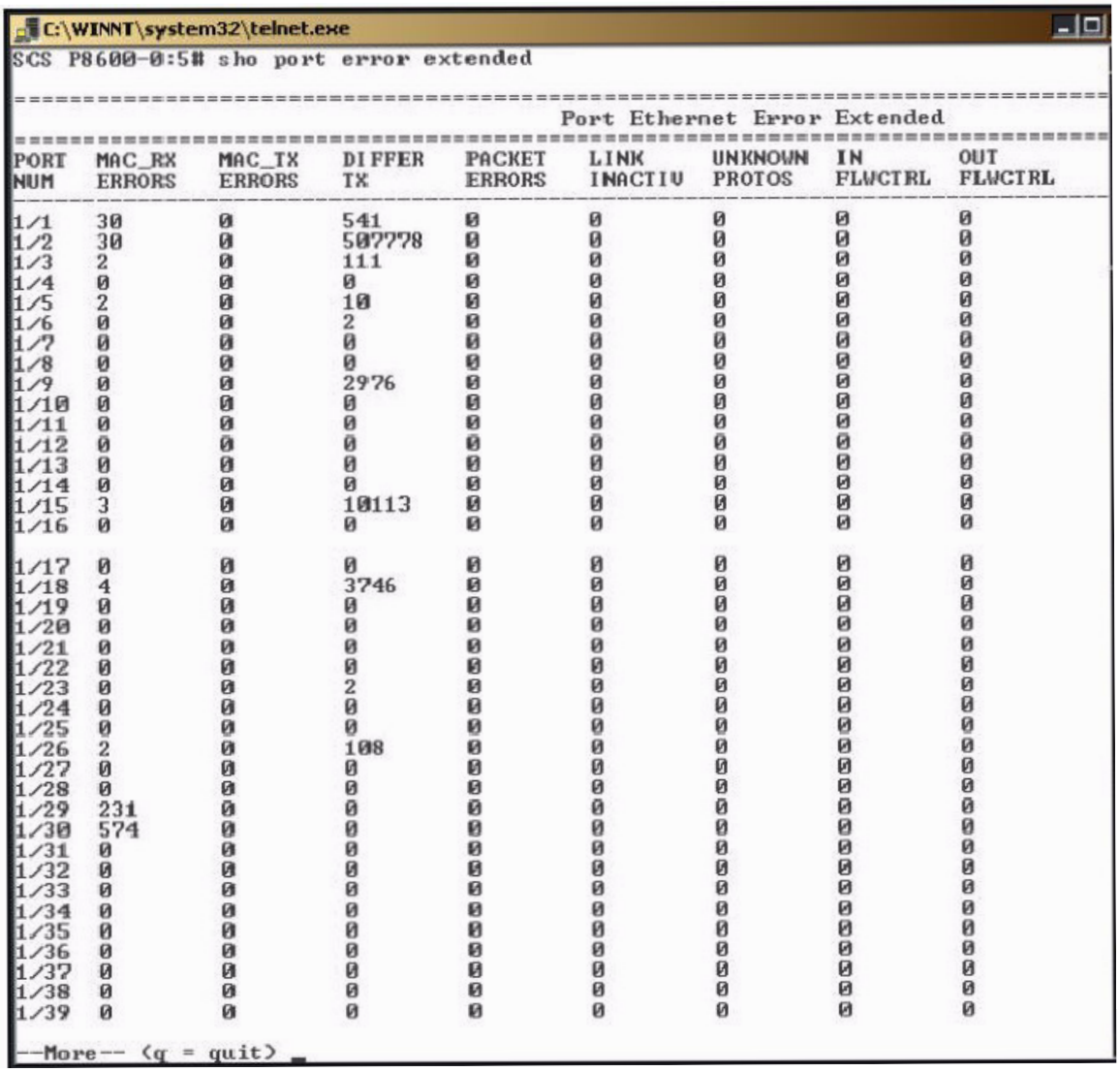
Compare the output for the IP ARP command against your expected configuration and correct any discrepancies.

4 Verify all subtending links and nodes as follows:

a Capture supplemental router port statistics by typing:

```
sho port error extended
```

Review the output for the extended port error command (see the following figure).



C:\WINNT\system32\telnet.exe

```
SCS P8600-0:5# sho port error extended

                                    Port Ethernet Error Extended
PORT  MAC_RX   MAC_TX   DIFFER  PACKET  LINK     UNKNOWN  IN      OUT
NUM   ERRORS   ERRORS   TX      ERRORS  INACTIV  PROTOS   FLWCTRL FLWCTRL
1/1   30       0        541     0       0        0        0       0
1/2   30       0        507778  0       0        0        0       0
1/3   2        0        111     0       0        0        0       0
1/4   0        0        0       0       0        0        0       0
1/5   2        0        10      0       0        0        0       0
1/6   0        0        2       0       0        0        0       0
1/7   0        0        0       0       0        0        0       0
1/8   0        0        0       0       0        0        0       0
1/9   0        0        2976    0       0        0        0       0
1/10  0        0        0       0       0        0        0       0
1/11  0        0        0       0       0        0        0       0
1/12  0        0        0       0       0        0        0       0
1/13  0        0        0       0       0        0        0       0
1/14  0        0        0       0       0        0        0       0
1/15  3        0        10113   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  4        0        3746    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        2       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  2        0        108     0       0        0        0       0
1/27  0        0        0       0       0        0        0       0
1/28  0        0        0       0       0        0        0       0
1/29  231      0        0       0       0        0        0       0
1/30  574      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
1/36  0        0        0       0       0        0        0       0
1/37  0        0        0       0       0        0        0       0
1/38  0        0        0       0       0        0        0       0
1/39  0        0        0       0       0        0        0       0

--More-- (q = quit) _
```

b capture router port error statistics by typing:

`sho port error main`

Review the output for the main port error command (see the following figure).

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
```

c Repeat steps 4a and 4b to capture error count increases.

5 Complete table Ethernet Routing Switch 8600 - Initial conditions by performing the commands in sub-steps step 5a through step 5e.

Ethernet Routing Switch 8600 - Initial conditions

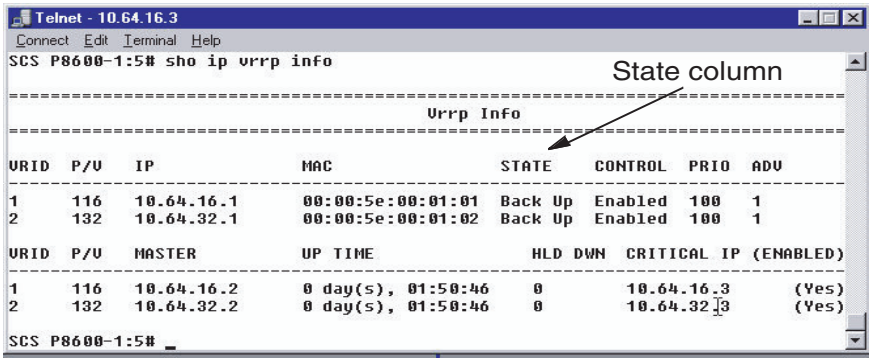
Status					
		Chassis 0		Chassis 1	
VID (P/V)	VRID	OSPF Metric (see Note)	VRRP PRIO	OSPF Metric (see Note)	VRRP PRIO
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Note: Only collect this metric if OSPF is configured on the Ethernet Routing Switch 8600.

a To display virtual router redundancy protocol information, 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 Ethernet Routing Switch 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 **VID (P/V)**, **VRID** and **PRIO** information for each CS LAN Ethernet Routing Switch 8600 Chassis 0 and 1 in the table.

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.

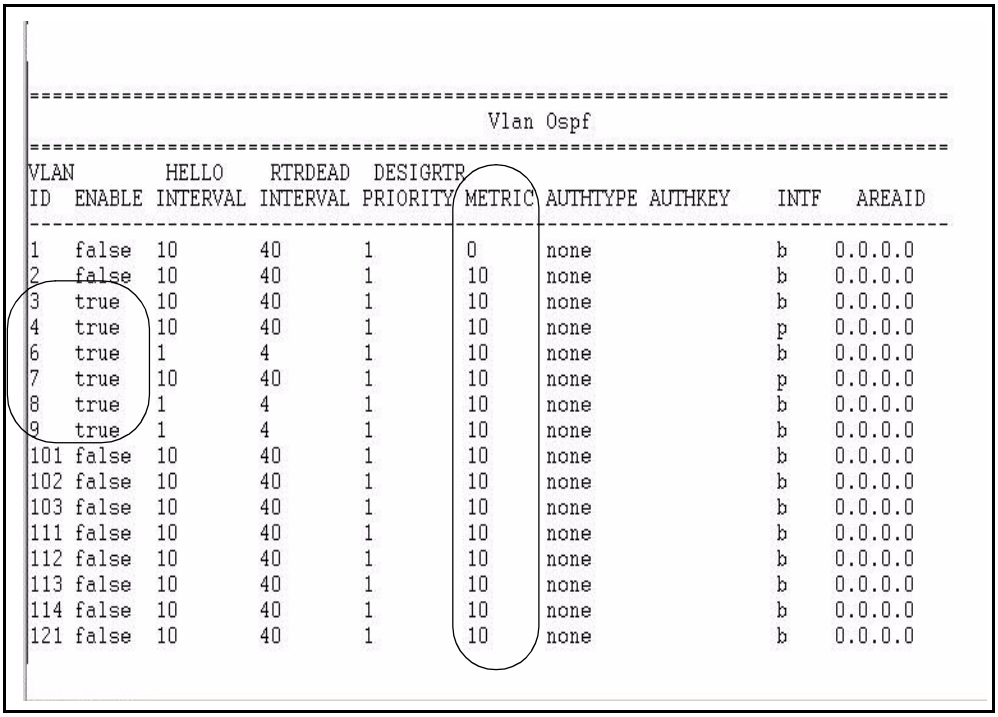
d Use the following table to determine the next step.

If	Do
OSPF is configured	Step e
otherwise	Step f

e Enter the following command to capture OSFP metrics for all VLANs that have OSPF ENABLE set to true, as shown in the following figure.

sho vlan info ospf

Output for the OSPF metrics appears.



```
================================================================================
                                    Vlan Ospf
================================================================================
VLAN        HELLO    RTRDEAD  DESIGRTR
ID  ENABLE INTERVAL INTERVAL PRIORITY METRIC AUTHTYPE AUTHKEY    INTF   AREAID
--------------------------------------------------------------------------------
1   false  10       40       1        0      none                b    0.0.0.0
2   false  10       40       1        10     none                b    0.0.0.0
3   true   10       40       1        10     none                b    0.0.0.0
4   true   10       40       1        10     none                p    0.0.0.0
6   true   1        4        1        10     none                b    0.0.0.0
7   true   10       40       1        10     none                p    0.0.0.0
8   true   1        4        1        10     none                b    0.0.0.0
9   true   1        4        1        10     none                b    0.0.0.0
101 false  10       40       1        10     none                b    0.0.0.0
102 false  10       40       1        10     none                b    0.0.0.0
103 false  10       40       1        10     none                b    0.0.0.0
111 false  10       40       1        10     none                b    0.0.0.0
112 false  10       40       1        10     none                b    0.0.0.0
113 false  10       40       1        10     none                b    0.0.0.0
114 false  10       40       1        10     none                b    0.0.0.0
121 false  10       40       1        10     none                b    0.0.0.0
```

Note: Standard results can reflect just the VRRP or OSPF in some VIDs. In some instances, it is also typical for both values to be collected.

f Use the following table to determine the next step.

If	Do
BGP is configured	Step g
otherwise	Step 6

g If BGP is configured on the Ethernet Routing Switch 8600, enter the following command:

```
sho ip bgp neighbor info
```

A sample output of the sho ip bgp neighbor info command follows:

```
BGP neighbor is 172.30.249.6 remote AS 65445, Internal Peer,
BGP state [Established]
remote router ID 192.168.223.103

                                    admin-state - BGP ON
                          connect-retry-interval - 120
                                   ebgp-multihop - disable
                                       hold-time - 6
                                  keepalive-time - 2
                              hold-time-configured - 6
                         keepalive-time-configured - 2
                                       max-prefix - 12000
                                   nexthop-self - enable
                               originate-def-route - disable
                                MD5-authentication - disable
                                    neighbor-debug - none
                                 remove-private-as - enable
                       route-advertisement-interval - 5
                             route-reflector-client - disable
                                   send-community - disable
                          soft-reconfiguration-in - enable

                               updt-source-interface - 0.0.0.0
                                             weight - 100
                                   Route Policy In -
                                  Route Policy Out -
BGP neighbor is 172.30.249.9 remote AS 65444, External Peer,
BGP state [Established]
remote router ID 192.168.223.101

                                    admin-state - BGP ON
                          connect-retry-interval - 120
                                   ebgp-multihop - disable
                                       hold-time - 6
                                  keepalive-time - 2
                              hold-time-configured - 6
                         keepalive-time-configured - 2
                                       max-prefix - 12000
                                   nexthop-self - enable
                               originate-def-route - disable
                                MD5-authentication - disable
                                    neighbor-debug - none
                                 remove-private-as - enable
                       route-advertisement-interval - 5
                             route-reflector-client - disable
                                   send-community - disable
                          soft-reconfiguration-in - enable
                               updt-source-interface - 0.0.0.0
```

h Record the IP addresses of all BGP neighbors and note whether the BGP peer is internal or external using the following table.

BGP neighbor IP address	Type of BGP peer (circle one)	BGP state = Established? (circle one)
	Internal/External	Y/N
	Internal/External	Y/N
	Internal/External	Y/N
	Internal/External	Y/N

i Verify that there is at least one (1) internal BGP peer and one (1) external BGP peer in the output of the command. If this condition is not met, contact your next level of support.

j Verify BGP state = Established on all BGP neighbors. If this condition is not met, contact your next level of support.

Use the Ethernet Routing Switch 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 Note the current image files.

8 Remove old image files from the /flash and /pcmcia directories as follows:

a Type

```
dir
```

b Delete all old image files, excluding the current image files, from the /flash directory by typing

```
remove /flash/<filename>
```

where

filename
is the name of the old image file, for example, p80aXXXX.img and p80bXXXX.img, where XXXX is the version of the software

c Delete all old image files, excluding the current image files, from the /pcmcia directory by typing

```
remove /pcmcia/<filename>
```

where

filename
is the name of the old image file, for example, p80aXXXX.img and p80bXXXX.img, where XXXX is the version of the software

9 Select the next step as follows.

If your CS-LAN	Do
is a dual CPU configuration per chassis	step 10
is a single CPU configuration per chassis	step 11

10

ATTENTION
Do not delete the current software load ***before*** successfully completing the upgrade. Current software must remain available as the secondary load to support Ethernet Routing Switch 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.X.X Release Notes.

Due to the implementation of DNS, the peer command option is not available unless you add the peer IP address in a new file called flash/etc/hosts.

You must create this file. No default file exists. Use a simple text editor to create it, similar to the text editor provided by the Ethernet Routing Switch 8600.

ATTENTION

Refer to section Text conventions on page100 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. Enter the following two commands:

Note: Before entering the sav config command, ensure sufficient free space exists in /flash (20% of total /flash size) to accommodate the configuration file.

```
sav config
```

```
sav bootconfig
```

For Ethernet Routing Switch 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. Enter the following two commands:

```
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 Ethernet Routing Switch 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 10b through step 10f.

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, for example p80a3320.img

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 Ethernet Routing Switch 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 Ethernet Routing Switch 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 Ethernet Routing Switch 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 12.

11

ATTENTION

Do not delete the current software load ***before*** successfully completing the upgrade. Current software must remain available as the secondary load to support Ethernet Routing Switch 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:

Note: Before entering the sav config command, ensure sufficient free space exists in /flash (20% of total /flash size) to accommodate the configuration file.

```
sav config
```

```
sav bootconfig
```

The Ethernet Routing Switch 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 11b through step 11f.

b Back up the software image file. Type:

```
copy /flash/<oldload> /pcmcia/
```

where

oldload
is the original software image filename, for example p80a3320.img

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 Ethernet Routing Switch 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 Ethernet Routing Switch 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 Ethernet Routing Switch 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 12.

Note: If upgrading the CS-LAN software in a PT-AAL1 solution, skip to step 119.

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

12

ATTENTION
Ensure that you have completed step 1 through step 11 on *both* routers during the first pass before continuing with this upgrade procedure.

Make sure that Ethernet Routing Switch 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 Ethernet Routing Switch 8600 Chassis N **<prio>** to 1 makes it slave (Chassis X **<prio>** is greater than 1 making it the master).

b Repeat substep a for each VLAN provisioned on the router.

c Use the following table to determine the next step.

If	Do
OSPF is configured	Substeps d and e
BGP is configured	Substep f
both OSPF and BGP are configured	Substeps d through f

d Set the OSPF priority to 1000 by typing

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

e Repeat substep d for each VLAN provisioned on the router.

After the VRRP priority and OSPF priority have been set for all provisioned VLANs, go to step 13. However if BGP is configured, continue with the next step.

f Repeat the following command for each external BGP neighbor entry recorded in the BGP neighbor address table in Upgrading Ethernet Routing Switch 8600 software for the CS-LAN, step h on page 129.

```
config ip bgp neighbor <external BGP neighbor
IP address> admin-state disable
```

g Check that the default route in the Ethernet Routing Switch 8600 route table correctly points to the master Ethernet Routing Switch 8600 typing:

`show ip route info`

A sample output of the show ip route info command follows:

```
MetroB-2:5# show ip route info

================================================================================
                                    Ip Route
================================================================================
            DST             MASK            NEXT COST VLAN  PORT PROT AGE TYPE PRF
--------------------------------------------------------------------------------
        0.0.0.0         0.0.0.0   172.30.249.12    1  402  -/-   BGP   0 IB    45
      10.21.0.0   255.255.255.0       10.21.0.1    1   72  -/-    LOC   0 DB     0
      10.22.0.0   255.255.255.0       10.22.0.1    1   73  -/-    LOC   0 DB     0
      10.54.0.0   255.255.255.0       10.54.0.1    1   54  -/-    LOC   0 DB     0
      10.55.0.0   255.255.255.0       10.55.0.1    1   55  -/-    LOC   0 DB     0
     10.240.0.3 255.255.255.255     10.250.0.10   20  100  -/-  STAT   0 IB     5
     10.240.0.4 255.255.255.255     10.250.0.26   20  101  -/-  STAT   0 IB     5
     10.250.0.0 255.255.255.240      10.250.0.6    1  100  -/-    LOC   0 DB     0
    10.250.0.16 255.255.255.240     10.250.0.22    1  101  -/-    LOC   0 DB     0
     30.30.30.0   255.255.255.0      30.30.30.1    1    2  -/-    LOC   0 DB     0
   172.18.181.0 255.255.255.128    172.18.181.1    1  200  -/-    LOC   0 DB     0
   172.30.249.8 255.255.255.248    172.30.249.9    1  402  -/-    LOC   0 DB     0
   172.30.254.0 255.255.255.252    172.30.254.1    1  240  -/-    LOC   0 DB     0
 172.30.254.192 255.255.255.192  172.30.254.193    1  260  -/-    LOC   0 DB     0
192.168.223.101 255.255.255.255 192.168.223.101    1    0  -/-    LOC   0 DB     0
```

The IP address in the NEXT field of the default route entry (DST = 0.0.0.0) should be the IP address of the BGP internal peer recorded in the BGP peer address table in Upgrading Ethernet Routing Switch 8600 software for the CS-LAN, step h on page 129. If this condition is not met, contact your next level of support.

13 Save the new Ethernet Routing Switch 8600 Chassis N configuration by typing:

Note: Before entering the sav config command, ensure sufficient free space exists in /flash (20% of total /flash size) to accommodate the configuration file.

`sav config`

This updates the new Ethernet Routing Switch 8600 configuration so that VRRP settings are maintained after any subsequent reboot.

14 Select the next step as follows:

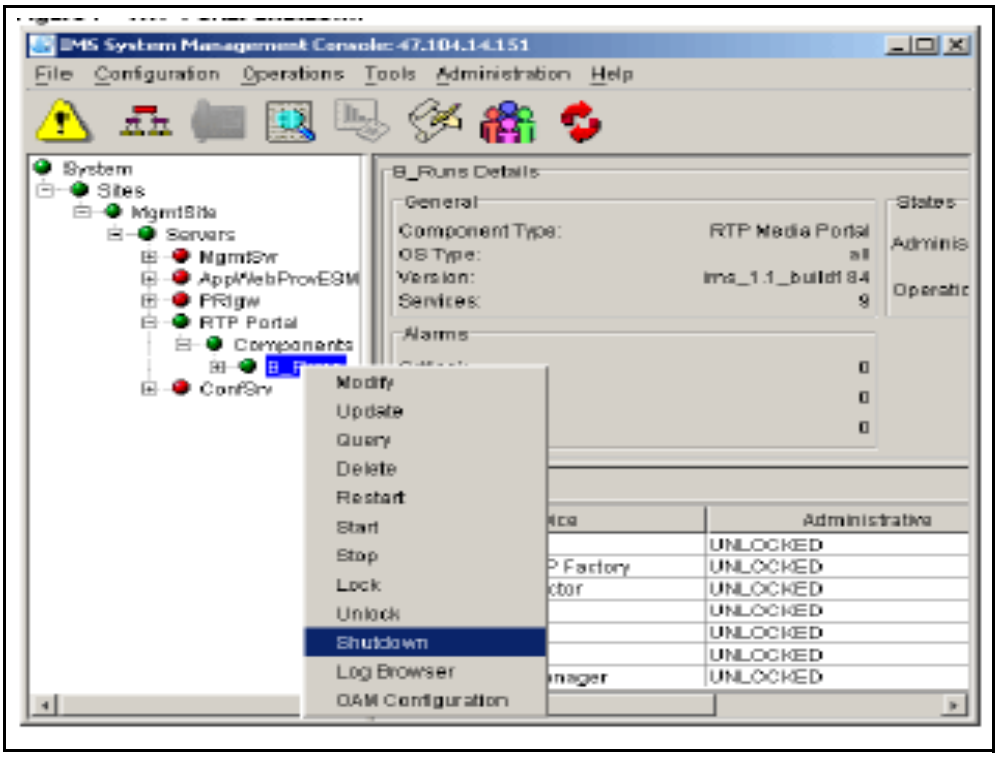
If your configuration includes	Do
multiple RTP Media Portals directly connected to the ERS 8600	step 15
does not include an RTP Media Portal	step 18

Use the System Management Console to shut down the RTP Media Portal connected to Chassis N to prevent it from accepting new service requests

15 In the System tree, right click on the target RTP Media Portal component.

Note: Ensure you are addressing the port that is connected directly to the Ethernet Routing Switch 8600.

16 From the pop-up menu, select **Shutdown** as shown in the example that follows.



Note: Alternately, the **Shutdown** command is available from the pull-down Operations menu.

A confirmation window appears.

```
Shutdown will affect the operations of this
component.
Do you want to continue?
```

17 Click the Yes button.

The RTP Media Portal shuts down gracefully and transitions into a LOCKED state when the last active media session ends. (Refer to the General Information area of the System Management Console.)

18 Select the next step as follows:

If your CS-LAN:	Do
includes ATM PVGs directly connected to the Ethernet Routing Switch 8600 (i.e., a non-VR solution)	step 19
includes PVGs connected by Gig Ethernet (GigE)	step 34
does not include PVGs	step 34
includes ATM interfaces connected to a PVG 15000 chassis running VR or VrAp	step 34

Note 1: The following steps (step 19 to step 33) offload PVG traffic from the Ethernet Routing Switch 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

19 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 Ethernet Routing Switch 8600 CLI to verify that the PVGs are set up redundantly

20 Check the VLAN configuration file by typing the following command on each Ethernet Routing Switch 8600 chassis:

```
sho config module vlan
```

This command outputs all VLANs provisioned on the Ethernet Routing Switch 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 Ethernet Routing Switch 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 26.

21 Check the routing table information for each Ethernet Routing Switch 8600 chassis as follows:

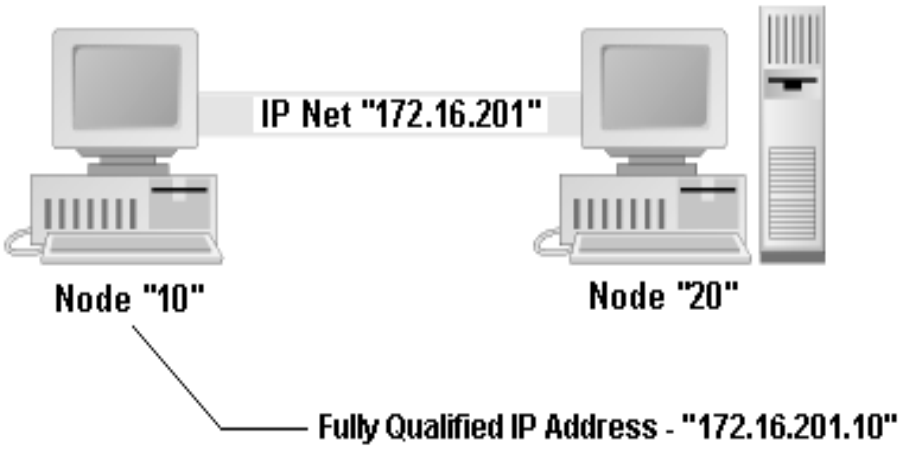
a Type:

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

where

x.y.z
specifies the IP Net address provided at step 19

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 Ethernet Routing Switch 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 Ethernet Routing Switch 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
```

ATTENTION

The routing information under the PROT column heading should indicate either VSP subnet LOC or OSPF.
If both Ethernet Routing Switch 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 Ethernet Routing Switch 8600 must be OSPF (LOC for Chassis X). See step 28 for details on forcing compliance to this requirement.

b repeat sub-step a for each VSP VLAN on the Ethernet Routing Switch 8600 Chassis N

c repeat sub-step a and sub-step b for Ethernet Routing Switch 8600 Chassis X.

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

22 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
```

23 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.

24 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 Ethernet Routing Switch 8600s

25 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 24*. If 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 24*. If is not identical, contact your next level of support.*

26 Check the physical connections between each PVG ATM interface and their related Ethernet Routing Switch 8600s.

Note: See step 20 for the Ethernet Routing Switch 8600 local route tables for the VSPs to be offloaded and verify the fiber connectivity between the PVGs and Ethernet Routing Switch 8600s. Refer to your engineering guidelines for additional information.

Use the PVG CLI to disable the ATM interface to the Ethernet Routing Switch 8600 undergoing the software upgrade.

27 Select the next step as follows (refer to step 21):

If all VSP VLANs for Ethernet Routing Switch 8600 Chassis N are	Do
OSPF (see Note)	step 34
Anything except OSPF	step 28

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.

28 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 Ethernet Routing Switch 8600 Chassis N by typing:

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

where

slot
is the slot number of the ATMIF blade

sonetif
is the Sonet interface on the ATM blade

Note: This command results in Sonet layer ALARMS.

c Record all locked Sonet interfaces.

29 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 AtmIf/141 (see step 25) to AtmIf151.

```
+=====+====+--------------------+------
|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 AtmIf/141 (see step 25) to AtmIf/151.

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

Use the Ethernet Routing Switch 8600 CLI to verify the IP route table for the offloaded VSP VLANs

30 Display the routing table for both Ethernet Routing Switch 8600s by typing:

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

where

x.y.z
is the IP Net address (see step 21)

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

31 Select the next step as follows:

If switchover of all VSPs is	Do
incomplete (i.e., not all VSPs switched over)	step 28
complete (i.e., all switched over)	step 32

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

32 Unlock all Sonet ports locked at step 28 by typing:

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

where

slot
is the slot number of the ATMIF blade

sonetif
is the Sonet interface on the ATM blade

Use the Ethernet Routing Switch 8600 CLIs to check the IP route tables

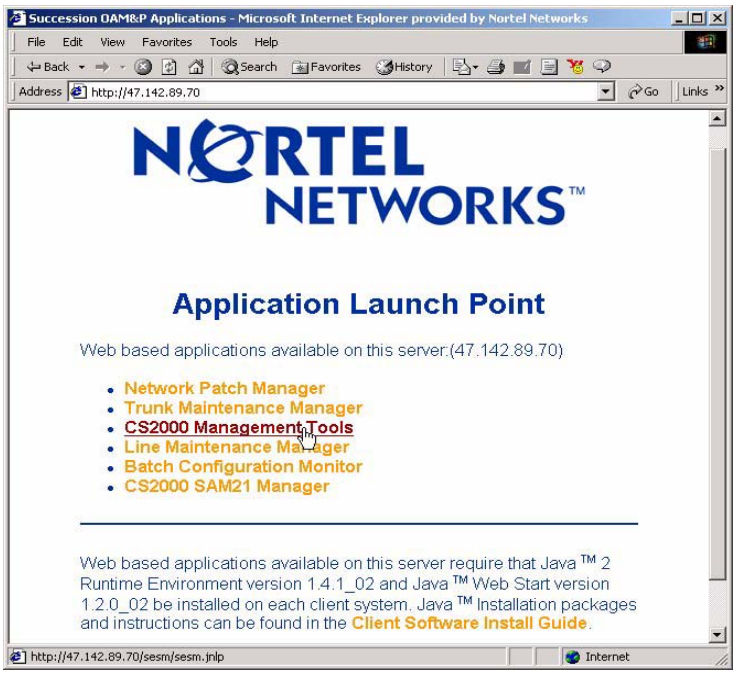
33 Make sure all VSP VLANs remain OSPF on Chassis N, and LOC on Chassis X by typing:

```
sho ip route info ip 172.16.201
```

The routing information under the PROT column heading must indicate OSPF for all VSP VLANs on Ethernet Routing Switch 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 Ethernet Routing Switch 8600 inactive:

34 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 and go directly to the CS Management Tools GUI. Continue from step 36.

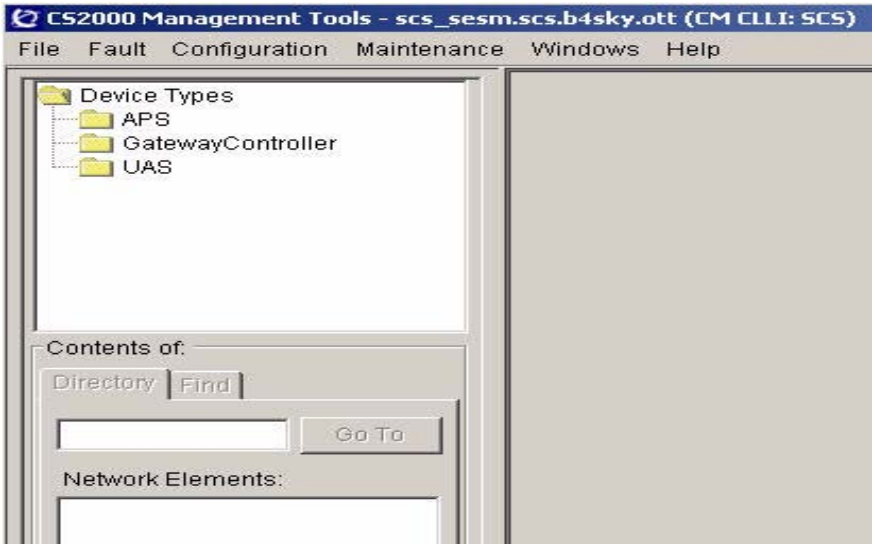
35 Click on the CS2000 Management Tools link.

The Login window appears.

36 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).

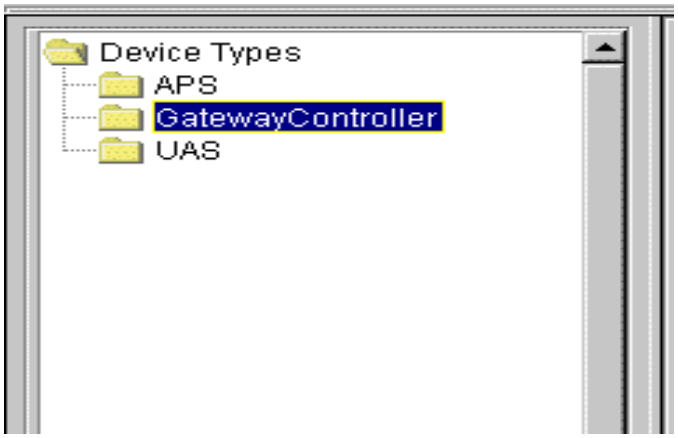
The CS 2000 Management Tools GUI opens in a new browser window.



37 Activate the Maintenance information window for the GWCs as follows:

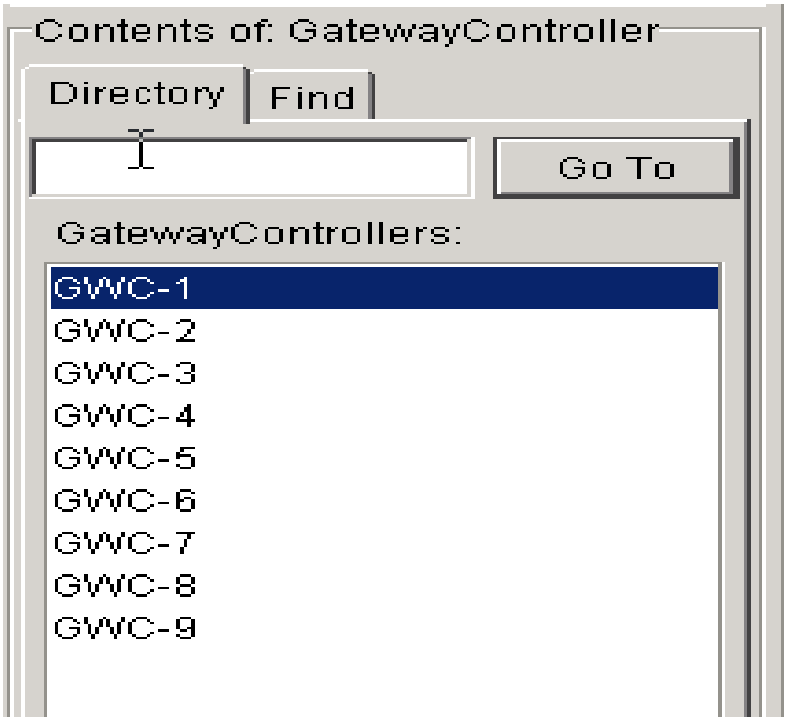
a Select **GatewayController** from the **Device Types** field of the CS2000 Management Tools GUI.

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



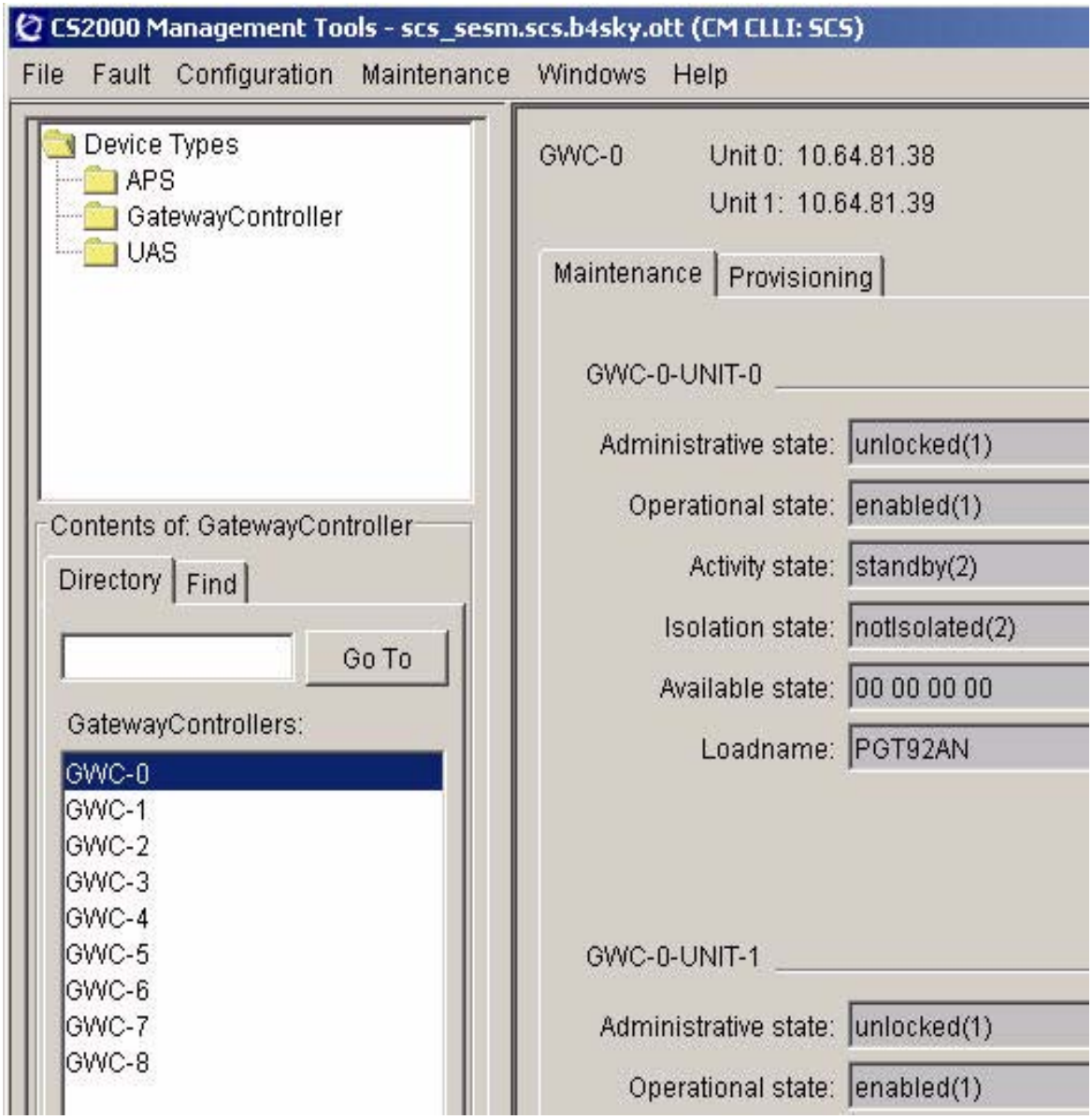
b Select the **Directory** tab on the **Contents of: Gateway Controlle**r field.

The list of Gateway Controllers (GWC) 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.

38 Make all GWCs inactive on Ethernet Routing Switch 8600 Chassis **N**.

Note: Recall that the recommendation at step 1 requires that GWC unit 0s subtend Ethernet Routing Switch 8600 Chassis 0. GWC unit 1s subtend Ethernet Routing Switch 8600 Chassis 1. The following table reiterates the Ethernet Routing Switch 8600 Chassis configurations.

Iteration	Slave Ethernet Routing Switch 8600	Master Ethernet Routing Switch 8600
First Pass	Chassis N = 0	Chassis X = 1
Second Pass	Chassis N = 1	Chassis X = 0

a Check the **Activity State** field for GWC Unit N to determine which unit is **active** and which is **standby**.

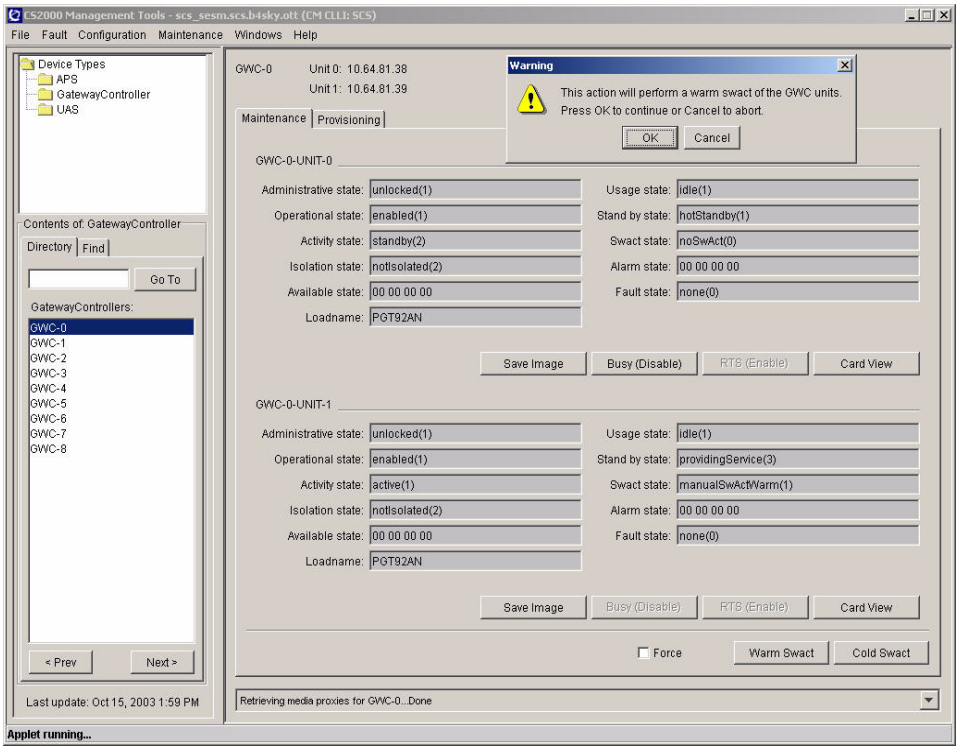
If the Activity State field is	Do
active	sub-step b
standby, instead of inactive	sub-step f

Note: For the first iteration, all GWC 0 units should be standby. For the second iteration, all GWC 1 units are standby.

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 38e
release SN06 (or greater)	step 38f

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.

39 Select the next step as follows:

If the Communication Server uses	Do
XA-Core and IOPs with ETHR packlets (EIOPs)	step 40
XA-Core and HIOPs or HCMICs	step 42
Compact chassis	step 44

Use the XA-Core MAP terminal to disable the Ethernet link with the inactive Ethernet Routing Switch 8600

40 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   .      .      .      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_
```

41 Refer to the following figure and table, and disable the Ethernet link between the XA-Core and Chassis N of the Ethernet Routing Switch 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
```

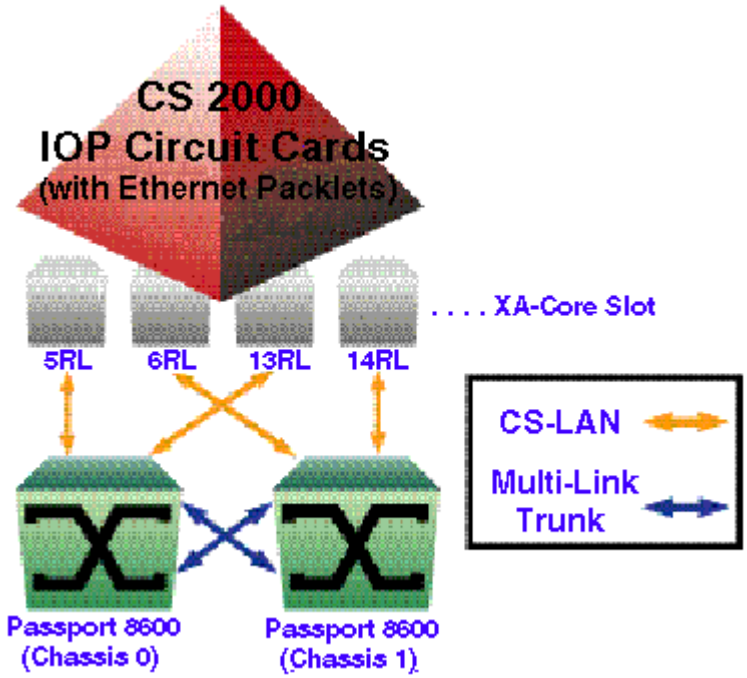
where:

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 Ethernet Routing Switch 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 Ethernet Routing Switch 8600 in any combination.

b Go to step 44.

42 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.

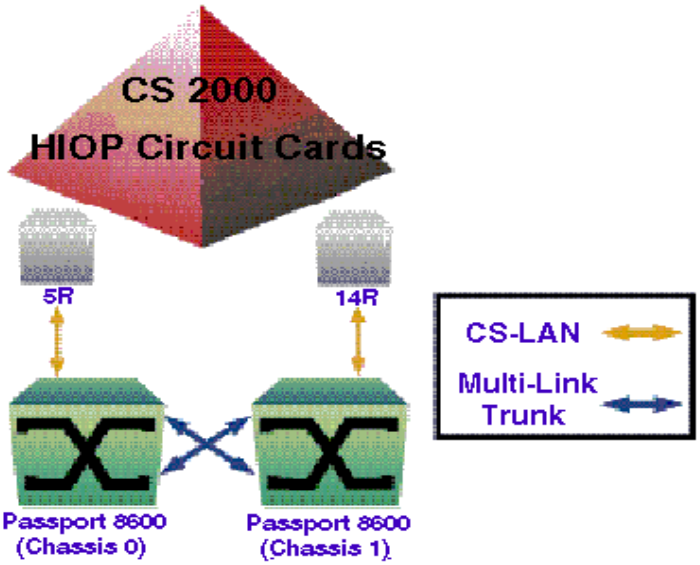
```
 XAC       MS      IOD       Net       PM       CCS      Lns      Trks      Ext      APPL
  .        .        .         .         .        .        .         .        .         .

 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_
```

Note: Refer to the IP addresses in table CMIPADDR. Verify that HIOP links 5R and 14R map to the correct arp table on both Ethernet Routing Switches.

43 Refer to the following figure and table, and disable the XA-Core to Ethernet Routing Switch 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 Ethernet Routing Switch 8600.

44 Select the next step as follows.

If you have	Do
a 3PC with a USP Compact	step 45
a 3PC with a standard USP	step 67
an XA-Core	step 87

Use the USPc GUI to prepare the slave USPc blade for locking:

45

ATTENTION

Prior to adhering to steps 46 to 61, ensure that the slave USPc blade is being addressed during the first iteration of the Ethernet Routing Switch 8600 software upgrade.

Refer to your network diagram and determine the USPc blade-to-Ethernet Routing Switch 8600 connectivity. The slave USPc blade must connect to Chassis N of the Ethernet Routing Switch 8600; master USPc blade to Chassis X. (This information coincides with the network element-to-Ethernet Routing Switch 8600 assumptions stated in step 1b of this procedure.)

Preparing the slave USPc blade for locking consists of the following steps:

- inhibiting all SS7 links on the slave USPc blade.

  Note: If only one link is available on a linkset, it cannot be inhibited. If there are other links on the linkset, ensure at least one of the links is available before attempting to inhibit the link.

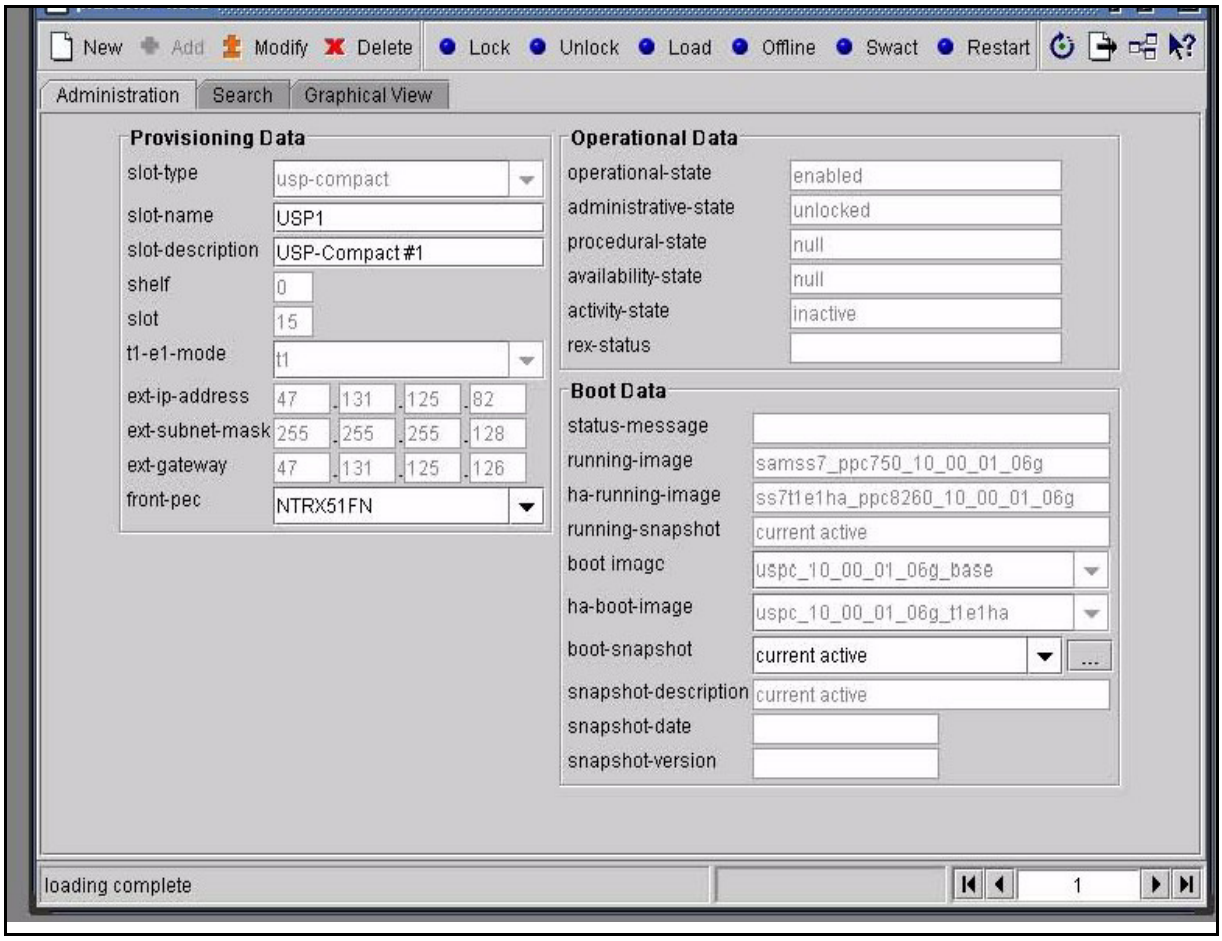
- deactivating all the SS7 links on the slave USPc blade
- bringing down all the IPS7 paths on the slave USPc blade
- locking the slave USPc blade from the USPc GUI

  Note: Both USPc blades carry traffic and are inservice.

46 Launch the USPc GUI.

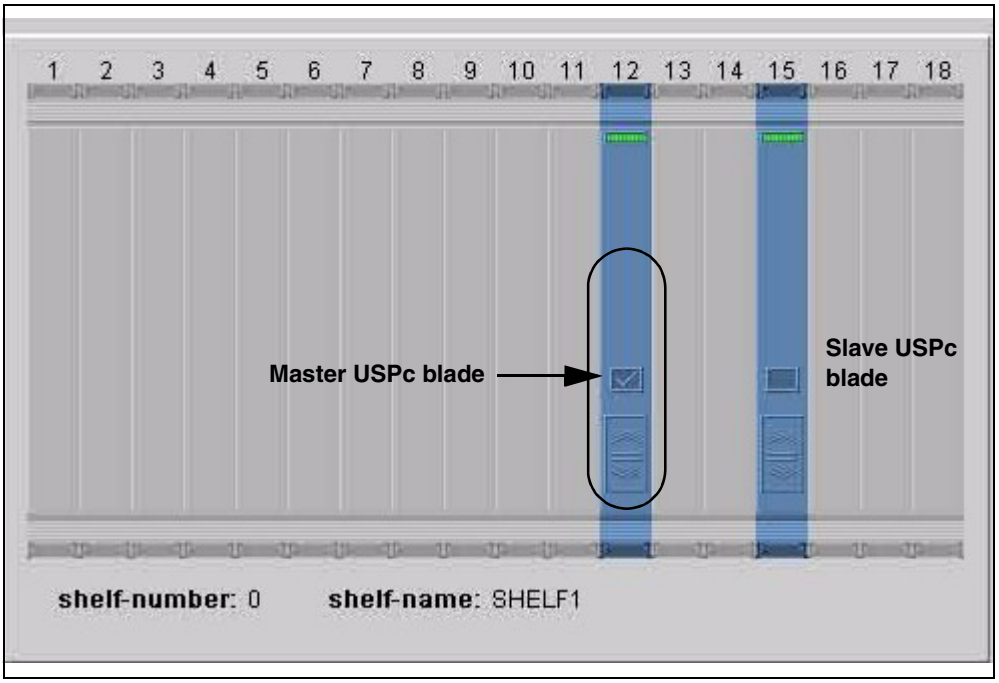
47 Select **Configuration --> platform --> Node**.

The Administration tab of the USPc GUI displays.



48 Verify the master and slave USPc blade-to-Ethernet Routing Switch 8600 connectivity by selecting the Graphical View tab.

The following figure displays the Graphical View of the USPc blades.



The blade icon with a checkmark identifies the master USPc. Slot 12 contains the master USPc blade. Slot 15 contains the slave USPc blade.

49 Select the next step as follows.

If the slave USPc blade is	Do
not connected to Chassis N of the ERS 8600	step 50
connected to Chassis N of the ERS 8600	step 51

50 Perform a SWACT on the two USPc blades.

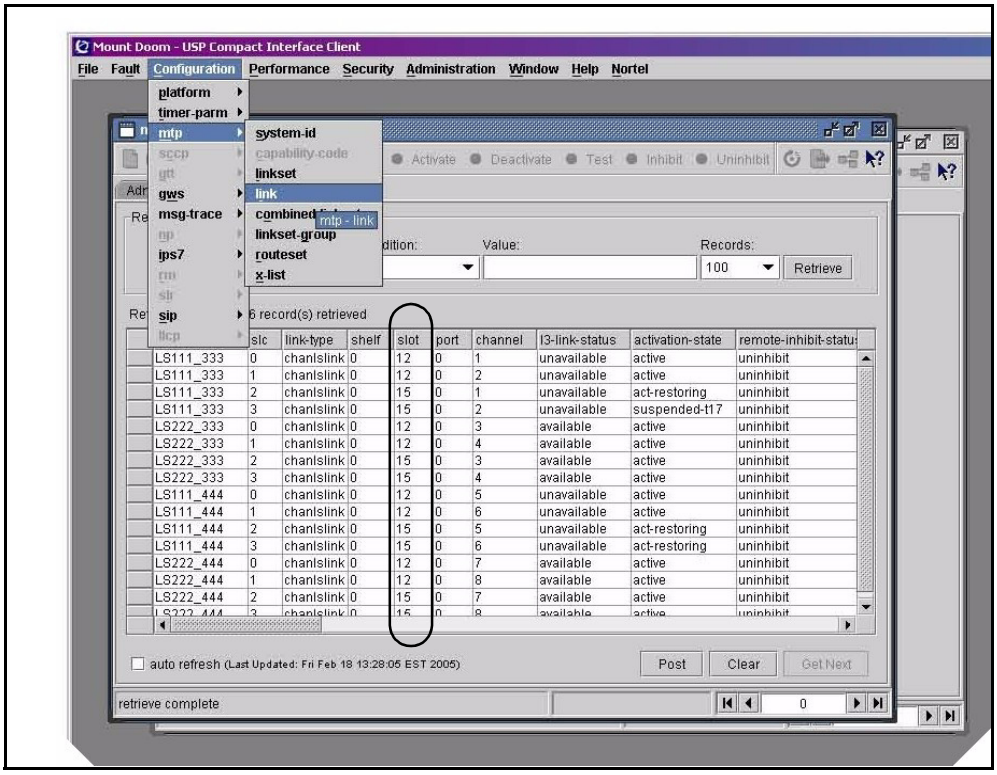
a During display of the Administration tab, press the Swact button in the upper right-portion of the screen.

b Continue to step 51.

51 Turn down the paths and the links associated with the slave blade to be locked.

Select **Configuration --> MTP --> Links** from the pull-down menu.

The following figure displays.



52 Refer to the Slot column to verify the SS7 links against the USPc blades. Select any SS7 links that are against the slave USPc blade.

Click the Inhibit button towards the upper-right portion of the screen to inhibit the links that apply to the slave USPc blade.

The following prompt displays.

```
The inhibit command will be executed for all
posted records.
Are you sure you want to continue?
```

53 Click Yes to execute the command on the selected links.

54 Using the same screen, reselect the links. Click the Deactivate button in the upper-middle portion of the screen.

The following prompt displays.

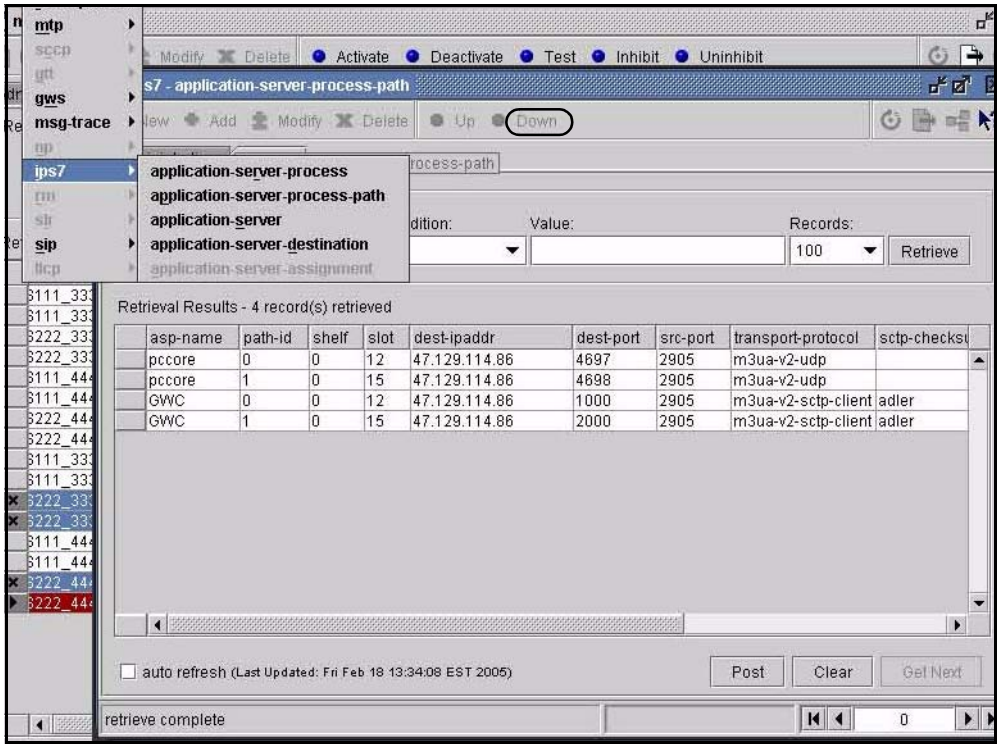
```
The deactivate command will be executed for all
posted records.
Are you sure you want to continue?
```

55 Click Yes to execute the command on the selected links.

56 Post the IPS7 paths that use the slave USPc blade.

Select **Configuration --> ips7 --> application-server-process-path**.

The following figure displays.



57 Select all the IPS7 paths against the slave USPc blade. Click the Down button in the upper-right portion of the screen.

The following prompt displays:

```
The down command will be executed for all posted
records. Are you sure you want to continue?
```

58 Click Yes to execute the command on the IPS7 paths on the slave USPc blade.

At this point, the IPS7 paths and SS7 links against the slave USPc blade have been deactivated.

59 Lock the slave USPc blade.

Select **Configuration --> platform --> Node**.

The Administration tab, as shown in step 47, redisplays.

60 Click the Lock button at the upper-middle portion of the platform-nodes screen.

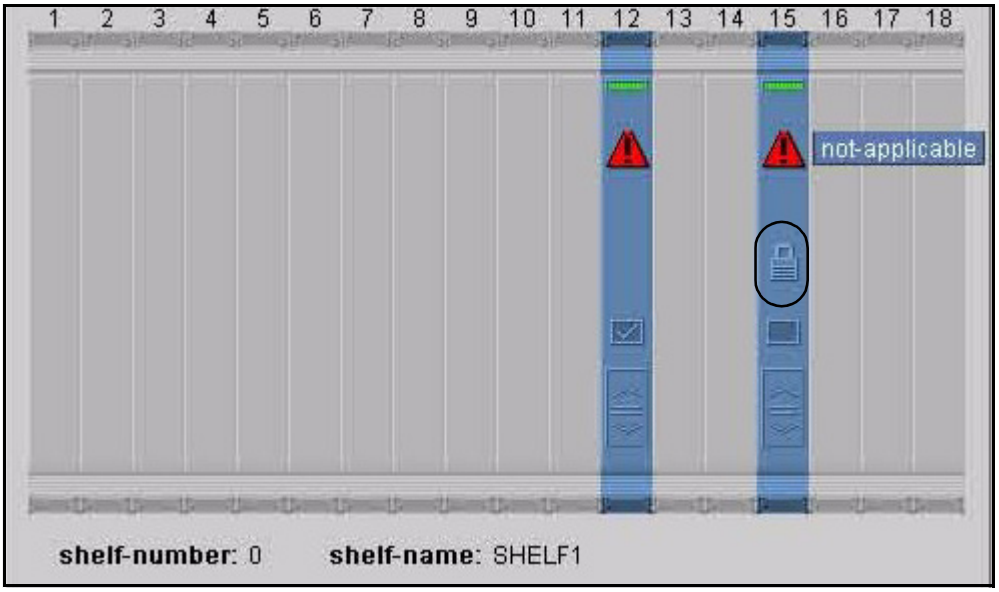
The following prompt displays:

```
The node lock command will impact the last
in-service link from at least 1 linkset which
may impact network traffic. Do you want to
continue?
```

61 Click Yes to lock the USPc blade.

Click the Graphical View tab.

The Graphical View tab shows that the USPc blade has a lock icon next to it, indicating it has been locked.

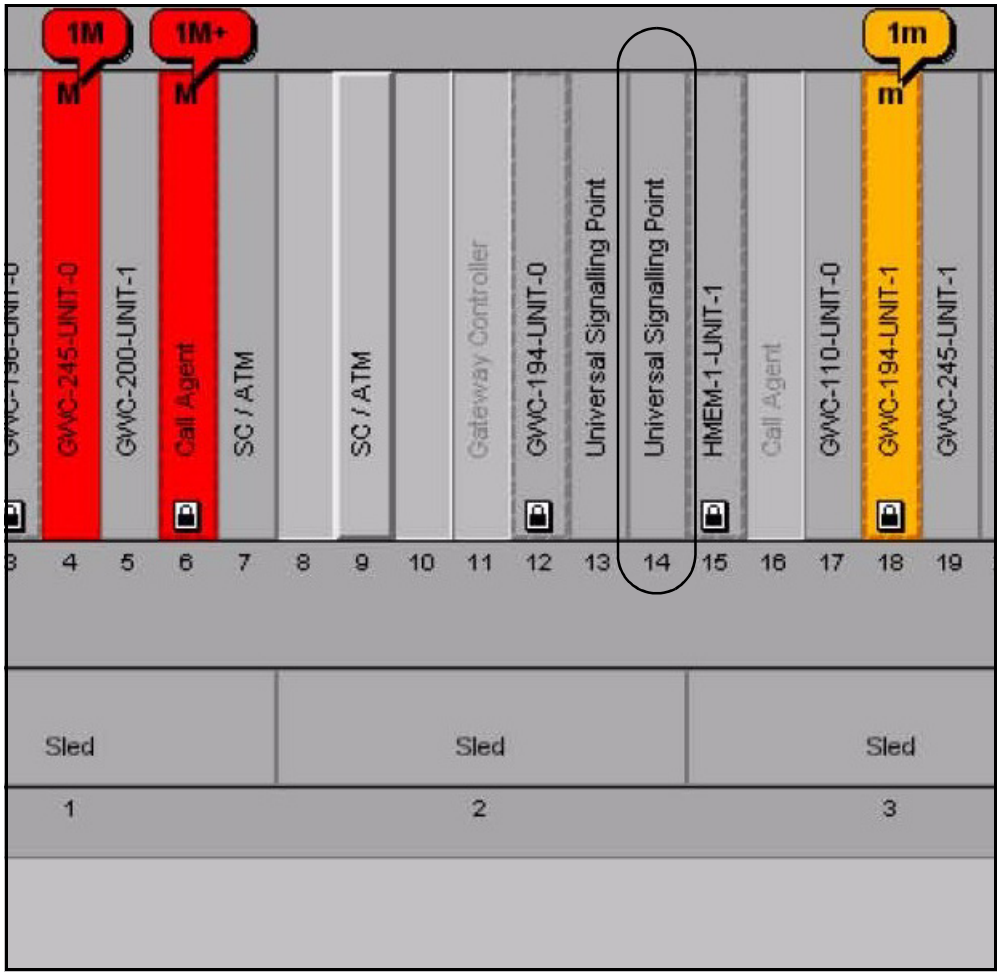


Use the SAM21 Element Manager to lock the USPc blade:

62 Access the SAM21 EM GUI.

63 Select the SAM21 shelf by double clicking on its icon.

The following figure shows an example of a shelf which contains a slave USPc blade residing on slot 14.



64 Right click on the icon which corresponds to where the slave USPc blade resides.

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

65 Click **Lock**.

The slave USPc blade is locked.

Note 1: *This prevents an automatic change of activity from occurring. An automatic SWACT at this point could cause a system outage.*

Note 2: *An alternative method to Lock the blade from the SAM21 EM is to first open the card by double clicking on it. Then click Lock button towards the upper-right portion from display of the States tab.*

66 Proceed to step 77.

Use the USP GUI to take down the paths to the ERS8600 Chassis N

67 Launch the USP GUI.

Taking down the paths to the ERS8600 Chassis N consists of the following tasks:

- identifying all IP cards in the USP, and noting which ERS Chassis they are connected to
- ensuring that for each path, there is an alternate in-service path through Chassis X
- taking down all IPS7 paths using Chassis N

68 Select **Configuration->platform->node**.

69 Click **retrieve**, and look for all records that have a slot-type of iplink.

70 Note the following information for each IP link card:

- Shelf
- Slot
- IP Address
- ERS8600 unit it is connected to

71 Select **Configuration->ips->application-server-process-path**

72 Click **retrieve**, and look for all paths on the cards noted in step 70, that are connected to Chassis N.

73 Click on the **asp-name** column to sort the table, and confirm that for each path connected to a card using Chassis N, there is an alternate path using Chassis X that has a path-state of up. Refer to the information you noted in step 70.

74

CAUTION
Potential service interruption
If the alternate path to any destination is not in service, performing the step that follows will result in a service interruption.

Select each path connected to Chassis N, and click **Post**, then confirm that only the paths associated with the cards connected to Chassis N, are selected. Refer to the information you noted in step 70.

75 Click **Down** to take the posted paths out of service.

76 Click **Yes** to confirm the command execution on the IPS7 paths associated with the cards connected to Chassis N.

Decide if STORM devices require rotating, demounting and busying

77

ATTENTION
Before proceeding with the following STORM-related steps, consider if other applications might be affected by the loss of STORM disk volumes.

Select the next step as follows

If	Do
STORM uses a Dothill device	step 78
STORM IA (SAM-XTS) device[1]	step 87

1. The SAM-XTS configuration uses dual-homed split multilink trunks (SMLT). Both STORM volumes are recognized by both Ethernet Routing Switch 8600 routers. Therefore, taking down one router in an SAM-XTS configuration does not affect the STORM volume being addressed.

78 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)[1]	step 79
the volumes on the STORM disk are not actively mounted DIRP[2]	step 87

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.
2. Regardless of whether DIRP volumes are mounted, the procedure can result in an unavailable STORM disk and associated volumes.

79 Refer to your network diagram and verify that the STORM device-to-Ethernet Routing Switch 8600 connectivity in your configuration is set up as follows:

- STORM volumes prefixed with sd00 reside on STORM device 0, which *must* connect to Ethernet Routing Switch 8600 Chassis 0.
- STORM volumes prefixed with sd01 reside on STORM device 1, which *must* connect to Ethernet Routing Switch 8600 Chassis 1.

Note: This information coincides with the network element-to-Ethernet Routing Switch 8600 assumptions stated in step 1b.

If the STORM-to-Ethernet Routing Switch 8600 connections in your configuration do not match these assumptions, adjust the commands in steps 80 to 86 to address the appropriate STORM device.

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

```
> table dirpssys; lis all
```

81 Access the DIRP level in SOS by typing:

```
> mapci nodisp;mtc;iod;dirp
```

82 Query all volumes associated with the subsystem.

```
> query <subsystem> all
```

where:

subsystem
is from the list of available subsystems executed in step 80

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 SD00DLG1         1     1 0 71 NO  8448 000D 1014
STANDBY1 AVAIL SD01DLG1         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 SD01DLG1 READY          N/A N/A N/A    8   10   11 8408 S1
  71 SD00DLG1 READY          N/A N/A N/A    8  112  116 8448 A

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

83 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 Ethernet Routing Switch 8600 chassis that is not being upgraded for this iteration.

```
> 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 1: Parallel is intentionally misspelled.

Note 2: Volumes associated with the slave Ethernet Routing Switch 8600 should *not* be active. Ensure that no volumes are active in each pass which are prefixed with:

sd0N
where N = 0 (first pass)
N = 1 (second pass)

For example, sd00 volumes should not be active during the first pass. Sd01 volumes should not be active during the second pass. (Rotate each subsystem with volumes prefixed with sd0N that are active.)

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

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
```

84 Repeat step 83 to ensure that all volumes needing rotating have been rotated successfully.

85 Demount all DIRP volumes connected to the Ethernet Routing Switch 8600 chassis that is to be upgraded.

```
> dmnt <subsystem> <volume> <variable>
```

where:

volume
is the volume on the STORM (prefixed with sd0N where N is defined in Note 2 of step 83)

variable
is regular or paralel

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

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

86 Busy all STORM volumes connected to the Ethernet Routing Switch 8600 chassis to be upgraded.

```
> diskadm sd0N; bsy all
```

where:

sd0N
is the STORM volume defined in Note 2 of step 83

Note 1: Nortel 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.

87 Select the next step as follows:

If the CS-LAN is used with	Do
a Trimodal solution	step 88
an ATM-based solution	step 88
an IP-based solution	step 90

Use the SAM21 EM to lock the inactive Shelf Controller blade connected to Chassis N:

88

ATTENTION

During a SWACT on the Shelf Controllers (SC), flapping (that is, rapid enabling and disabling) of the router port connected to a SC can result in a temporary loss of Ethernet connectivity. This could cause ongoing failures on the newly active SC following the SWACT.

To prevent the possibility of an outage due to this condition, monitor ongoing or recent logs for Ethernet instability on the router ports that are associated with SCs.

Do ***not*** SWACT the SCs until all network problems involving flapping are addressed.

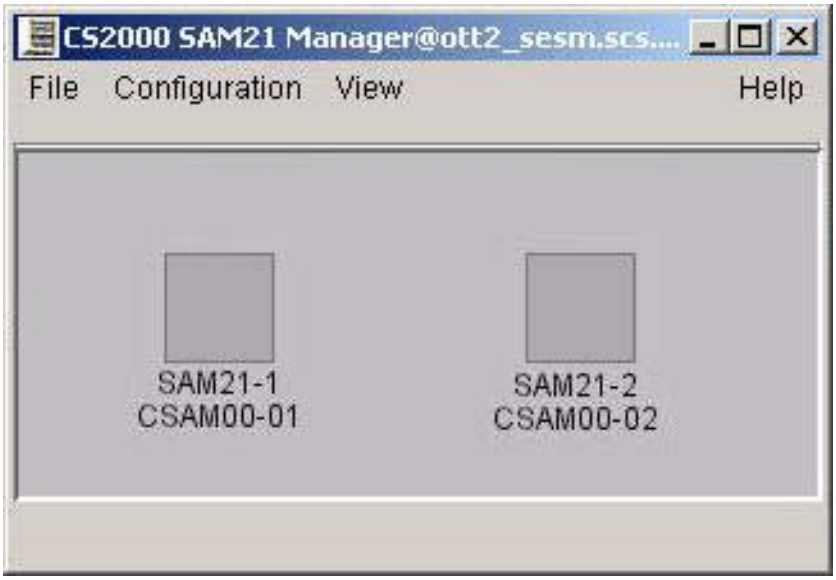
Confirm that Shelf Controller (SC) blade connectivity complies with the recommendation at step 1b for all SAM21 shelves.

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

89 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.

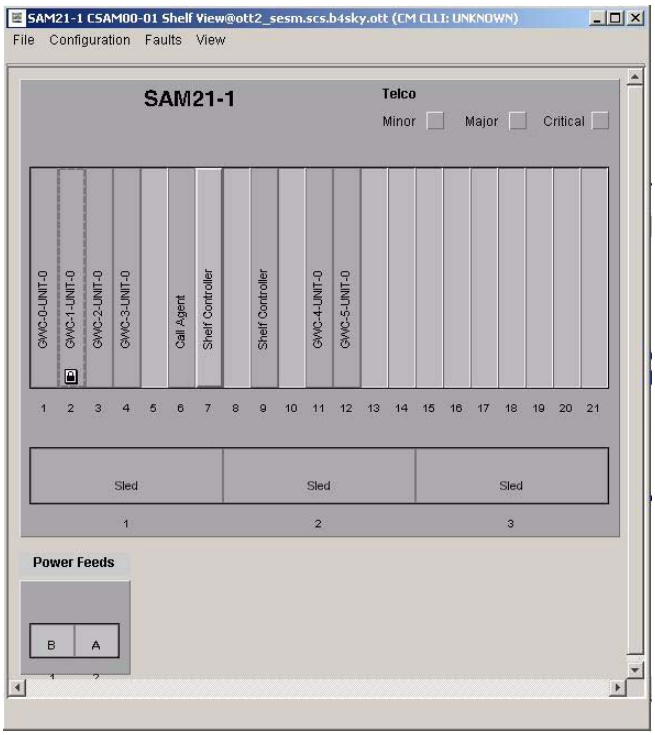


b use the cursor to select the shelf icon for the first SAM21 shelf displayed

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.



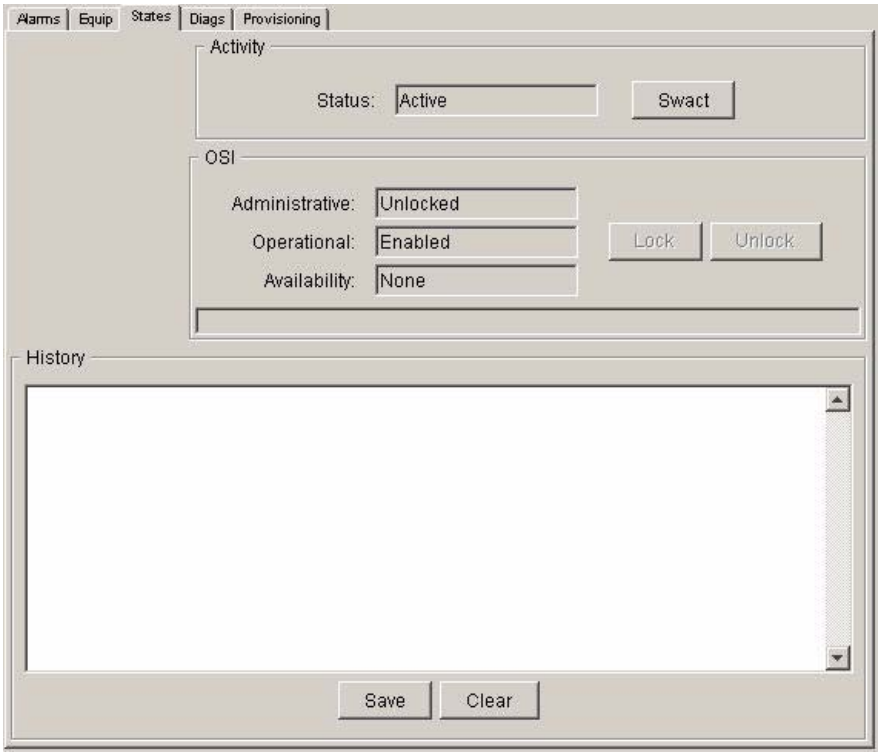
d right-click on the icon for the SC blade associated with the inactive Ethernet Routing Switch 8600 Chassis.

Note: The SC blade in slot 7 subtends Ethernet Routing Switch 8600 Chassis 0, slot 9 subtends Chassis 1 (see note to step 88)

*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 117
not all locked	select the next SAM21 Shelf and repeat sub-step c

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

90 Select the next step as follows:

If your office is	Do
in a Geographic Survivability environment	step 91 through step 116
not in a Geographic Survivability environment	step 117

Use the Integrated Element Management System (IEMS) GUI to lock the Media Server 2000 (MS 2000) Series node connected to Chassis N

91 Launch the IEMS GUI.

Note: Refer to NTP *Integrated EMS Basics*, NN10329-111, for details on logging into the IEMS GUI.

92 Select **Applications ---> Integrated EMS --->Network Elements**.

93 Select the MS 2000 Series node to be locked and right click on its icon.

94 Select the Config and Maintenance Tool from the pop-up menu.

The Config and Maintenance Tool launches.

Note: *For details, refer to procedure "Launching the Maintenance and Configuration tool" in section Configuring and maintaining MS 2000 devices, NTP Integrated EMS Configuration Management, NN10330-511.*

95 From the left side of the Config and Maintenance Tool screen, click the **Graceful Lock** button under the Lock State options to lock the MS 2000 node.

Note: A graceful lock signals to the node that a lock has been requested. The node then stops allocating new audio resources and waits for the last resource to be freed before locking the node. (A forced lock causes the node to immediately free up any resources in use and lock the node.)

96 Click the Lock button to gracefully lock short-duration calls from the MS 2000 node.

Note: Since a graceful lock prevents new calls from being originated on the node, existing calls will be taken down on their own. Therefore for calls still active after an extended period of time, *it is up to the discretion of the craftsperson to determine whether to issue a forced lock, or to proceed when the Ethernet Routing Switch 8600 is rebooted.*

Drop sync the inactive Call Agent

97 Before locking the inactive Call Agent card, perform a drop synchronization on the inactive Call Agent card from the active Call Agent Manager by typing the following commands.

```
> ccamtc
> coremtc
> appl
> dpsync
```

98 Select the next step as follows

If the (active) Call Agent card is	Do
connected to ERS 8600 Chassis N	step 99
not connected to ERS 8600 Chassis N	step 106

Use the MAP display to perform a LIMITED_PRESWACT

99 At the MAP display, enter the following command:

```
> BCSUPDATE; LIMITED_PRESWACT
```

Note 1: If a LIMITED_PRESWACT process fails to complete, LIMITED_PRESWACT stops and displays additional information. When this occurs, use the information to investigate and correct the problem.

Note 2: All LIMITED_PRESWACT steps must be completed prior to SWACTing.

The LIMITED_PRESWACT command displays a warning:

```
Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", "N"):
```

100 Enter Y.

```
> Y
```

A series of steps execute and complete. LIMITED_PRESWACT stops at MATE_RESTART_RELOAD.

```
MATE_RESTART_RELOAD              executing
There are users still logged on the Inactive.
Do you want to continue?
MATE_RESTART_RELOAD              not complete
ACT - Error: Restart aborted. Type
LIMITED_PRESWACT to continue
Investigate and correct if needed.
```

101 If the LIMITED_PRESWACT process halts, re-enter the following command to continue.

```
> LIMITED_PRESWACT
```

The following warning displays.

```
MATE_RESTART_RELOADexecuting
There are users still logged on the Inactive.
Do you want to continue?
Please confirm (“YES”, “Y”, “NO”, “N”):
```

102 Enter Y.

```
> Y
```

The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated by display of the following message:

```
Total execution time for all complete procedures
00:07:31.362
All LIMITED_PRESWACT steps completed
successfully.
```

Perform a NORESTARTSWACT

103 If the active Call Agent card is connected to the Ethernet Routing Switch 8600 to be upgraded, minimize the possibility of an outage by performing a NORESTARTSWACT.

a Check the status:

```
> BCSUPDATE;SWACTCI;STATUSCHECK
```

The following response displays:

```
SWACTCI:
Checking Nodes Status
STATUSCHECK successful
```

b Execute the NORESTARTSWACT.

```
> NORESTARTSWACT
```

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"):
>
```

c Enter a Y if the only alarm is an APPL simplex.

```
> Y
```

The final progress follows. Activity also switches at the Call Agent Manager.

```
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
```

d The telnet session to the active and inactive call processing applications are lost. Re-establish the connection. Refer to the Interface set in section Call Agent Upgrades for this procedure.

Perform a POSTSWACT

104 At the MAP display, enter the following command to run a Postswact through completion.

```
> BCSUPDATE;POSTSWACT
```

105 Enter N when prompted at the CA_SYNC step to leave the switch out of sync.

```
> N
```

Lock the inactive Call Agent card

106

CAUTION

Possible service interruption

DO NOT ATTEMPT TO LOCK THE ACTIVE CALL AGENT CARD.

Locking the active until causes a complete service outage.

To lock the inactive Call Agent, follow these steps:

a Access the SAM21 EM GUI.

b Select the SAM21 shelf by double clicking on its icon.

c From the Shelf View, right click on the card that corresponds to the inactive Call Agent card.

d Select the **Lock** option from the context menu.

Note: Lock is also available from the States tab of the Card View window.

e Wait for the Lock icon to appear on the selected card.

Demount active DIRP volumes off of SD01

107 At the MAP display, enter the DIRP level.

```
> MAPCI NODISP;MTC;IOD;DIRP
```

108 Query the subsystem to determine which files are active and which are standby.

```
> QUERY JF FILES
```

```
> QUERY DLOG FILES
```

109 Demount all volumes on SD01 for the subsystems that are not active.

```
> DMNT DLOG SD01DLG0
```

```
> DMNT DLOG SD01DLG1
```

```
> DMNT DLOG SD01DLOG2
```

110 Rotate the subsystems to a standby volume on SD00.

```
> ROTATE JF
```

```
> ROTATE DLOG
```

111 Query the subsystem again to verify that the active files are on SD00.

```
> QUERY JF FILES
```

```
> QUERY DLOG FILES
```

112 Demount any remaining volumes on SD01.

```
> DMNT JF SD01JF
```

```
> DMNT DLOG SD01DLG3
```

113 Query the subsystem again to verify that no volumes on SD01 are used.

```
> QUERY JF FILES
```

```
> QUERY DLOG FILES
```

The display should indicate that the JF and DLOG subsystems are not using any volumes on SD01.

114 Repeat step 108 for any additional DIRP subsystems.

115 Quit the DIRP level.

```
> QUIT ALL
```

Busy all STORM disk volumes on SD01 to ensure that the call processing application does not attempt to access the STORM unit

116 At the MAP display, enter the following command to busy all disk volumes on device SD01.

```
> DISKADM SD01;BSY ALL
```

If the devices do not pass, determine which application has open files. Perform maintenance on those applications so that the application closes the files.

Note: Refer to the STORM upgrade documentation, Upgrading the STORM, in this document for details.

Use the Ethernet Routing Switch 8600 CLI to make sure devices subtending the Ethernet Routing Switch 8600 Chassis X are active (Chassis N devices inactive):

117 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 38. If the problem persists, contact your next level of support.

Use the Ethernet Routing Switch 8600 CLI to upgrade the software load on Ethernet Routing Switch 8600 Chassis N:

118 Access the Ethernet Routing Switch 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 Ethernet Routing Switch 8600 power supply then try again. If the problem persists contact your next level of support.

119

ATTENTION

Refer to section Text conventions on page 100 for brief definitions and examples of the software filenames used in the following commands.

Select the next step as follows

If your CS-LAN:	Do
is a dual CPU configuration	step 120
is a single CPU configuration	step 125

120

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.X.X Release Notes.

Due to the implementation of DNS, the peer command option is not available unless you add the peer IP address in a new file called flash/etc/hosts.

You must create this file. No default file exists. Use a simple text editor to create it, similar to the text editor provided by the Ethernet Routing Switch 8600.

For an Ethernet Routing Switch 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 Ethernet Routing Switch 8600 automatically copies files to the flash card using the same name as the current file. When entering the copy command if a destination name is not specified, then the system uses the same name as the source filename.Therefore, it is not necessary to enter a new filename for the backup version of this file in step 120a through step 120e.

a TFTP the new software image file.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<newload> /flash/** **copy /flash/<newload> peer:/flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<newload> /flash/** **copy /flash/<newload> peer:/flash/**

where

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

newload
is the name of the new software image file, which must be in lower case, for example p80a3722.img

b TFTP the new boot monitor image file.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<newboot> /flash/** **copy /flash/<newboot> peer:/flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<newboot> /flash/** **copy /flash/<newboot> peer:/flash/**

where

newboot
is the name of the new boot monitor image file, which must be in lower case, for example p80b3722.img

The boot flash image and software image is backed up to the PCMCIA card on the Ethernet Routing Switch 8600 Chassis N.

Note 1: *If either file transfer fails, verify TFTP server IP address and connectivity with Ethernet Routing Switch 8600 Chassis N. Confirm Ethernet Routing Switch 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 Ethernet Routing Switch 8600 uses an ATM blade, TFTP the ATM Flash image to the Flash card on the Ethernet Routing Switch 8600 Chassis N.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<newATM> /flash/** **copy /flash/<newATM> peer:/flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<newATM> /flash/** **copy /flash/<newATM> peer:/flash/**

where

newATM
is the name of the new ATM file

Otherwise go to step 121.

Note: Notes 1 and 2 from step 120, sub-step b apply.

d If the Ethernet Routing Switch 8600 uses DES, TFTP the file.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<newDES> /flash/** **copy /flash/<newDES> peer:/flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<newDES> /flash/** **copy /flash/<newDES> peer:/flash/**

where

newDES
is the name of the new DES file

e If the Ethernet Routing Switch 8600 uses 3DES, TFTP the file.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<new3DES> /flash/** **copy /flash/<new3DES> peer:/flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<new3DES> /flash** **copy /flash/<new3DES> peer:/flash/**

where

new3DES
is the name of the new 3DES file

121 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
```

122 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>
```

where

newload
is the name of the new software image file, for example p80a3722.img

b Type:

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

where

oldload
is the original software image filename, for example p80a3320.img

c

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

Disable the flag setting by typing

```
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
```

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 Ethernet Routing Switch 8600 Chassis N to reboot.

123

CAUTION
Potential crash of standby CPU
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, for example p80b3722.img

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/<newboot>
```

where

newboot
is the name for the new monitor image file, for example p80b3722.img

124 Delete the previous image files from the /flash and /pcmcia directories as follows:

a Type

```
dir
```

b Delete the previous image files, excluding the current image files, from the /flash directory by typing

```
remove /flash/<filename>
```

where

filename
is the name of the old image file, for example, p80aXXXX.img and p80bXXXX.img, where XXXX is the version of the software

c Delete the previous image files, excluding the current image files, from the /pcmcia directory by typing

```
remove /pcmcia/<filename>
```

where

filename
is the name of the old image file, for example, p80aXXXX.img and p80bXXXX.img, where XXXX is the version of the software

Go to step 129.

125 For an Ethernet Routing Switch 8600 with a single CPU configuration, TFTP upgrade software to the flash on Chassis N of the Ethernet Routing Switch 8600.

a Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<newload> /flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<newload> /flash/**

where

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

newload
is the name of the new software image file, for example p80a3722.img

Note: The Ethernet Routing Switch 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 125b through step 125e.

b Type the following commands depending on your core manager platform.type./

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<newboot> /flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<newboot> /flash/**

where

newboot
is the name of the new boot monitor image file, for example p80b3722.img

The boot flash image and software image is backed up to the PCMCIA card on the Ethernet Routing Switch 8600 Chassis N.

Note 1: *If either file transfer fails, verify TFTP server IP address and connectivity with Ethernet Routing Switch 8600 Chassis N. Confirm Ethernet Routing Switch 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 Ethernet Routing Switch 8600 uses an ATM blade, TFTP the ATM Flash image to the Flash card on the Ethernet Routing Switch 8600 Chassis N.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<newATM> /flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<newATM> /flash/**

where

newATM
is the name of the new ATM file

Otherwise go to step 126.

Note: Notes 1 and 2 from step 125, sub-step b apply.

d If the Ethernet Routing Switch 8600 uses DES, TFTP the file.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<newDES> /flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<newDES> /flash/**

where

oldDES
is the original DES filename

e If the Ethernet Routing Switch 8600 uses 3DES, TFTP the file.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	**copy <a.b.c.d>:/swd/pp8600/XXX/<new3DES> /flash/**
CBM	**copy <a.b.c.d>:/pp8600/XXX/<new3DES> /flash/**

where

old3DES
is the original 3DES filename

126 Prepare to reboot Ethernet Routing Switch 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>

where **<newload>** is the name of the new software image file, for example p80a3722.img

b Type:

config bootconfig choice secondary image-file /flash/<swloadbkup>

where

swloadbkup
is the name of the backup version of the software image file, for example p80a3721.img

c

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

Disable the flag setting by typing

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 Ethernet Routing Switch 8600 Chassis N to reboot.

127

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 Ethernet Routing Switch 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, for example p80b3722.img

Serial connectivity is maintained between the terminal server and Ethernet Routing Switch 8600 Chassis N during the 60 to 90 seconds required to load the new software image.

128 Delete the previous image files from the /flash and /pcmcia directories as follows:

a Type

```
dir
```

b Delete the previous image files, excluding the current image files, from the /flash directory by typing

```
remove /flash/<filename>
```

where

filename
is the name of the old image file, for example, p80aXXXX.img and p80bXXXX.img, where XXXX is the version of the software

c Delete the previous image files, excluding the current image files, from the /pcmcia directory by typing

```
remove /pcmcia/<filename>
```

where

filename
is the name of the old image file, for example, p80aXXXX.img and p80bXXXX.img, where XXXX is the version of the software

Use the Ethernet Routing Switch 8600 CLI to verify all hardware and software on the Ethernet Routing Switch 8600 Chassis X:

129 Make sure Ethernet Routing Switch 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.

130 If using an XA-Core, skip to step 136.

131 Select the next step as follows.

If	Do
an inservice CPU memory upgrade for an Ethernet Routing Switch 8600 chassis is anticipated for future expansion	Power down the shelf of the Ethernet Routing Switch 8600 ***before*** pulling out the shelf. OTHERWISE AN OUTAGE CAN RESULT! 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 an Ethernet Routing Switch 8600 is not anticipated	step 132

132 Select the next step as follows.

If	Do
STORM uses a Dothill device	step 133
STORM IA (SAM-XTS) device[1]	step 136

1. The SAM-XTS configuration uses dual-homed split multilink trunks (SMLT). Both STORM volumes are recognized by both Ethernet Routing Switch 8600 routers. Therefore, taking down one router in an SAM-XTS configuration does not affect the STORM volume being addressed.

133 Select the next step as follows.

If	Do
the volumes on any STORM disk (for example, sd01) are actively mounted in DIRP[1]	step 134
the volumes on the STORM disk are not actively mounted in DIRP[2]	step 136

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.
2. Regardless of whether DIRP volumes are mounted, the procedure can result in an unavailable STORM disk and associated volumes.

134 Return to service all disk volumes connected to the Ethernet Routing Switch 8600 chassis that were upgraded.

```
> diskadm sd0N; rts all
```

where:

sd0N
is the STORM volume defined in Note 2 of step 83

135 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 recommends recording all subsystems, volume, and variable information for each volume remounted in this step.

Use the SAM21 EM to unlock the inactive SCs:

136 Launch the SAM21EM client.

The SAM21 EM GUI appears.

137 Select the next step as follows:

If upgrading with	Do
a Trimodal solution	step 138
an ATM solution	step 138
an IP solution	just step 138d

138 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	Do
a USP Compact is used	step 144
a Standard USP is used	step 139
neither is used	step 179

At the USP GUI

139 Post the IPS7 paths that use nodes connected to Chassis N by selecting **Configuration->ips7->application-server-process-path**.

140 Select each path connected to Chassis N and click **Post**, then confirm that only the paths associated with the cards connected to Chassis N, are selected.

141 Click **Up** to bring the posted paths back into service.

142 Click **Yes** to confirm the command execution on the IPS7 paths associated with the cards connected to Chassis N.

143 Proceed to step 157.

Use the SAM21 EM to unlock the inactive slave USPc blade:

144 Re-access the SAM21 EM. Unlock the locked slave USPc blade.

Note 1: Unlocking the slave USPc blade from the SAM21 EM enables the USPc GUI.

Note 2: An alternative method to Unlock the blade from the SAM21 EM is to first open the card by double clicking on it. Then click the Unlock button towards the upper-right portion from display of the States tab.

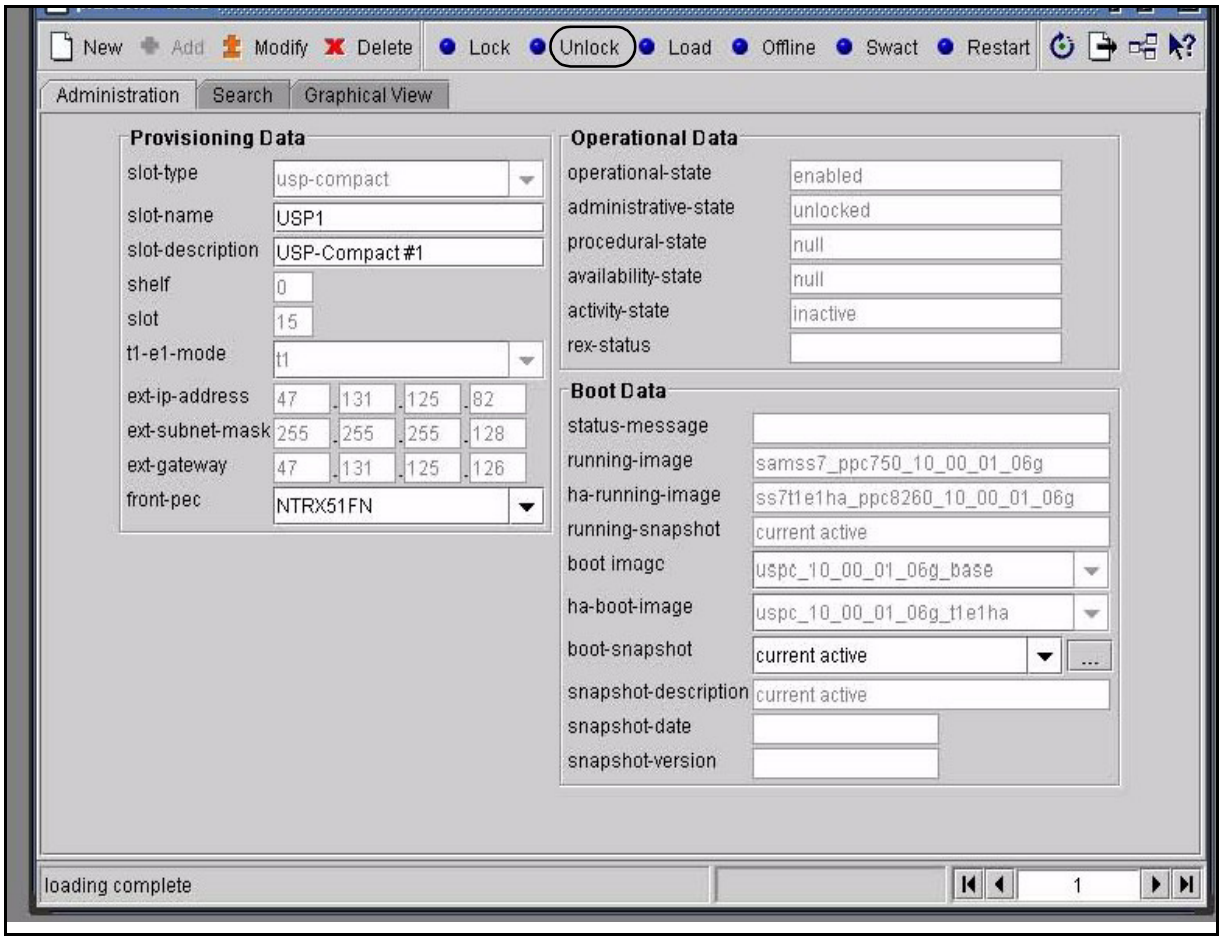
Use the USPc GUI to perform the following additional steps:

145 Re-access the USPc GUI, waiting to ensure that the inactive blade is enabled and locked.

Note: Re-accessing the USPc GUI can take several minutes.

146 Select **Configuration --> platform --> Node**.

The Administration tab of the USPc GUI displays.



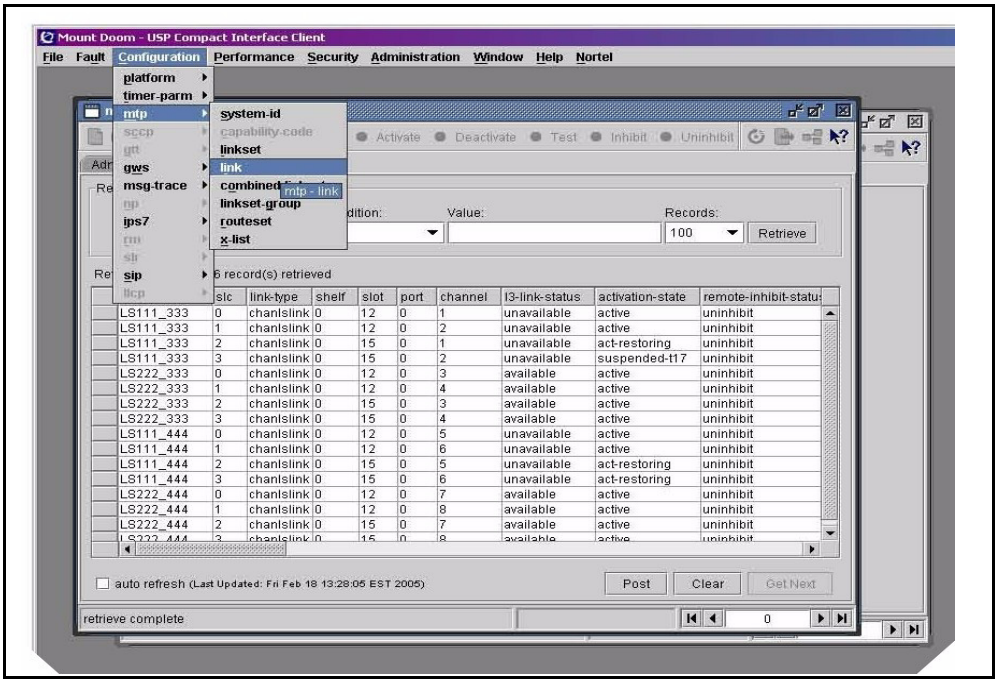
147 Unlock the slave USPc blade.

Click the Unlock button in the upper-middle portion of the screen.

148 Reactivate the SS7 links and the paths associated with the slave USPc blade.

From the Administration tab, select **Configuration --> MTP --> Links** from the pull-down menu.

The following figure appears.



149 Select any SS7 links displayed in the form that are against the slave blade. Click the Activate button towards the upper-middle portion of the screen.

150 Select Yes to execute the command on the selected links.

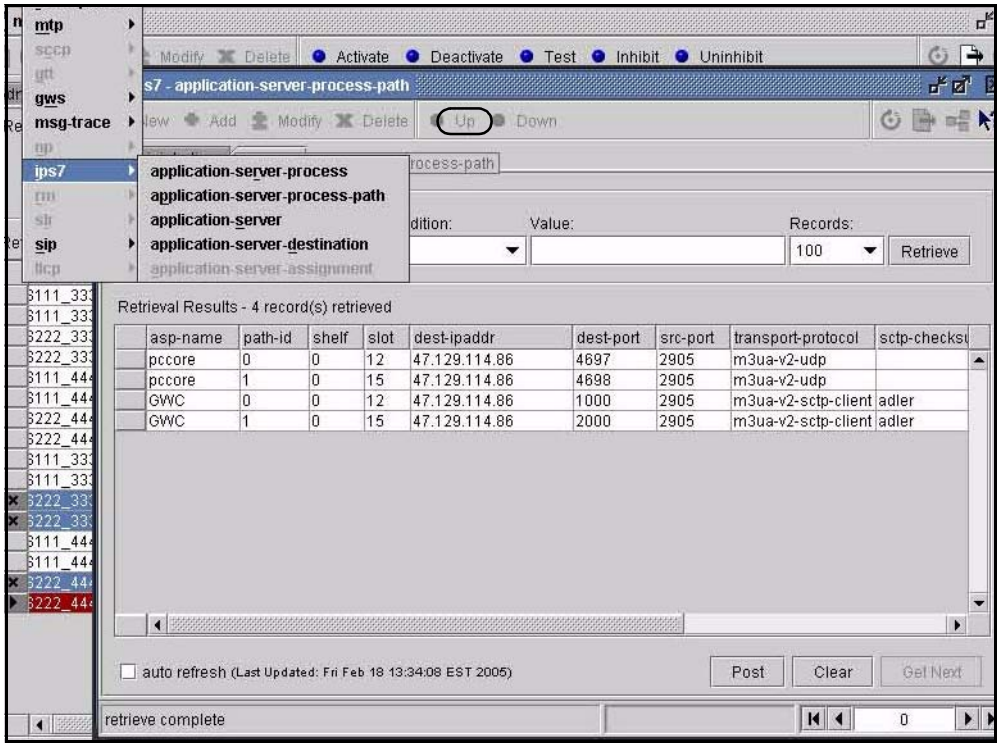
151 Using the same screen, reselect the links. Click the Uninhibit button in the upper-right portion of the screen.

152 Select Yes to execute the command on the selected links.

153 Post the IPS7 paths that use the slave USPc blade.

From the menu, select **Configuration --> ips7 --> application-server-process-path** from the pull-down menu.

The following figure displays.



154 Select all the IPS7 paths against the slave USPc blade. Click the Up button in the upper-right portion of the screen.

The following prompt displays:

```
The up command will be executed for all posted
records. Are you sure you want to continue?
```

155 Select Yes to execute the command on the IPS7 paths on the slave USPc blade.

156 If desired, perform an optional SWACT on the USPc blades to restore initial mastership states.

To perform a SWACT, redisplay the Administration tab, as shown in step 146. Press the Swact button in the upper-right portion of the screen.

157 Select the next step as follows:

If your office is	Do
in a Geographic Survivability environment	step 158 through step 178
not in a Geographic Survivability environment	step 179

Use the SAM21 EM to unlock the inactive Call Agent card

158 Re-access the SAM21 EM. Unlock the locked inactive Call Agent card.

Note: An alternative method to Unlock the blade from the SAM21 EM is to first open the card by double clicking on it. Then click the Unlock button towards the upper-right portion from display of the States tab.

159 Wait for the lock icon to disappear.

160 At the Call Agent Manager, verify that the call processing application loads successfully and waits for synchronization.

Use the MAP display to perform a LIMITED_PRESWACT on the inactive Call Agent

161 If the switch is in sync, first perform a drop synchronization from the ccamtc apply level.

```
> ccamtc
> coremtc
> appl
> dpsync
```

162 At the MAP display, enter the following command:

```
> BCSUPDATE; LIMITED_PRESWACT
```

Note 1: If a LIMITED_PRESWACT process fails to complete, LIMITED_PRESWACT stops and displays additional information. When this occurs, use the information to investigate and correct the problem.

Note 2: All LIMITED_PRESWACT steps must be completed prior to SWACTing.

The LIMITED_PRESWACT command displays a warning:

```
Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", "N"):
```

163 Enter Y.

```
> Y
```

164 If the LIMITED_PRESWACT process halts, re-enter the following command to continue.

```
> LIMITED_PRESWACT
```

The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated by display of the following message:

```
Total execution time for all complete procedures
00:07:31.362
All LIMITED_PRESWACT steps completed
successfully.
```

165 Select the next step as follows

If the (inactive) Call Agent card is	Do
not connected to the ERS 8600 being upgraded	step 166
connected to the ERS 8600 being upgraded	step 180

Perform a NORESTARTSWACT

166 If the active Call Agent card is connected to the Ethernet Routing Switch 8600 to be upgraded, minimize the possibility of an outage by performing a NORESTARTSWACT.

a Check the status:

```
> BCSUPDATE:SWACTCI;STATUSCHECK
```

The following response displays:

```
SWACTCI:
Checking Nodes Status
STATUSCHECK successful
```

b Execute the NORESTARTSWACT.

```
> NORESTARTSWACT
```

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”):
>
```

c Enter a Y if the only alarm is an APPL simplex.

```
> Y
```

The final progress follows. Activity also switches at the Call Agent Manager.

```
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
```

d The telnet session to the active and inactive call processing applications are lost. Re-establish the connection. Refer to the Interface set in section Call Agent Upgrades for this procedure.

Perform a POSTSWACT

167 At the MAP display, enter the following command to run a Postswact through completion.

```
> BCSUPDATE;POSTSWACT
```

168 Enter Y when prompted at the CA_SYNC step.

```
> Y
```

Verify availability of NFS mounts on STORM

169 At the Call Agent Manager, query the NFS mounts to ensure that they are accessible on STORM 1.

```
> ccamtc
> coremtc
> sys
> querynfs
```

170 From the resulting screen display, verify that all mounts are accessible.

171 Select the next step as follows.

If all mounts	Do
are accessible	step 172
are not accessible	Refer to procedure “Verify NFS Availability” in section *Upgrading the STORM* in this document for details.

Return to service disk volumes on SD0X

172 Return to service all disk volumes connected to the Ethernet Routing Switch 8600 chassis that were upgraded.

```
> diskadm sd0N; rts all
```

where:

sd0N
is the STORM volume defined in Note 2 of step 83

Mount DIRP volumes

173 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 recommends recording all subsystems, volume, and variable information for each volume remounted in this step.

Use the IEMS GUI to unlock the MS 2000 node

174 Launch the IEMS GUI.

Note: Refer to NTP *Integrated EMS Basics*, NN10329-111, for details on logging into the IEMS GUI.

175 Select **Applications ---> Integrated EMS --->Network Elements**.

176 Select the MS 2000 Series node to be unlocked and right click on its icon.

177 Select the Config and Maintenance Tool from the pop-up menu.

The Config and Maintenance Tool launches.

178 From the left side of the Config and Maintenance Tool screen, click the **Unlock** button under the Lock State options to unlock the MS 2000 node.

179 Select the next step as follows:

If the Communication Server uses:	Do
an XA-Core	step 180
a Compact chassis	step 182

Use the XA-Core MAP terminal to enable Ethernet links with the Ethernet Routing Switch 8600:

180 Access the ETHR level of the MAP display by typing:

```
> MAPCI;MTC;XAC;ETHR
```

181 Refer to the tables below and enable the Ethernet link between the XA-Core and Ethernet Routing Switch 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 182

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 Ethernet Routing Switch 8600 CLI to reset VRRP priority settings and OSPF cost metrics:

182 Make sure Ethernet Routing Switch 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.

183 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 Repeat substep a for each VLAN prioritized on Chassis N.

c Use the following table to determine the next step.

If	Do
OSPF is configured	Substep d
otherwise	Substep f

d Reset the OSPF metrics by typing

```
config vlan <vid> ip ospf metric <value>
```

Note: See for the OSPF metric for <value>.Use the original metric value recorded in the Upgrading Ethernet Routing Switch 8600 software for the CS-LAN in step 5 on page 125.

The OSPF metrics reset to their original value.

e Repeat step d for each VLAN on Chassis N.

f Use the following table to determine the next step.

If	Do
BGP is configured	Substep g
otherwise	Substep h

g For each external BGP peer in the table above, execute the following command on the ERS 8600:

```
config ip bgp neighbor <external peer IP address> admin-state enable
```

Refer to the BGP neighbor IP address table in substep 5h on page 129.

h Save the new Ethernet Routing Switch 8600 configuration by typing:

Note: Before entering the sav config command, ensure sufficient free space exists in /flash (20% of total /flash size) to accommodate the configuration file.

```
sav config
```

This updates the new Ethernet Routing Switch 8600 configuration so that VRRP settings are maintained after any subsequent reboot.

i Re-enable the flag settings and save the bootconfig file.

```
config bootconfig flags verify-config true
sav bootconfig
```

184 Increment the iteration index (N = N+1), and select the next step as follows:

If	Do
N=1	step 12 (for second pass)
N=2	step 186

Note: In the second iteration (where N=1) when repeating steps step 12 through step 184, use Chassis X in place of Chassis N. Ethernet Routing Switch 8600 Chassis 1 (identified as Chassis N) is the slave and Ethernet Routing Switch 8600 Chassis 0 (identified as Chassis X) is the master.

185 Edit the object properties in the IEMS for the Ethernet Routing Switch 8600 to reflect the new software version. Refer to one of the following procedures to update the software version in the Device Version field.

- Editing and viewing object properties using Web Client on page 1846
- Editing and viewing object properties using Java Web Client on page 1841

186 The procedure is complete.

Multiservice Data Manager (MDM)

Before upgrading the Multiservice Data Manager

Perform the required prerequisite upgrade as follows:

Note: Upgrading the Ethernet Routing Switch 8600 is only required if currently on SN06.2. An upgrade is not required if currently on SN07.

Network	MDM applies to:	Previous Upgrade
ATM	PT-AAL1, UA-AAL1, PT-AAL2	Ethernet Routing Switch 8600 on page 94
IP	IAC- International, CHS - International, IAW, PT-IP and UA-IP [1]	Ethernet Routing Switch 8600 on page 94
Tri-Modal	all applications	Ethernet Routing Switch 8600 on page 94

1.Includes IP International: PT-IP and UA-IP

After upgrading the Multiservice Data Manager

Perform the next required upgrade as follows:

Network	MDM applies to:	Next Upgrade
ATM	PT-AAL1	CS 2000 Core Manager on page 303
	UA-AAL1 and PT-AAL2	Depending on configuration: CS 2000 Core Manager on page 303 Core and Billing Manager (CBM) 850 on page 455 (only if upgrading from SN07)
IP	IAC- International, CHS - International, IAW, PT-IP and UA-IP [1]	Depending on configuration: CS 2000 Core Manager on page 303 Core and Billing Manager (CBM) 850 on page 455 (only if upgrading from SN07)
Tri-Modal	all applications	Depending on configuration: CS 2000 Core Manager on page 303 Core and Billing Manager (CBM) 850 on page 455

1.Includes IP International: PT-IP and UA-IP

About the Multiservice Data Manager

For PT-AAL1, UA-AAL1 and UA-IP network applications, Multiservice Data Manager (MDM) provides the network element management for Multiservice Switch node. For the UA-IP network application, MDM also provides the network element management for the Media Gateway 15000. Nortel Networks Multiservice Data Manager (MDM) integrates, monitors and controls the Multiservice Switch portfolio.

These procedures are intended for people who are upgrading Nortel Networks Multiservice Data Manager (MDM) servers from MDM 14.2 or 14.3 to MDM 15.2 within the context of a Packet Trunking - AAL1 (PT-AAL1), Universal Access - AAL1 (UA-AAL1), or Universal Access - Internet Protocol (UA-IP) solutions upgrade from SN06 to SN08 or, from a MDM 15.1 to MDM 15.2 upgrade from SN07 to SN08.

Note: If you have upgraded from a pre-SN07 release to SN07 in an IP and Media Gateway solution and you comply to the MDM Succession feature baseline you can perform an SN07 to SN08 upgrade using the MDM upgrade procedure in this document. However, if you have not migrated to SN07, you must establish the MDM SN07 feature baseline first.

MDM server upgrade overview and prerequisites

This section describes the upgrade task flow, prerequisites that must bet met before starting an upgrade, and factors you must consider before performing an upgrade on MDM servers.

The upgrade task flow outlines the sequence of tasks required to upgrade one MDM server. After you have updated one server, repeat the process to upgrade the second server.

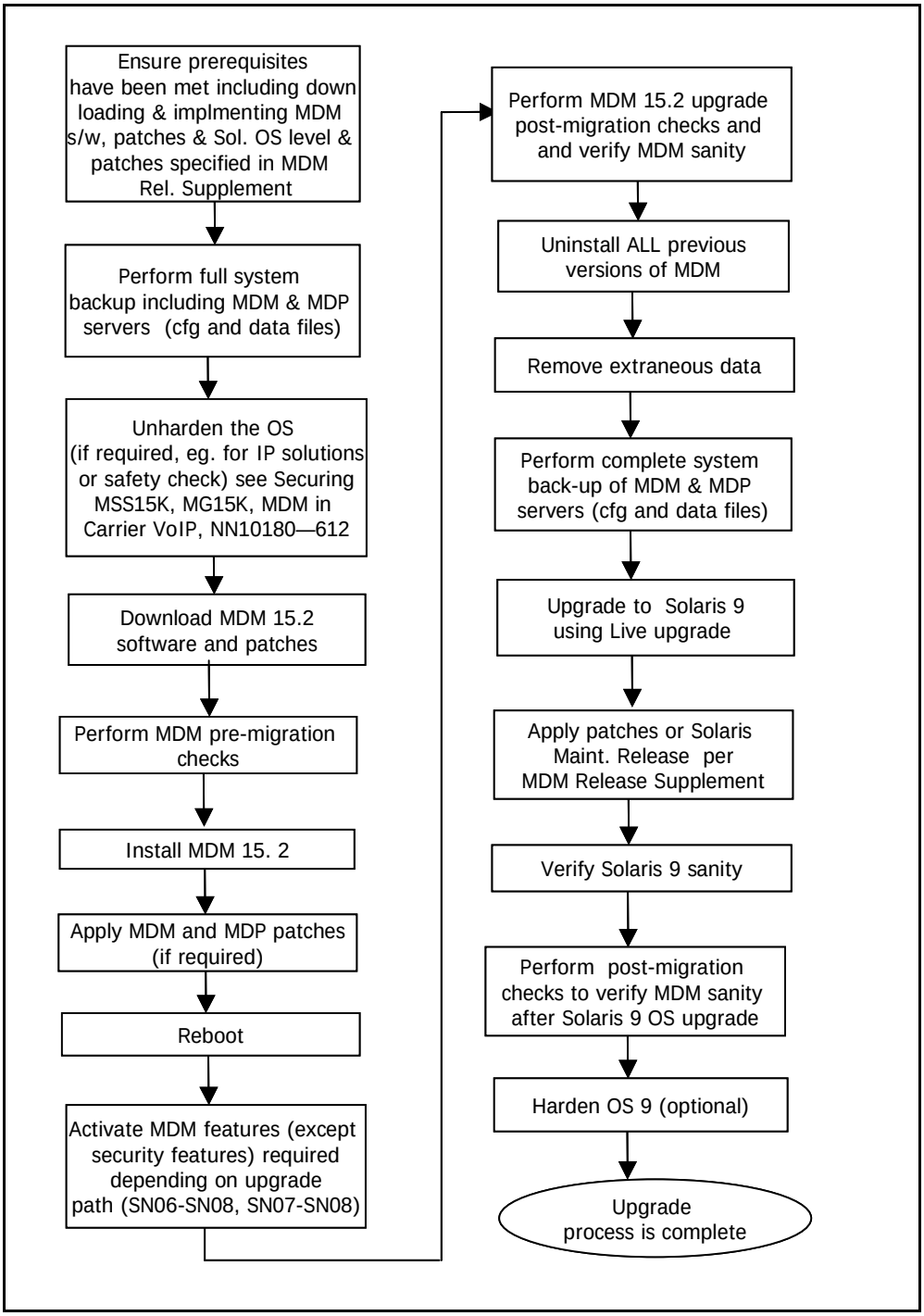
See:

- MDM server upgrade task flow on page 218
- Prerequisites to performing a server upgrade on page 220
- MDM deployment considerations on page 223
- Solution level migration logistics on page 225
- MDM Carrier Voice over IP feature baseline on page 227

MDM server upgrade task flow

The figure MDM server upgrade task flow on page 218 shows a high level outline of tasks required to upgrade a server.

MDM server upgrade task flow



Go to the following links for more information.

- Downloading and backing up node software on page 242
- Pre-migration checks for upgrading MDM servers on page 257
- MDM software installation on page 268
- Activating new features for MDM in SN08 on page 286
- Post-migration checks on page 296
- Upgrading the Solaris operating system on page 232

> ***Note:*** This section includes post-migration checks that must be performed after the Solaris OS 9 upgrade to ensure OS sanity.

After upgrading both servers, upgrade the MSS 15000/MG 15000 nodes. For more information, see NN10070-461 *Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1* and NN10419-461 *Upgrading Nortel Multiservice Switch 15000 and Media Gateway 15000/20000 in Carrier Voice over IP Networks*.

Prerequisites to performing a server upgrade

Before undertaking the upgrade, confirm that you have met the following prerequisites.

- You have read the *Multiservice Data Manager Release 15.2 Supplement* and Bulletin 2005005709 to determine the correct set of MDM patches and, you have implemented the patches indicated in the Supplement and Bulletin.
- You have read the Multiservice Data Manager Release 15.2 Supplement to determine the correct Solaris OS level and level of patches required before the MDM upgrade (Solaris 8 and patches must be at Solaris 8 level).
  - — After the MDM nodes have been upgraded, the Solaris OS must be upgraded to Solaris 9. Download Solaris 9 OS, the Solaris 9 Maintenance Release 9/04 and the Sun OS patches as specified in the Multiservice Data Manager Release 15.2 Supplement. The Sun Fire TM V480 server hardware has not changed during the upgrade to SN08.
- You **must** have extensive knowledge of Unix and MDM tools and software.
- Upgrade MDM servers before upgrading the MSS 15000/MG 15000 nodes they manage. MDM software is backwards compatible and can manage the current and previous releases of MSS/MG, but is not necessarily forward compatible. To upgrade Multiservice Switch 15000 nodes, see NN10070-461 *Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1* and NN10419-461 *Upgrading Nortel Multiservice Switch 15000 and Media Gateway 15000/20000 in Carrier Voice over IP Networks*.
- To ensure that one MDM server remains in contact with the CS2000 Core Manager, Integrated Element Management System (EMS), 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 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 or critical 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 MDM deployment within Carrier Voice over IP, which involves the configuration of a Sun Fire TM V480 servers located in the Network Operation Center.

  MDM, Multiservice Switch 15000 and Media Gatewayreleases for VoA and VoIP were aligned in SN07 and an MDM Carrier Voice over IP baseline configuration defined to achieve a consistent deployment. The baseline configuration must be achieved before performing an MDM 14.2, 14.3 or 15.1 upgrade to MDM15.2 in SN08. This section briefly discusses the baseline configuration for:

  — standalone/server

  — client-sets (optional)

  — Sun workstation configuration

  — MDM Carrier Voice over IP feature baseline

  See MDM deployment considerations on page 223 and Solution level migration logistics on page 225 for more information regarding standalone/server and client-sets baseline configuration. The Sun workstation configuration is covered in other points in this section.

  The MDM Carrier Voice over IP feature baseline on page 227 lists the features that must be activated before you upgrade to MDM 15.2.

- If you have deployed client-sets and are not re-deploying them as MDM Admin servers, upgrade them before completing the upgrade task flow described in MDM server upgrade task flow on page 218. See Activating new features for MDM in SN08 on page 286.

- If you have not deployed MDM servers according to the standard deployment, follow the upgrade task flow described in MDM server upgrade task flow on page 218 as a guideline, but selected steps may be different. Refer to the Multiservice Data Manager (MDM) base documentation and release notes for additional information.

- If you are upgrading MDM servers from CD-ROM, you must have an X11 terminal with IP connectivity to the Sun Fire TM 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 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.

- Review the *Multiservice Data Manager Release 15.2 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.
- 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 Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP*.
- You must have MSS/MG 15000 patch distribution schedule information that includes:
  - the time at which MSS/MG 15000 patch updates are put on the SDSs
  - the time intervals, which include the time of week, time of day, start, and end times, scheduled for MSS/MG 15000 patch applications to the switches
- You must have IP addresses for the SDM or Integrated EMS.

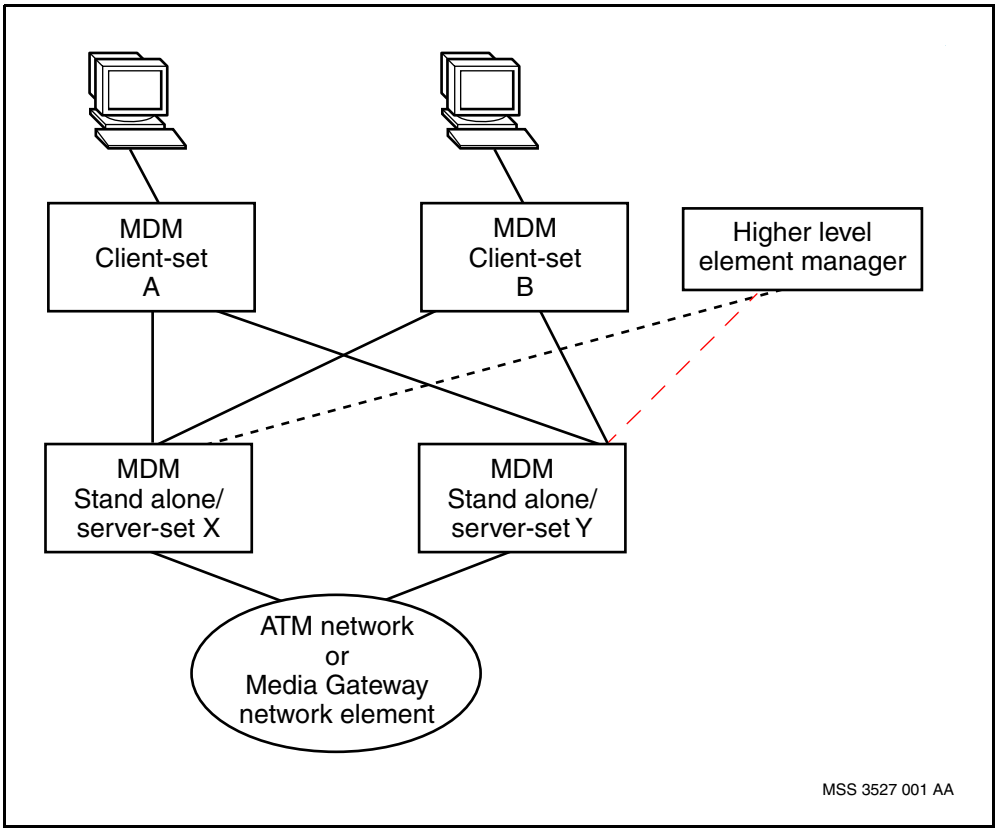
MDM deployment considerations

Since Nortel 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 MDM in a Carrier Voice over IP deployment. Some common Carrier Voice over IP deployment options are:

- stand-alone/server-set (combined server and client-sets)
- separate client-sets
- distributed server and client-sets
- MDM Admin Server (V0A only)
- MDM Server (VoIP only)

Typical client-set/standalone/server-set deployment on page 223 illustrates the common deployments. Note that the server and client-sets are deployed as a redundant pair.

Typical client-set/standalone/server-set deployment



Standalone/server-sets

Standalone/server-sets support the main server processes that allow MDM to perform surveillance and gather network data (fault and/or performance). They are usually run without a monitor and keyboard.

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 MDM nodes. Client-sets may host operator desk tops (remote users) as indicated in Typical client-set/standalone/server-set deployment on page 223.

Separate standalone/server and client-sets

While separate server and client-sets are not mandatory to Nortel MDM deployment, they do optimize performance in a large network.

Note: A single MDM supporting a VoA and VoIP (a tri-modal) configuration is not a Carrier Voice over IP supported configuration.

MDM Servers in VoIP

MDM Servers in a VoIP solution provide web access to Operator Client environment from remote operator desktops and X11 access to MDM Toolset environment. They support the main server processes for performing surveillance, gathering network data (fault, security, and/or performance), and provide network data to higher level management systems. They also provide an interface to the IEMS central AAA service and host the Java Web Start (JWS) server for the Operator Client user environment.

MDM Admin Servers in VoA solutions

MDM Admin Servers in a VoA solution provide web access to Operator Client environment from remote operator desktops and X11 access to MDM Toolset environment. They support the main server processes for performing surveillance, gathering network data (fault, security, and/or performance). They also host the central AAA service and the Java Web Start (JWS) server for the optional Operator Client user environment.

Solution level migration logistics

Before performing an upgrade, you must consider:

- redundancy (stand-alone/server-set, client-sets)
- impact on the OSS and the higher level element manager (this could be the CS2000 Core Manager (VoA) or Integrated EMS (VoIP))
- order of migration of the server vs.client-sets

Note: If an MDM server pair is managing multiple Carrier Voice over IP offices, you not required to migrate all Carrier Voice over IP offices prior to the upgrade of the MDM server pair.

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 system is running in simplex mode. To minimize the risk of losing the ability to observer the network and collect data, upgrade only one of the redundant servers (both server and client-sets) at any given time.

A Nortel 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 applications
- SDM and/or Integrated EMS
- client-set A
- client-set B
- Standalone/server-set A
- Standalone/server-set B
- Multiservice Switch and/or Media Gateway nodes

Note: For Carrier Voice over IP solution specific requirements, refer to the Solution level upgrade procedures.

Migrate the client-sets before the standalone/server-sets because 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 you will see an outage because clients do not dynamically switch from one client-set to another. This way, you can service select a client-set that is not actively being migrated. Migrate one standalone/server-set at a time.

MDM Carrier Voice over IP feature baseline

MDM features can be Carrier Voice over IP-specific, or not specific to Carrier Voice over IP. This section lists the features that are relevant to Carrier Voice over IP. These features are already installed for the current VoA customer base (UA-AAL1/PT-AAL1) who have upgraded to SN07, current ILEC UA-IP customers, and for those who have done a greenfield ILEC UA-IP installation in SN08 using the Installation Method.

For VoIP and Media Gateway customers **outside** these deployments, you must activate the features listed in table MDM In Carrier Voice over IP - baseline feature list on page 227. This table:

- lists the features that must be activated (appropriate to individual deployments)
- identifies the applicability of the feature to the server vs. client-sets
- identifies the Carrier Voice over IP release where the feature was introduced
- identifies the MDM release where the feature was introduced
- identifies where the feature originated from: MDM base or Carrier Voice over IP

Activate these features on MDMs in all Media Gateway installations to ensure compatibility with the MDMs managing the MSS 15000. You must establish this baseline before you can upgrade to MDM 15.2. If you are migrating from a SN06 release (MDM14.2 or 14.3) to MDM 15.2, you must activate the baseline configuration described in SN07 Helmsman documentation, plus the features described in MDM features new in SN08 on page 230. See Activating new features for MDM in SN08 on page 286 for additional information. (This document does not describe how to achieve the baseline configuration.)

MDM In Carrier Voice over IP - baseline feature list

Feature Name	Required for Solution?		Server or Client-set feature	Carrier Voice over IP Release	MDM Release	Originator
	VoA	VoIP				
Core functionality:						
MDM Patched to current level	Y	Y	server, client-set	all	all	MDM base
client-set servers	N	N	client-set	SN06.2	all	MDM base

MDM In Carrier Voice over IP - baseline feature list

Feature Name	Required for Solution?		Server or Client-set feature	Carrier Voice over IP Release	MDM Release	Originator
	VoA	VoIP				
Redundancy (server-set)	Y	Y	server, client-set	n/a	all	MDM base
Redundancy (client-sets- if deployed)	N	N	server, client-set	SN06.2	all	MDM base
Software Distribution Site	Y	Y	server (simplex)	all	all	MDM base
Data Collection (MDP)	Y	Y	server (simplex)	all	all	MDM base
Generating and setting secure passwords for MDM servers (FMDR, PMSP) password encryption	Y	Y	server	SN05	13.4	MDM base
Secure FTP	Y	Y	server	SN05	13.4	MDM base
Multiservice Switch backup and Restore	Y	Y	server	SN06	all	MDM base
Network Model & Viewer configuration	Y	Y	server	all	all	MDM base
MDP Administration enhancement	Y	Y	server	SN07	14.3	MDM base
Shelf View enhancement	Y	Y	client-set	SN07	14.3	MDM base
Server Administration enhancements	Y	Y	server	SN07	14.3	MDM base
Additional features:						
XNTP Support	Y	Y	server, client-set	all prior to SN07	all prior to 15.1	MDM base
Network Time Protocol Support	Y	Y	server, client-set	SN07	15.1 and later	MDM base
FDTM Succession configuration	Y	Y	server	SN02	13.1	Carrier VoIP

MDM In Carrier Voice over IP - baseline feature list

Feature Name	Required for Solution?		Server or Client-set feature	Carrier Voice over IP Release	MDM Release	Originator
	VoA	VoIP				
Support for Seasonal time change	N	N	server	SN06	14.2	Carrier VoIP
pserver process	Y	Y	server	SN04	13.3	MDM base
NP template installation	Y	Y	server	SN04	13.3	MDM base
Multiservice Switch 15000 Configuration Model Server	Y	Y	server	SN06	14.1	MDM base
MDP to make BDF files accessible	Y	Y	server	SN06	14.1	MDM base
MDP file prober collection times	Y	Y	server	SN06	14.1	MDM base
Succession Enabling	Y	Y	client-set	SN06	14.1	Carrier VoIP
Note: Enabling Succession also ensures that the SASM and SISM tools appear in the MDM toolset.						
PMs (pmsp & supporting directory structures)	Y	Y	server	SN06	14.1	Carrier VoIP
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
Support for 5 min. PMs	Y	Y	server	SN07	15.1	Carrier VoIP
SASM	Y	N	server	SN06	14.2	Carrier VoIP
Succession Release Name GUI	Y	Y	server	SN07	15.1	Carrier VoIP

New features in SN08

Nortel Multiservice Data Manager (MDM) base features added in SN08 are from the MDM 15.1 and MDM 15.2 releases. Table MDM features new in SN08 on page 230 lists all of the new features for SN08.

Note: Activating these features completes the MDM 15.1 to MDM 15.2 upgrade.

MDM features new in SN08

Feature Name	Required for Solution?		Server, client-set or MDM Admin Server impact	Carrier VoIP Release	MDM release	Originator
	VoA	VoIP				
Operator client (OC)	N	Y	MDM Admin server, Operator Client	SN08	15.1	MDM base
Centralized user management	Y if OC is used	Y if Inte-grated EMS is used	MDM Admin server	SN08	15.1	MDM base
Security Audit logging	Y	Y	server	SN08	15.1	MDM base
SCC2 SALs	Y	Y	server	SN08	15.2	Carrier VoIP
Nodal Provisioning Template Audit	Y	Y	server	SN08	15.2	Carrier VoIP
OS hardening	N	N	client-set, server, MDM Admin server	SN08	15.1	MDM base
SSH	N	Y	server, MDM Admin server	SN08	15.1	MDM base
IPSec	N	Y	server, MDM Admin server	SN08	15.1	MDM base
HSM Migration (UA-IP MG)	n/a	Y	server	SN08	15.2	Carrier VoIP
MDM auto-patch of MSS/MG nodes	Y	Y	server	SN08	15.1	MDM base

MDM features new in SN08

Feature Name	Required for Solution?		Server, client-set or MDM Admin Server impact	Carrier VoIP Release	MDM release	Originator
	VoA	VoIP				
Solaris 9 Upgrade	Y	Y	server, client-set, MDM Admin server, Operator client (UNIX)	SN08	na	Carrier VoIP
Note: Perform the Solaris 9 upgrade after upgrading MDM.						

Upgrading the Solaris operating system

The operating system on the MDMs for this release must be upgraded from Solaris 8 to Solaris 9 after the MDM 15.2 upgrade has been performed and the system verified as sane. SN06 and SN07 currently run on Solaris 8. The Solaris 9 upgrade must be performed before deploying MDM Admin Servers for centralized authentication and authorization in an Operator Client environment.

Upgrading with Live Upgrade

Use Live Upgrade to upgrade Solaris operating systems. MDM is a flexible system that supports different deployments, therefore, the migration needs to be performed on each MDM in each set. The following server sets and client-sets are deployed as redundant pairs:

- distributed server and client-set server
- separate server and client-set server
- stand-alone (combined server and client)

Note: Upgrade the client-sets followed by the server sets.

The Live Upgrade feature provides both a command-line interface (CLI) and a character-based interface (CUI). Use the command-line interface to perform the upgrade. The CUI does not have the full feature set of the CLI and there are limitations on using it remotely.

In normal operation the Solaris operating system runs in one boot environment (BE). Live Upgrade creates a clone of the BE for an upgrade. The two BEs are the active boot environment (BE) and the alternate boot environment (ABE). The upgrade uses the (ABE), which is a clone of the current OS, to perform the OS upgrade without any impact on the OS that is running in the BE. The main requirement is that each BE have enough disk space for its own root partition.

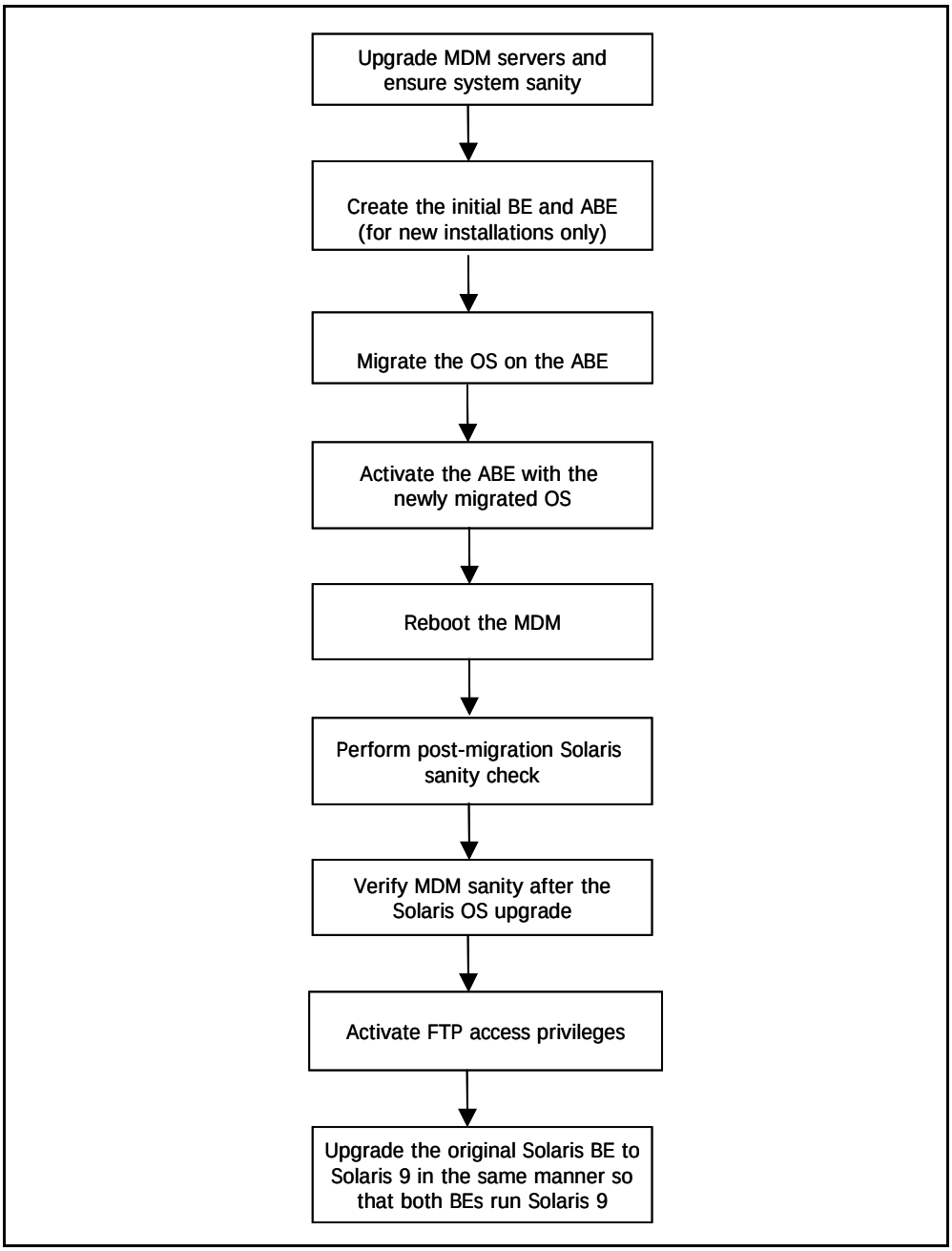
The naming convention used to identify the two BEs is as follows:
`Solaris<release number>_<mmyy>`
As an example, Solaris8_0703 corresponds to the Solaris 8 release dated 07/2003. The Live Upgrade utilities make use of the two logical names to identify the BE that is being manipulated.

All the new Solaris OS software is installed in the ABE while the current Solaris OS continues operating in the boot environment (BE). Once the new Solaris OS is installed in the ABE, it is activated in the ABE. At this point you must test the ABE to see if there are any problems.

Make sure that all the Post-migration checks on page 296 have passed in the BE before upgrading the ABE. If there are no problems, reboot (init 6) the ABE. The new Solaris OS does not become functional until after a reboot. If you find there is a problem after both BEs are at the new version of Solaris OS, you will need to uninstall the new version and re-install the old version in the BEs, then start the upgrade again.

The workstation is fully available to users throughout this entire procedure with the exception of the reboot. See the Workflow for Solaris 9 upgrade on page 234 strategy.

Workflow for Solaris 9 upgrade



CAUTION
Rolling back after an MDM 15.2 software upgrade
Once both boot environments have been updated to Solaris 9, you can only rollback to MDM 14.2 or MDM 14.3 by re-installing Solaris 8.

When you create an initial BE from the current OS, two boot environments are created:

- one for the current OS named Solaris8_0703 for example
- one clone of the current OS named Solaris9_0404 for example, which is used for the upgrade

  In subsequent upgrades, this step is omitted. The ABE created here can be used to perform the upgrade.

Prerequisites to performing the Solaris upgrade

Ensure the following prerequisites are performed prior to the upgrade:

- Verify the current OS, OS maintenance release and patch level are at the correct level. The OS must be at Solaris 8 and the patches must be at patch level for Solaris 8 before you upgrade to Solaris 9. Use the command:

  cat /etc/release

- You have downloaded the Solaris 9 operating system, Solaris 9 Maintenance Release 9/04, and the Sun OS 9 patches as specified in the Multiservice Data Manager Release 15.2 Supplement.
- Install and implement patches for the current OS (if required). See the *Multiservice Data Manager Release 15.2 Supplement* to determine the latest set of patches.
- Both 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 or critical 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 you proceed with the upgrade.
  - Verify that you can access the MSS/MG15000 using Command Console.
  - If using disk mirroring, it must be enabled on both servers and operating without any errors.
- Both MDM servers must have been upgraded to MDM 15.2.
- Disable disk mirroring using the Sun documentation for disk mirroring provided in “Solaris Live Upgrade 2.0 Guide“, Sun Microsystems, 2004
  http:// www.sun.com/software/solaris/liveupgrade
- Disable volume managers using the vendor information and Sun information provided in “Solaris Live Upgrade 2.0 Guide“, Sun Microsystems, 2004
  http:// www.sun.com/software/solaris/liveupgrade
- Create disk partitions using the Sun documentation (if required).
- Unharden the OS.
- Backup system and user data. Refer to NN10180-611 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice*

Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP.

- Install Live Upgrade packages using the Sun documentation, go to the Sun Microsystems Documentation Center at: http://www.sun.com/documentation

Upgrading to Solaris 9

1 Obtain the required software from Sun Microsystems Inc.

2 Install the Solaris 9 operating system according to the instructions provided in “Solaris Live Upgrade 2.0 Guide“, Sun Microsystems, 2004
http:// www.sun.com/software/solaris/liveupgrade.

Note: If the documentation is not available or to ensure that the latest documentation was provided, go to the Sun Microsystems Documentation Center at ‘http://www.sun.com/documentation’.

ATTENTION
When installing Solaris 9, choose “Entire distribution plus oem support 2.2" to ensure that SSH and IPSec are installed. The “End User system support 2.3" option does not include these packages. IPSec and SSH are required for the Security feature.

Post migration checks

Ensure the following post migration checks are performed after the upgrade:

- Verify that the OS is at Solaris 9, Solaris 9 Maintenance Release 9/04 and the OS patch levels are at the level specified in the *Multiservice Data Manager 15.2 Release Supplement*. Use the command:

  `cat /etc/release`

> **ATTENTION**
> SPFS SN08 includes an upgrade from Solaris 8 to Solaris 9. Some configuration files are not updated from the Solaris 8 defaults. When a full filesystem restore is performed it attempts to use the Solaris 9 defaults, leaving the system in an unstable state. Patch JFJ40OZ8 should be applied immediately. Take a fresh full filesystem backup after applying the patch.

- Verify MDM sanity:
  - — Both servers must be in service, operating in a redundant capacity, and capable of supporting traffic and network management functions with no major or critical alarms.
  - — Check the Alarm Display and the System Log Display tools and ensure there are no serious or unexplained logs or alarms.
  - — Verify that you can access the MSS/MG15000 using the Command Console.
  - — If using disk mirroring, it must be enabled on both servers and operating without any errors.
- Test the BE in the case that you may be required to revert back to the previous OS.
- Perform the procedure Activating FTP access privileges on page 240.
- Enable disk mirroring using the Sun documentation. Refer to “Solaris Live Upgrade 2.0 Guide“, Sun Microsystems, 2004 (http:// www.sun.com/software/solaris/liveupgrade).
- Enable volume managers using the vendor information and Sun information. Refer to “Solaris Live Upgrade 2.0 Guide“, Sun Microsystems, 2004 (http:// www.sun.com/software/solaris/liveupgrade).
- Harden the OS, if necessary. Refer to NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice*

Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements.

Activating FTP access privileges

MDM requires proxy FTP to receive spooled data (SCN, alarms and logs) from the MSS. If the destination server (MDM) where the data file is going is running Solaris 9, configure the file /etc/ftpd/ftpaccess.

Activating FTP access privileges

1 Create the following entries in the file: /etc/ftpd/ftpaccess

port-allow realusers 0.0.0.0/0

port-allow guestusers 0.0.0.0/0

pasv-allow realusers 0.0.0.0/0

pasv-allow guestusers 0.0.0.0/0

Creating a `port-allow <class> 0.0.0.0/0` entry prevents FTP from checking the IP address of the port command from any address.

Rollback to previous Solaris version before activation of the new Solaris version

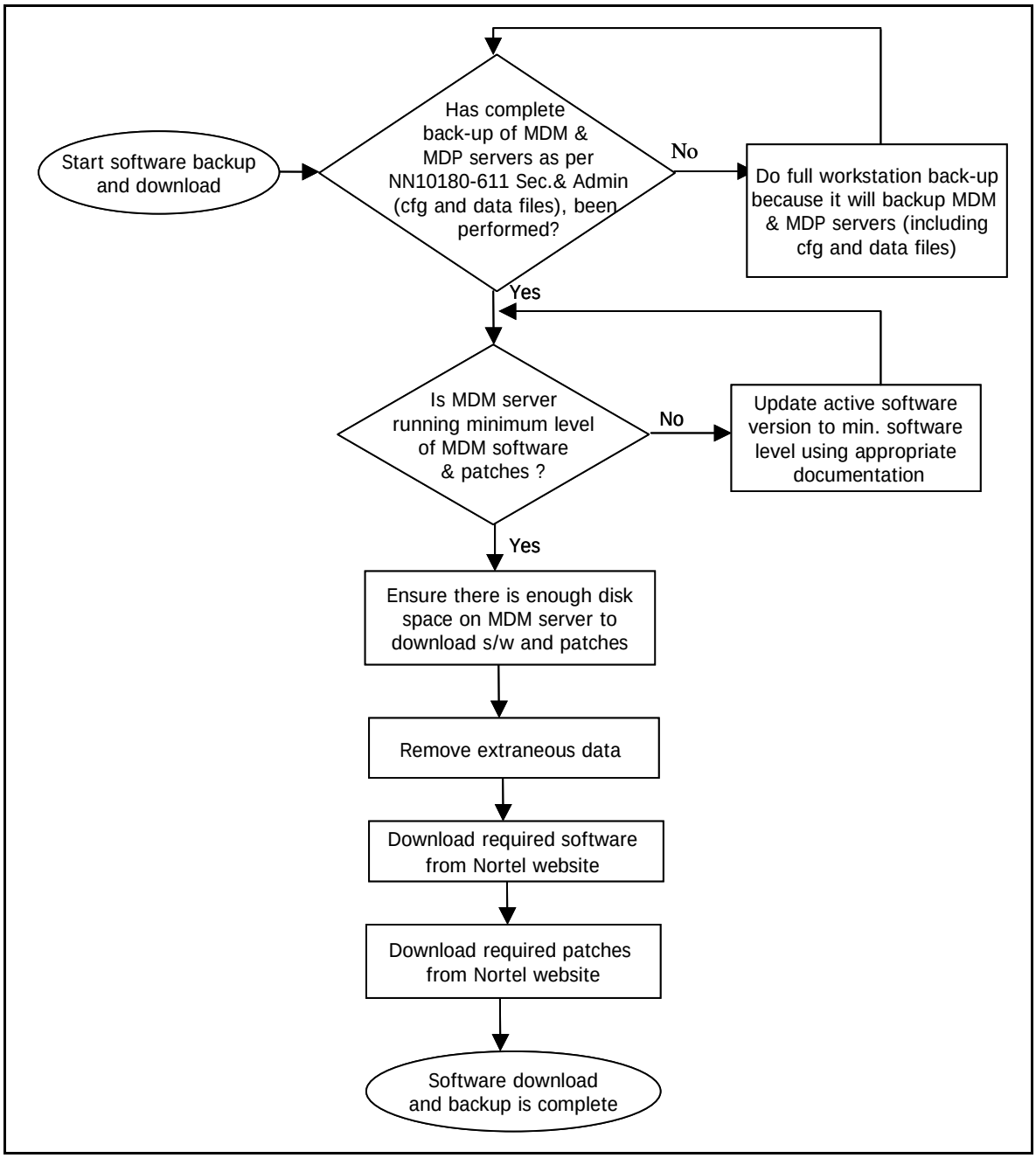
If testing indicates that there are problems with the new OS, activate the BE that hosts the old version of the Solaris OS and then reboot according to the Sun documentation. Refer to “Solaris Live Upgrade 2.0 Guide“, Sun Microsystems, 2004 (http:// www.sun.com/software/solaris/liveupgrade).

CAUTION
Do not perform a manual OS sync.
Differences between Solaris OS versions can be destructive. Do not perform a manual OS sync and make sure that you use init 6 or shutdown for reboots.

Downloading and backing up node software

The following figure displays the sequence of tasks you must perform to do a complete system backup and download Nortel MDM software and patches.

MDM Downloading and backing up software task flow



Perform the following procedures before installing MDM software and patches:

- Performing a complete system backup on page 244
- Checking the currently active software version on page 249
- Ensuring that there is enough disk space on the servers on page 250
- Downloading MDM software from Nortel website on page 253
- Downloading MDM patches from Nortel website on page 255

Performing a complete system backup

Perform a full system backup before starting the MDM upgrade. See the NN10180-611 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP* guide for information on how to perform a full system backup.

During the MDM upgrade, the contents of the /opt/MagellanMDP/data and the /opt/MagellanMDP/cfg subdirectories may be overwritten. The /opt/MagellanNMS/data and /opt/MagellanNMS/cfg are affected as well.

Note: It can take some time to back up these directories depending on their size.

Back up the entire disk partition on which the MDM software resides. If a disk partition backup has not been done recently, back up the directories listed in MDM directories to save on page 244. Save the indicated directories to a location on another workstation or on a temporary storage device so that if you encounter problems during the upgrade, you can restore the information stored in those directories.

MDM directories to save

Directory	Description
/opt/MagellanNMS/cfg	MDM base software configuration.
/opt/MagellanNMS/data	MDM base software data.
/opt/nortel/EPIC/cfg	Supports the Enhanced MSS Interface Controller. MDM release 14.1 and above.
/opt/nortel/WMS/cfg	Supports Web NMS tool. MDM 14.3 and earlier.
/opt/nortel/DVR/cfg	Supports the Data Viewer tool. MDM 14.2 and earlier.
/opt/nortel/config	Supports the Admin Server MDM release 15.1 and above.
/opt/nortel/data	Supports the Admin Server MDM release 15.1 and above.
/opt/nortel/logs	Supports the Admin Server MDM release 15.1 and above.

MDM directories to save

Directory	Description
/opt/MagellanMDP/cfg	MDP base software configuration. Backup is only required if MDP is installed.
/opt/MagellanMDP/data	MDP base software data. Backup is only required if MDP is installed.

Refer to the NN10180-611 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP* guide for more information.

Prerequisite

Before performing a backup, remove extraneous data. Refer to Ensuring that there is enough disk space on the servers on page 250 to identify obsolete software and data.

Backing up MDM information

1 Log in to the MDM workstation as user ID root.

2 Back up the MDM configuration and data information.

a Back up the MDM software configuration files.

cd /opt/MagellanNMS/cfg

tar cvfp mdmcfg_<release>.tar ./*

mv mdmcfg_<release>.tar <safe directory>

where

<release is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

b Back up the MDM software data files.

cd /opt/MagellanNMS/data

tar cvfp mdmdata_<release>.tar ./*

mv mdmdata_<release>.tar <safe directory>

where

<release is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

c If this MDM workstation includes the Management Data Provider (MDP) software, back up the MDP software configuration files.

cd /opt/MagellanMDP/cfg

tar cvfp mdpcfg_<release>.tar ./*

mv mdpcfg_<release>.tar <safe directory>

where

<release is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

3 If this MDM workstation includes the Management Data Provider (MDP) software, back up the MDP data files.

cd /opt/MagellanMDP/data

tar cvfp mdpdata_<release>.tar ./*

mv mdpdata_<release>.tar <safe directory>

where

<release is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

4 If this MDM workstation uses MDM 15.1 or above, back up additional MDM software configuration files.

a **cd /opt/nortel/config**

tar cvfp nortelconfig_<release>.tar ./*

mv nortelconfig_<release>.tar <safe directory>

where

<release is the MDM software release (for example, 151)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

b If this MDM workstation uses MDM 15.1 or above, back up additional MDM software data files.

cd /opt/nortel/data

tar cvfp norteldata_<release>.tar ./*

mv norteldata_<release>.tar <safe directory>

where

<release> is the MDM software release (for example, 151)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

c If this MDM workstation uses MDM 15.1 or above, back up the MDM log files.

cd /opt/nortel/logs

tar cvfp nortellogs_<release>.tar ./*

mv nortellogs_<release>.tar <safe directory>

where

<release is the MDM software release (for example, 151)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

5 If this MDM workstation uses MDM 14.1 or above, back up the EPIC configuration files.

cd /opt/nortel/EPIC/cfg

tar cvfp nortelEPICcfg_<release>.tar ./*

mv nortelEPICcfg_<release>.tar <safe directory>

where

<release is the MDM software release (for example, 151)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

6 If this MDM workstation uses MDM 14.3 or earlier, back up the WMS configuration files.

cd /opt/nortel/WMS/cfg

tar cvfp nortelWMScfg_<release>.tar ./*

mv nortelWMScfg_<release>.tar <safe directory>

where

<release> is the MDM software release (for example, 14.3 and earlier)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

7 If this MDM workstation uses MDM 14.2 or earlier, backup the DVR configuration files.

cd /opt/nortel/DVR/cfg

tar cvfp nortelDVRcfg_<release>.tar ./*

mv nortelDVRcfg_<release>.tar <safe directory>

where

<release> is the MDM software release (for example, 14.2 and earlier)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

Checking the currently active software version

To determine if Nortel 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 *MDM151xxx*, proceed with the upgrade.

Note: For additional information on locating and downloading MDM patches, see Downloading MDM patches from Nortel website on page 255. For information on MDM patches and how to list the most recent patches, see Installing MDM patches on page 280.

Ensuring that there is enough disk space on the servers

If you will be using Nortel ESD page to download the software (not installing it from a CD), ensure that you have sufficient disk space to accommodate the downloaded software.

Increase the available disk space by removing obsolete MDM software and data. Some of the MDM directories that can contain obsolete software and data are listed in the table Obsolete software and data on page 251.

Checking server disk space

From the MDM server

1 Log in. See Logging into MDM platform on page 295.

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/d06196234182399743102750 30%     /
fd           0       0       0       0%      /dev/fd
/dev/md/dsk/d40188656717822016517500 10%     /var
```

Note: 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 *MDM supporting PP15K* entry in *Multiservice Data Manager Release 15.2 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 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: When you delete obsolete MDM packages to increase server space, your configuration is not lost because MDM software configuration is persistent. The MDM does not delete the contents of the cfg and data directories. However during an upgrade, the files may be overwritten and altered as cfg and data information is migrated into a format appropriate for the new release.

Obsolete software and data

Directory	Description
Older versions of MDM software	/opt/MagellanNMS/loads/<software_loadname>/
old Passport data models	/opt/MagellanNMS/cfg/PassportSchema/
old Network Models	/opt/MagellanNMS/data/model/nmf/
RTAC alarm files	/opt/MagellanNMS/data/rtac/data
old backup data	/opt/MagellanNMS/data/Backup_Data
MDM software patch temporary files	files located in /tmp

Retrieving MDM software and patches from a drop box

After verifying that the server has sufficient disk space, you can begin to download Nortel MDM software. 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

The prerequisites are as follows:

- You need a dropbox and an account with a user name and password. Contact your Nortel customer representative for more information on accessing Nortel website.
- You must have performed the procedure: Ensuring that there is enough disk space on the servers on page 250.
- Refer to the software downloads area of Nortel website (*www.nortel.com*) to verify that the drop box contains the software files you need to retrieve. If there are no patches listed for this release, then there are no patches currently required for this release.

Retrieving software from a drop box

From the MDM server

1 Log in. See Logging into MDM platform on page 295.

2 Retrieve the required software files and patches according to your retrieval procedure:

- MDM 15.2 Supplement
- MDM15.2 CD1
- MDM 15.2 CD2
- MDM 15.2 CD3
- MDM Enhanced Security (if the MDM Enhanced Security package is ordered)

Downloading MDM software from Nortel website

After verifying that the server has sufficient disk space, begin downloading software. One method is to download the required software from Nortel website. When you download the software from this website, a copy of the software is placed in the directory you specify.

Prerequisites

You must have:

- Referred to the software downloads area of Nortel website *www.nortel.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.
- Downloaded all the software files that belong to the release you require. The software you need to download may be composed of more than one file.
- Downloaded the associated patches after downloading the required software release from the website. For more information, see Downloading MDM patches from Nortel website on page 255.
- Performed the procedure: Ensuring that there is enough disk space on the servers on page 250.

From the MDM server

1. Log in. See Logging into MDM platform on page 295.
2. Change directories to the / directory: **cd /**
3. Create a directory to which you can download the software: **mkdir MDM152**

   Note: Remove this directory at the end of the installation procedure.
4. On the web, go to *www.nortel.com*.
5. In the Support & Training section of the window, select *Software Downloads*.
6. In the Product Family section of the Software Downloads window, select *Preside*.
7. Under the Multiservice Data Manager for Succession PT/UA-AAL1 section, click *Software*.

   Note: This link is used for all solutions, IP and PT/UA-AAL1.

   The Software Downloads window opens.

8 The loads and patches for the release are identified at *www.nortel.com*

Note: Software loads are contained in zip files, while each patch is contained in a single file. The MDM 15.2 Supplement is found under the Documentation tab. The software is found under the Software tab.

9 Select the version of the release of the software you want to download. Download the following software

- MDM R15.2 Supplement
- MDM 152 CD1
- MDM 152 CD2
- MDM 152 CD3
- MDM Enhanced Security (if required)

10 Enter the following directory to indicate where you want the software load files placed: */MDM152*.

11 When prompted, enter your user name and password for the log in.

12 Click *Save*.

13 On the MDM server, change directories to the directory containing the software:

cd /MDM152

14 Uncompress the software load file:

uncompress <swload_name>.tar.Z

15 Untar the software load file: **tar xvf <swload_name>.tar**

16 Repeat step 14 through step 15 for every software file you downloaded.

17 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 MDM patches from Nortel website

In addition to the main software release, you may need to download patches from Nortel website to the 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 must have

- A dropbox and an account with a user name and password. Contact your Nortel customer representative for more information on accessing Nortel website.
- Refer to the software downloads area of the website *www.nortel.com* to determine which patches you need to download.

  Note: Consult the Release Notes for this release to identify the most current list of patches you require. 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.

- Performed the procedure: Ensuring that there is enough disk space on the servers on page 250.

From the MDM server

1. Log in — see Logging into MDM platform on page 295.
2. Change directories to the / directory: **cd /**
3. Create a directory to download the software to: **mkdir patch152**

   Note: Remove this directory when the patches are installed.
4. On the web, go to *www.nortel.com*.
5. In the Support & Training section of the window, select *Software Downloads*.
6. In the Product Family section of the Software Downloads window, click *Preside*.
7. Under the Multiservice Data Manager for Succession PT/UA-AAL1 section, click *Software*.

   Note: This link is used for all solutions, IP and PT/UA-AAL1.

   The Software Downloads window opens.
8. Refer to the software downloads area of Nortel website (*www.nortel.com*) to determine which patches you want to download.

9 Download and implement the following patches if you are upgrading from MDM 15.1 to MDM15.2:

Note: If you are upgrading from MDM14.2 or 14.3 to MDM15.2, you do not require these patches. Go to step 10.

- MDM151_NNAUTHEN_4.2.0_2004_WK48: PATCH
- MDM151_NNDESKTOP_4.2.0_2004_WK50: PATCH
- MDM151_NNLOGBWSR_1.0.0_2004_WK48: PATCH
- MDM151_NNSECUI_1.0.0_2004_WK50: PATCH

See Bulletin 2005005709 for more information.

10 When prompted to log in, enter your user name and password for the log in.

11 Click on the file listed beside the File Download heading.

12 Enter the following directory to indicate where you want the patch placed: **/patch152**

13 Click *Save*.

14 Repeat steps 12 through 13 for the other patches you need.

Pre-migration checks for upgrading MDM servers

Before starting to upgrade Nortel Multiservice Data Manager (MDM) servers, you must verify that the servers are in a state that will permit the upgrade.

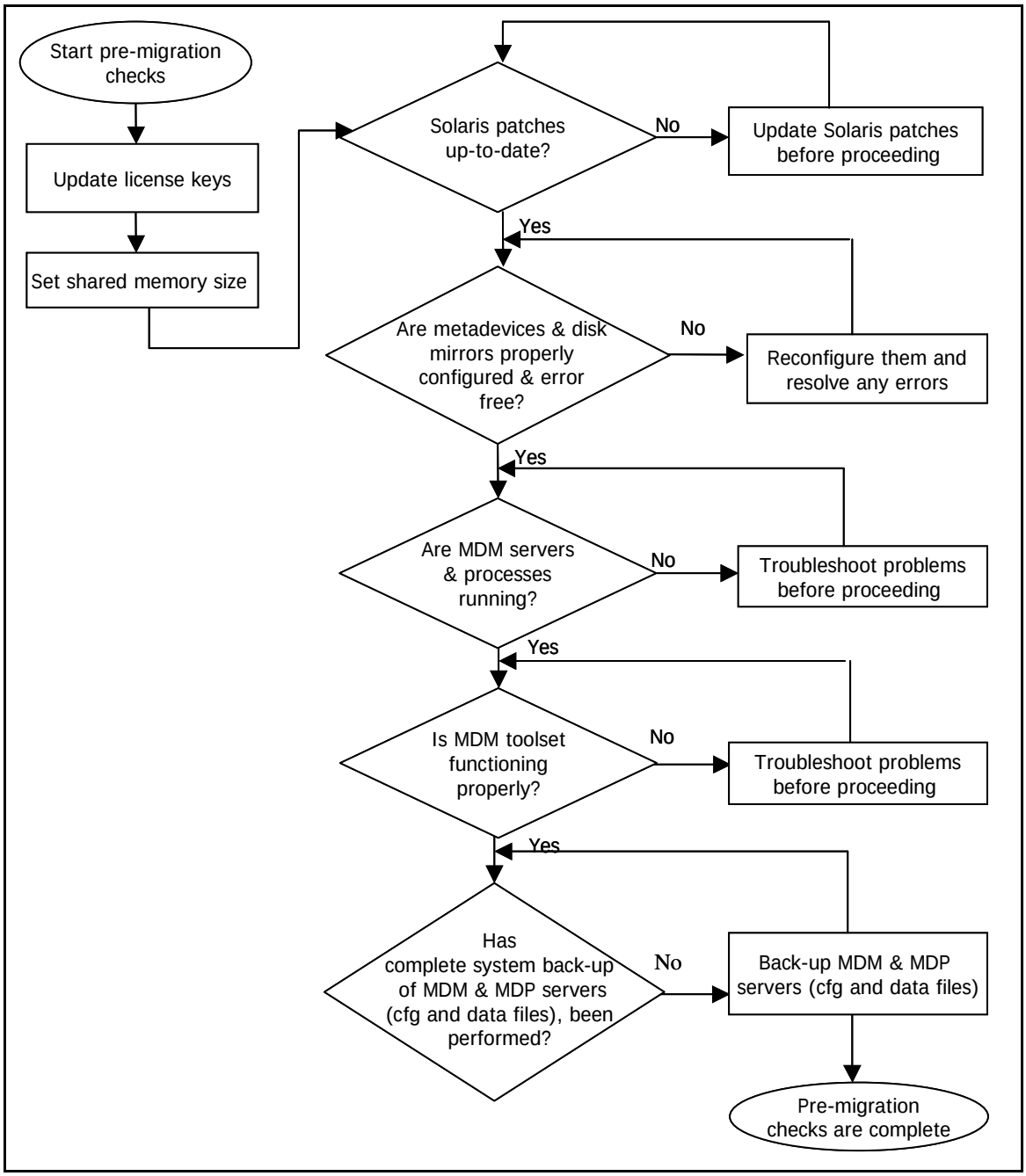
Prerequisites

You must have:

- extensive knowledge of UNIX, MDM tools and software.
- 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.
- ensured that the prerequisites in Prerequisites to performing a server upgrade on page 220 have been met.
- performed a full backup of the MDM workstation. Refer to NN10402-600 *ATM/IP Solution-level Security and Administration* guide.

The figure MDM pre-migration checks task flow on page 258 shows you the sequence of procedures you must perform to determine the status of the servers.

MDM pre-migration checks task flow



To link to one of the pre-migration procedures, click on one of the following:

Updating MDM license files

Before you can run MSS MDM server software, you need a license password and a customer identifier. This comes with your MSS 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 *Nortel Multiservice Data Manager Software Installation and Initial Configuration*. If you do not have the license, you will need to order one. Contact your Nortel Sales Representative for additional information.

MDM15.2 is available as an Entry or Comprehensive package. Other MDM optional features such as MDP are offered as well.

The MDM Operator Client and centralized user management is an optional feature. The number of Operator Client sessions and active Sun ONE Identity Server (IS) users dictates sizing requirements. You can order a 10 Client/100 user package, a 50 Client/500 user package, or a 100 Client/1000 user package. A license is required for Operator Client User Administration.

In previous releases, the MDM Entry and Comprehensive packages included the software CD ROMs and the Electronic Software Download (ESD) entitlement in addition to the license component. In MDM15.2, the Entry and Comprehensive packages now only include the License RTU component. A separate order code for the MDM Software CD ROM set is provided and must be ordered separately if required. Electronic Software Distribution will only be available to users with valid support agreements

Software license keys are provided based on the features ordered, and on a per site basis. Users migrating from MDM 14.2 or earlier must obtain a new key for MDM R15.x installations. Keys for previous releases will not work. The MDM Enhanced Security packages contains security software and functionality and must be ordered separately. See the *Multiservice Data Manager Release 15.2 Supplement* for more information on packaging and licensing.

Setting the shared memory size

Before beginning the upgrade, you need to set the shared memory size to the value 256.

Prerequisites

- Check the *Multiservice Data Manager Release 15.2 Supplement* to determine if the specific value should be greater than 256.

Setting the shared memory size

From the MDM server

1 Log in - see Logging into MDM platform on page 295.

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 MDM 15.2 upgrade, determine if the Sun workstation OS is at the right level with the correct patches. The correct OS version before starting the MDM upgrade is Solaris 8. Check the *Multiservice Data Manager 15.2 Release Supplement* to determine which Sun OS patches you should install before performing the MDM upgrade. Use the supplement that was obtained from the Electronic Software Distribution (ESD) page (*www.nortel.com*).

Verifying Solaris and its patch level

From the MDM server

1. Log in - see Logging into MDM platform on page 295.
2. Open an xterm session.
3. Check what release of OS is currently running on the workstation:

   cat /etc/release

   If the OS version is less than Solaris 8, an upgrade to Solaris 8 is required. An example of a Solaris <OS version> <release> output is as follows:

   ```
   Solaris 8 HW 7/03 s28s_hw3wos_05a SPARC
   ```

   In the example, the OS version is Solaris 8 with a version date of 7/03.
4. Compare the output with the Solaris Maintenance Releases as specified in the *Multiservice Data Manager 15.2 Release Supplement*.
5. If the OS version is equal to the OS version as specified in the *Multiservice Data Manager 15.2 Release Supplement*, an upgrade is not required.

   If the OS version is less than the version specified in the *Multiservice Data Manager 15.2 Release Supplement*, you must install the correct version of the Solaris OS Maintenance release. Refer to the *Multiservice Data Manager 15.2 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 MDM servers and processes are running

The state of Nortel 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 MDM server

1 Log in — see Logging into MDM platform on page 295.

2 Open a MDM window — see Opening the MDM Toolset on page 295.

3 From the 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 *Nortel Multiservice Data Manager Server Reference* 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 MDM window choose System -> Administration -> GMDR Administration.

Note: For more information, see Using the GMDR Administration tool in the 241-6001-303 *Nortel Multiservice Data Manager Customization and Administration*.

10 Ensure that there are two FMDR servers for every distinct Carrier Voice over IP office, and two OAMC 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.

Verifying that the MDM toolset is functioning

During a pre-migration check, perform the following procedure to verify that Nortel Multiservice Data Manager (MDM) processes are working correctly.

Verifying MDM toolset is functioning

From the MDM server

1. Log in, see Logging into MDM platform on page 295.
2. Open a 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 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 MDM window, select Fault > Network Viewer.
   a. From the 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 MDM window, select Configuration > 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 MDM.

13 From the MDM toolset, select the help menu and choose the *On Window* menu item. Ensure that the Help system opens.

MDM software installation

This module contains:

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 MDM server, communication from this server to the CS2000 Core Manager or Integrated EMS, and the Multiservice Switch network stops. The other MDM server reports alarms as long as the server being upgraded is out of service.

Load balancing between MDM servers is not available and the MDM platform compliance to connectivity standards cannot be met during the upgrade.

Prerequisites to installing MDM software

Before installing new Nortel Multiservice Data Manager (MDM) software and patches, you must have:

- extensive knowledge of UNIX and MDM tools and software
- removed extraneous software and data
- backed-up the entire disk partition on which the MDM software resides. If a disk partition backup has not been done recently, backup the directories listed in Backing up MDM information on page 245.
- an understanding that the upgrade procedure uses the software installation tools and procedures that are packaged with Multiservice Data Manager 15.2 release. MDM software will not support copying the software, configuration, or data from one server to the other. This approach would cause MDM references and process calls to fail.
- ensured that the correct version of Solaris and Sun OS patches are installed. Review the *Multiservice Data Manager Release 15.2 Supplement*.

- reviewed the *Multiservice Data Manager Release 15.2 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.
- have a Multiservice Data Manager 15.2 software license. If you do not have the license, you will need to order one. Contact your Nortel Sales Representative for additional information.

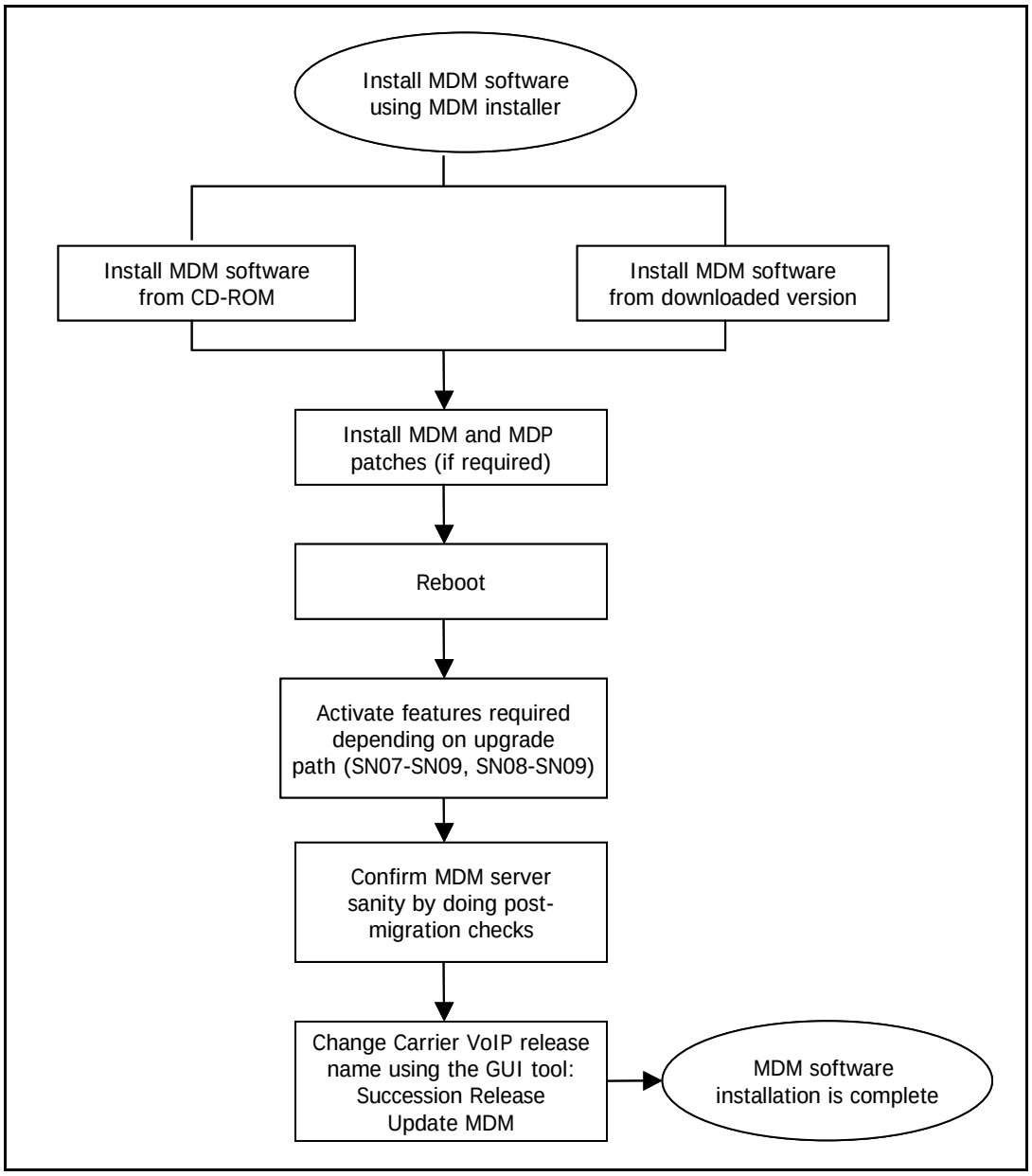
  If you are deploying Operator Client, you must obtain a new key. Contact your Nortel Sales Representative for additional information.
- performed the procedure: Downloading MDM software from Nortel website on page 253 or Retrieving MDM software and patches from a drop box on page 252.
- made a note of the directory name where the software that you downloaded or retrieved was placed.
- referred to the software downloads area of Nortel website (*www.nortel.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.
- have an X11 terminal with IP connectivity to the Sun Fire ™ V480 server you are upgrading if you are upgrading MDM servers from CD-ROM. 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 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.
- ensured that the UNIX group “nortel” exists. If the UNIX group “nortel” does not exist, create it using the Solaris admintool.

  If the UNIX user “nortel” does not exist, create it, with a Primary Group of “nortel” using the Solaris admintool.

MDM software installation task flow

The following figure shows you the tasks you need to perform to install new MDM software and patches.

MDM software installation task flow



To link to any task, go to the list that follows the task flow chart:

- Installing MDM software on page 272
- Downloading MDM patches from Nortel website on page 255
- Activating new features for MDM in SN08 on page 286
- Confirming successful MDM server installation on page 283 by performing Post-migration checks on page 296
- Setting the Solution release name identification on page 284

ATTENTION

Install Nortel Multiservice Data Manager (MDM) and MDP software packages using the MDM Installer tool. **DO NOT** use Solaris software package tools.

Installing 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 MDM software on the server as a back-up while installing the new version.

MDM configuration data is persistent. As a result, you will not lose your configuration data when MDM packages are deleted. For more information about installing MDM software, see 241-6001-100 *Nortel Multiservice Data Manager Software Installation and Initial Configuration*.

Installing MDM software

Installing MDM software

From the MDM server

1 Open a UNIX xterm using the user ID root.

2 Stop the MDM servers. For releases 14.3 and higher, the following command stops both the MDM and MDP servers:

/etc/init.d/nmssvm.server stop

3 If you are running release MDM 14.2, you must use separate commands to stop the MDM and MDP servers. Use the command in step 2 to stop the MDM server. Use the following command to stop the MDP servers.

su - <mdpadm userid> (for example: mdpadmin)

cd /opt/MagellanMDP/bin/mdpadm stop all

Note: This command must be executed using the mdpadmin user ID.

4 If you are upgrading from MDM 15.1 to MDM15.2, you must install four patches specified in step 9 Downloading MDM patches from Nortel website on page 255. See Bulletin 2005005709 for more information.

If you are upgrading from MDM14.2 or 14.3 to MDM15.2, these patches are not required.

5 If you are not installing the MDM software from CD-ROM, proceed to step 9. If you are installing using CDs go to step 6.

6 Insert the MDM 15.2 software disk 1 of 3 into the CD-ROM drive, pattern side up. If your drive uses a disk caddy, insert the disk into the caddy pattern side up, then slide the disk caddy into the CD-ROM drive.

MDM software is delivered on four CDs. These are called CD 1 of 3, CD 2 of 3, CD 3 of 3 and MDM Enhanced Security.

Note: Do not change directories (cd /cdrom/cdrom0) before executing the command install_mdm. Changing directories will cause problems when attempting to eject and load the CD-ROM.

7 Launch the MDM Installer:

/cdrom/cdrom0/install_mdm

8 Proceed to step 10.

9 Launch MDM Installer from the directory that contains the software that you downloaded in Downloading MDM software from Nortel website on page 253:

<MDM_software_pathname>/install_mdm

10 You are prompted for a DISPLAY environment variable. The default is to use a console local to the MDM workstation.

Enter the environment DISPLAY to launch the MDM Installer GUI [:0.0]

If your console is not local to the workstation, type the DISPLAY environment value (for example, BELTOR32:0.0)

The Nortel splash screen opens, a countdown occurs, then the window closes.

The Introduction window opens.

The left panel of the window indicates the current phase of the installation. As selections are made, the indicator for each phase changes color. The contents of the right panel changes as each installation phase is presented.

Note: The MDM Installer can be stopped at anytime before you press the Install button in step 22. Do not attempt to stop the software installation after the installation process has begun.

If you make a mistake while selecting installation options, you can uninstall the MDM software after completing the installation process and then re-install the MDM software. For information about uninstalling MDM software, see Uninstalling MDM software on page 301.

To stop the MDM Installer, click **Cancel**.

11 Click **Next**.

The License agreement window opens.

12 Review the license information.

Click **I accept the terms of the License Agreement**, then click **Next**.

Another window opens requesting that you wait while the workstation is examined.

The System information window opens.

This window indicates:

- details about the Solaris operating system currently installed on this workstation
- the sizes of the disk partitions on this workstation and the disk partition sizes recommended for Carrier Voice over IP MDM software
- the MDM software (by release) currently installed on this workstation
- the MDM software licenses currently installed on this workstation

13 If the actual sizes of the partitions are equal to, or larger than, the partition sizes recommended in NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP*, click **Next**.

The *MDM 15.2 Install Options* window opens.

14 Select the MDM and MDP software packages to install on this workstation.

15

ATTENTION

DO NOT install Operator Client on server-sets. Server-set servers are dedicated to providing fault and PM information.

Operator Client (OC) is an optional feature in the VoA solution.

a To install Operator Client in a VoA solution, select the software package: **MDM Operator Client and User Administration**.

This enables the Security Server and the Java Web Start Server.

If you do not want OC in your VoA solution, do not make a selection for this attribute.

b Operator Client is a mandatory feature in a secure VoIP solution.

To install Operator Client in a VoIP solution, select the software package **MDM Operator Client and User Administration**.

De-select the Security Server.

If the software package *MDM Operator Client* and *User Administration* is selected and the package *Security server* is not selected, a data entry box is displayed beside the *Java Web Start* server option.

In the data entry box: *SunONE IS,* type the name of the Integrated EMS server.

Note: Do not select the Security Server option for VoIP.

16 Click **Next**.

The *MDM 15.2 Installation Source Path* window opens.

17 If the indicated directory corresponds to the location of the software, click **Next.**

If you are installing from a directory other than the indicated directory, click **Choose**, select the appropriate folder, click **Select**; then click **Next**.

If the software packages are located in different directories, you are provided with prompts to select the appropriate directory for each package selected in step 14.

- If the MDM CD-ROMs are available, the default source path is: /cdrom/cdrom0
- If the MDM CD-ROMs are not available, the default source path is the directory that contains the MDM Installer: /MDM152

18 If the *<host name>.<domain name>* of this workstation cannot be automatically resolved, the *Enter domain name* window opens.

Type the *<domain name>* required to locate this MDM workstation on the network. If you do not know the domain name, contact your network or system administrator.

If the MDM workstation does not belong to a domain, you must assign a domain name in the /etc/hosts file. For 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
```

Note: If you do not know your domain name, contact your Nortel system administrator.

19 Click **Next**.

20 The *Network Viewer Background Pixmaps* window opens.

This window allows you to select optional bitmap images to use as the background for the Network Viewer (for example, the map of the world as the background).

Click **No**.

21 The *Pre-installation summary* window opens.

This summary identifies the software packages that will be installed and the disk space requirement for each package.

If the list of software packages to install is incorrect, click **Previous** to return to the *MDM 15.2 install options* window and select the correct software packages.

If the amount of disk space required to install the software exceeds the amount of available disk space, click **Cancel** to stop the installation and ensure there is enough disk space on the servers (see Ensuring that there is enough disk space on the servers on page 250).

22 Click **Install**.

The MDM Installer displays the name of each software package as the package is installed.

If you are installing from a CD-ROM, the MDM Installer prompts for additional CD-ROMs until all of the selected software is installed. To eject the current disk, from the command prompt in the terminal screen, type:

```
eject cdrom
```

Insert the next disk and click **OK**.

Note: Do not attempt to stop the software installation after the installation process has begun.

If you made a mistake while selecting installation options, you can uninstall the MDM software after completing the installation process and then re-install the MDM software. For more information about uninstalling MDM software see Uninstalling MDM software on page 301.

23 The *Enter new license* window opens after the software is installed if a valid 15.2 license key is not located on this workstation.

Type a new MDM software license in the provided data entry box and click **Next**.

If you do not enter a software license key, a temporary software license is generated. The license key is valid for all of the MDM software for a maximum of 30 days. When you have a permanent software license, manually apply the new license using the appropriate procedure in 241-6001-303 Nortel Multiservice Data Manager Customization and Server Administration.

The *Install complete* window opens.

MDM software installation is now complete.

24 Click **Done**.

The MDM Installer window closes.

25

ATTENTION

You must check the logs for any errors in the installation. If the installation logs indicate failure to install any of the MDM packages, follow the instructions in Recovering from an incomplete MDM software installation in the 241-6001-123 Nortel Multiservice Data Manager Upgrade guide.

Examine the MDM software installation logs for any errors. The logs are located in the directory:

/opt/MagellanNMS/data/log/<release>_Install_logs

Variable definitions

Variable	definition
hostname.domain name	the fully qualified host name of this workstation
domain name	the domain name used on this network
MDM_software_path name	the absolute pathname of the directory that contains the MDM Installer

MDM Installer logs

Log	Description
Install_summary.log	This file contains the following information for each software package: package - version added or replaced - installation success or failure

MDM Installer logs

Log	Description
stopServers	This file identifies the Multiservice Data Manager servers that were stopped by the MDM Installer during a Multiservice Data Manager software upgrade.
Package_logs	This file contains each package installation or package removal. For example: install_MDM151Pbe, remove_MDM143Pac, install_MDMHELP.

Installing MDM patches

After installing Nortel Multiservice Data Manager (MDM) software, you need to install the patches for MDM and MDP (if required).

MDM patches are jumbo patches that include all previous patches. Install only 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 an MDM patch as an example. Repeat the procedure for all the patches that you need to install.

Prerequisites

- Ensure you have performed the procedure Installing MDM software on page 272.
- Refer to the software downloads area of Nortel website (*www.nortel.com*) to determine which patches you need to install. If there are no patches listed, it means that there are no patches currently required for this release.
- See Downloading MDM patches from Nortel website on page 255 to download the required MDM patches.

From the MDM server

1 Log in - see Logging into MDM platform on page 295.

2 Display the patches that are currently installed on the system:

cd /var/sadm/patch

ls

showrev -p | grep MDM

showrev -p | grep MDP

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 *patch152* directory:

cd /patch152

Note: The *patch152* directory was created in step 3 of Downloading MDM patches from Nortel website on page 255. 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 website (*www.nortel.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 <patch_name>.tar

11 Change directories to the specific patch subdirectory:

cd /patch152/<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 MDM server should return to service without any problem.

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, MDM152-01.

Confirming successful MDM server installation

After installing Nortel Multiservice Data Manager (MDM) server software and patches, you must confirm that the installation was successful by performing Post-migration checks on page 296.

Setting the Solution release name identification

To help identify which Solution (Carrier Voice over IP) release the MDM is running, and help operators determine if that release is compatible with other elements in the network, the MDM toolset allows you to set the Carrier Voice over IP release name on the MDM tool launcher.

Prerequisites

- the file /opt/MagellanNMS/cfg/.SuccessionEnabled must exist

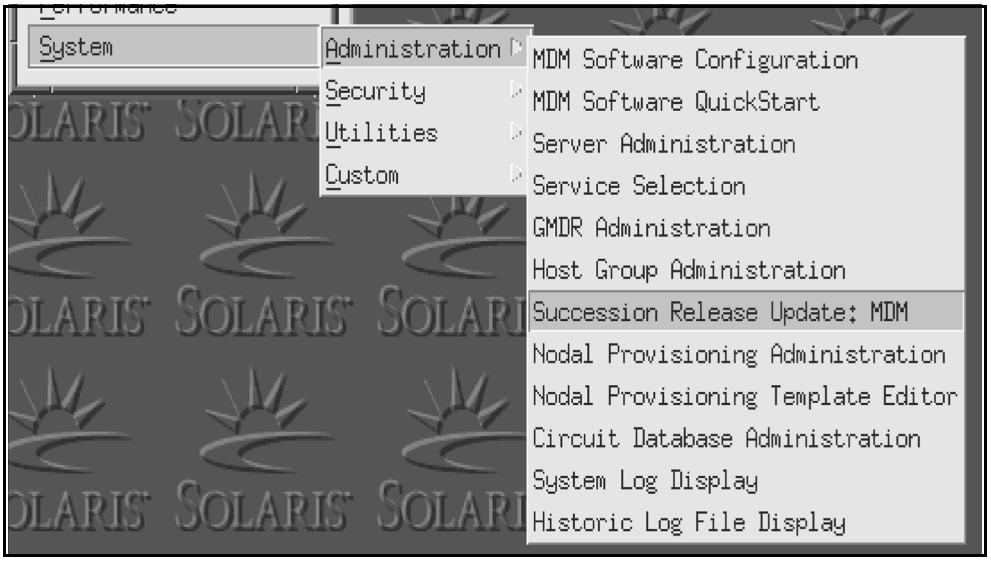
Setting the Solution release name on the MDM

From the MDM server

1 Log in - see Logging into MDM platform on page 295.

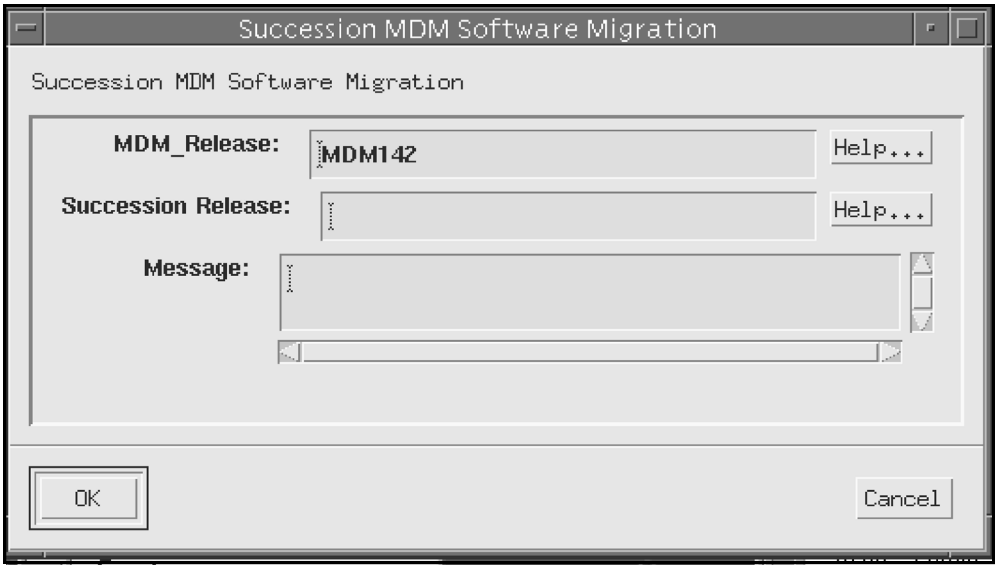
2 From the MDM window, choose System > Administration > Succession Release Update: MDM.

The Succession MDM Software Migration window opens and displays the current MDM release.



3 Enter the Carrier Voice over IP release name using the format: SNxx.y For example: SN07.

The Succession MDM Software Migration window opens displaying the current MDM release.



4 Click *OK*.

The file */opt/MagellanNMS/system/info/release.name* is changed and the MDM toolset icon displays the MDM release name followed by the Carrier Voice over IP (in the format SNxx) 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.

Note: The updated release name will not appear until you exit the tool and re-start it.

Activating new features for MDM in SN08

ATTENTION

Before you activate any SN08 features, activate the MDM Carrier Voice over IP features listed in the MDM Carrier Voice over IP feature baseline on page 227.

Refer to SN07 Helmsman documentation for how to activate features for MDM 14.1, 14.2 to MDM 15.1. These feature activations still apply for the MDM 14.2 to MDM 15.2 upgrade. Once the baseline features are activated, you can activate the SN08 features.

The following features must be activated in SN08:

- Auto-patching for MSS/MG15000 nodes
- Nodal provisioning template audit
- Security audit logs real time to SCC2
- Enhanced security in VoIP

Note: See the NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements* guide for information on security features.

The following feature is activated automatically:

- Centralized AAA and user administration for VoA networks with the Operator Client application

  However, you must configure MDM Admin Servers and access policies. See Centralized AAA and user administration for VoA networks with the Operator Client application on page 290 for more information.

MSS SN08 features can be activated in any order once the upgrade is completed successfully. See:

- Activating auto-patch on page 287
- Centralized AAA and user administration for VoA networks with the Operator Client application on page 290
- Nodal provisioning template audit on page 291
- Activating security/audit logs (SALs) real time to SCC2 on page 292

Activating auto-patch

To fully automate provisioning and activating MSS15000/MG15000 patches, you must use a use Nortel MDM workstation. Scheduling and control of the auto-patch script is from the MDM which issues on-switch commands that trigger the calculation and update of the Sw patchList. Use the crontab utility (or your usual scheduling utility) to configure the script. At the appointed time, the MDM will trigger the switch to download the latest version of the Patch Av.

Configure the MDMs to run the auto-patch download and application at different times. That is, the MDM designated to be the SDS can be scheduled to perform the downloads to the switches at one time and at another time, the same MDM can run the script to apply the patches on the switches. See “Scheduling the MDMs for auto-patching” in NN10114-511 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP*.

Setting up the script for auto-patching

From the MDM

1 Log in to the server as the **root** user.

2 Create a cron job that will regularly run the *ppautopatch* script at scheduled times.

a Set up the cron job to start the next night according to your schedule with a line in the standard format:

```
<min> <hour> <day> <mon> <dow> <command>
```

where:

- **command** specifies the *ppautopatch* script command string

Use the following syntax for the command string:

```
ppautopatch (-download -host <sds host name>
-huser <sds host userid> <sds host password>)
```

and/or **(-apply [-log_verbose])**

```
-nodes <group> | <node> | <filename>
-nuser <node userid> <node password>
[-max_duration <n> h | m]
[-successfile <filename>]
[-failedfile < filename]
```

where the following attributes are mandatory:

- **-download**, selects the patch download to the switch operation
- **-apply**, selects the patch application operation on the switch

  Note: **-download** and **-apply** can be scheduled independently.

- **-host**, enter the SDS host name or IP address of the SDS
- **-huser**, enter the user ID and password for the SDS This is the user ID and password required to connect to the SDS.
- **-nodes**, enter the HGDS group with all **MSS**/**MG15000** nodes

  This is for one or more MSS nodes in an HGDS group. You can enter a node name, a group of nodes, or a list of nodes. Any node or group name must be configured in HGDS.

- **-nuser**, enter the user ID and password for the **MSS**/**MG15000**s

  This is the user ID and password required to connect to the MSS/MG15000 node(s). The user ID permissions must have a user scope of network and a user impact of debug, administration, or configuration.The password may either be stored in the clear or be the name for a file that contains an encrypted password.

- **-max_duration**, enter in the format: **<<n> h l m>**

  This defines the maximum time the Auto-patch tool has to complete the patch download and, or application operations on each node. You can enter the time in hours from 1 - 23 or in minutes from 1 -1439. One hour (1h) is recommended for the max_duration.

The following attributes are optional:

- **-successfile**, allows you to identify a file other than the default file to store the names of all of the nodes where the auto-patch tool successfully performed the download and, or apply operations. You can use this option with the -nodes parameter to record successful downloaded and applied patches or for customer auditing purposes. If you do not use this option, the names of the nodes will be

stored in
/opt/ MagellanNMS/data/ppautopatch/<filename>.

The filename will include the date, operation requested, nodes variable, and an incrementing index <N> to ensure the filename remains unique, as follows:

<YYYYMMDD>_SUCCESS_<DL | APPLY>.<NODES>.<N>.hosts

- **-failedfile**, allows you to identify a file other than the default file to store the names of all of the nodes where the Auto-Patch tool unsuccessfully performed the download and, or apply operations. You can use this option with the -nodes parameter to record successful downloaded and applied patches or for customer auditing purposes. If you do not use this option, the names of the nodes will be stored in
/opt/ MagellanNMS/data/ppautopatch/<filename>.

  The filename includes: the date, operation requested, nodes variable, and an incrementing index <N> to ensure the filename remains unique, as follows:

  <YYYYMMDD>_FAILED_<DL | APPLY>.<NODES>.<N>.hosts

- **-log_verbose**, allows you to include the output of the patch query that is run by the Auto-Patch tool. The output includes the state of all patches and the software patchlist for every node. The operation runs before the download and apply operations. If you do not select this operation, the patches that require manual intervention are output by default. This includes patches that have been declared obsolete, patches with an emergency removal notice or defect, and patches which are service affecting.

For more information about activating the auto-patch script, refer to “Configuring the auto-patch process” in NN10400-300 *Nortel Multiservice Data Manager Administration Tools*.

Centralized AAA and user administration for VoA networks with the Operator Client application

This feature is automatically activated, however, there is configuration required to deploy MDM Admin Servers in the VoA network. See the following table.

To	refer to
deploy client-sets as MDM Admin Servers	Installing MDM software on page 272
configure both the MDMs to provide centralized authentication and authorization This includes configuration of the MDM Admin Servers, RADIUS interface, and RADIUS client.	NN10114-511 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP*
create policies, configure roles with policies, and associate users with roles	NN10180-611 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP*
see the attributes you need to configure for policies, roles, and users	NN10225-512 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP*

Nodal provisioning template audit

The Nodal Provisioning template audit can help locate problems with configuration data on the MSS15000. When the NP template is used, the NP server generates security audit logs (SALs) that capture all information related to the template and the MSS15000. The Configuration Audit verifies whether the on-switch provisioned data matches the data applied from a selected template and user inputs.

To activate the logging, edit the NP Config Manager server startup information to include the -cfgSAL option in the Server Administration tool (/opt/MagellanNMS/bin/configman -cfgSAL). The usual Server Administration tool prerequisites for editing a server configuration apply.

Activating Nodal provisioning audit

From the MDM

1. Start Service Administration from the NMS Toolset.
2. Select **Authorize** under the *Security* menu to specify the password.
3. Select the **NP Configuration Manager**. Select the **Edit->Edit Server** function.
4. Add the *-cfgSAL* option to the start up command:

   /opt/MagellanNMS/bin/configman -cfgSAL
5. Click **Save and Restart**.

Activating security/audit logs (SALs) real time to SCC2

To enable logging of MDM and MSS15000/MG15000 security audit logs, configure an instance of SALC (Security Audit Log Collector) that is running in MDM to specify the target host and the facility that will be used on that host to receive the logs.

SALC supports a redundant architecture that feeds security audit logs between two peer MDM servers, that is, the MDM server-set servers, that filters out duplicate SALCs. The configuration described below sets up this redundant feed.

In order for SALC server to generate logs to syslog in Custlog V2 (SCC2) format, a -node ID <nodeId>" argument is required (see NN10225-512 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP* for configuration attributes). The presence of this option triggers the salcserver to begin generating logs in the Custlog V2 format.

The installation and initial configuration must be performed on both MDM servers in the server set.

See 241-6001-310 *Nortel Multiservice Data Manager Server Reference* for information on creating the configuration file.

Prerequisites

- Start the FMDR server with the user ID that has system administrator privileges.

Installation and initial configuration

From the MDM

1 Create the salcserver configuration file. The configuration file name must have the following format:

/opt/MagellanNMS/cfg/SALCServer_<nodeId>.cfg.

See NN10225-512 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP* for valid configuration attribute values.

2 Use the Server Administration tool to start the salcserver:

/opt/MagellanNMS/bin/salcserver -OAMCFacility <custlog facility> -passportFacility <custlog facility> -outputSyslog <SDM IP address> -nodeId <nodeId> -outputFile

3 Repeat these steps for each Carrier Voice over IP office being managed.

See NN10225-512 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP* for valid configuration attribute values.

Upgrading to SN08 from a previous release

If you are upgrading to SN08 from an earlier release, do the following:

1 Ensure that OSS applications are updated to handle security audit log data.

2 Upgrade the first MDM server-set:

- **a** OAMC should already be handled by the base MDM procedures.
- **b** If the FMDR (common to fault stream for the Carrier Voice over IP office) is actually common to multiple groups (relying on the PSERVER filtering), split up the FMDR's to be per office.
- **c** SALC can initially point to the local OAMC, client-set OAMC, and local FMDR only. It should not yet point at the SDM, but can be storing security audit logs in the local file system.
- **d** As each MSS/MG15000 gains connectivity to MDM server-sets running SALC, the security audit logs will automatically start flowing as they are generated.

3 Upgrade the second MDM server-set:

- **a** OAMC should already be handled by the base MDM procedures.
- **b** If the FMDR (common to fault stream for the Carrier Voice over IP office) is actually common to multiple groups (relying on the PSERVER filtering), split up the FMDR's on a per office basis.
- **c** SALC can initially point to the local OAMC, local FMDR, remote OAMC, and remote FMDR. It should not yet point at the SDM, but can be storing SAL's in the local file system.

d As each MSS/MG15000 gains connectivity to MDM server-sets running SALC, the SAL's will automatically start flowing as they are generated.

4 Return to the first MDM server-set:

a Stop SALC.

b Point SALC at the remote OAMC and remote FMDR.

c Start SALC.

5 Upgrade each MSS/MG15000. As each gains connectivity to MDM server-sets running SALC, the security audit logs will automatically start flowing as they are generated but only after the point of connectivity. Prior to that, security audit logs originating on MSS/MG15000 are spooled to the CP disk).

6 Upgrade the SDM for the office according to the standard Carrier Voice over IP upgrade procedures and in the order that the solution-level deployment demands. SDM is normally upgraded after MDM.

7 For each MDM server-set:

a Stop SALC.

b Point SALC at the SDM now running SN08.

c Start SALC.

MDM access procedures

These procedures describe how to log into Nortel Multiservice Data Manager (MDM) servers and open the toolset menu.

Logging into MDM platform

To log in to a MDM server, perform the following steps.

From the MDM server

1. Log in as the root user.
2. Enter the root password when prompted.

Opening the MDM Toolset

Open a Multiservice Data Manager (MDM) window before beginning the upgrade process.

From the MDM server

1. If the window does not automatically open at log in, open the window with the following command:

   /opt/MagellanNMS/bin/nmstool &

   The copyright dialog opens, followed by the MDM window. Click *OK* to close the copyright dialog.

Post-migration checks

After completing the software upgrade for Nortel Multiservice Data Manager (MDM) servers, you must verify that the servers are functioning correctly.

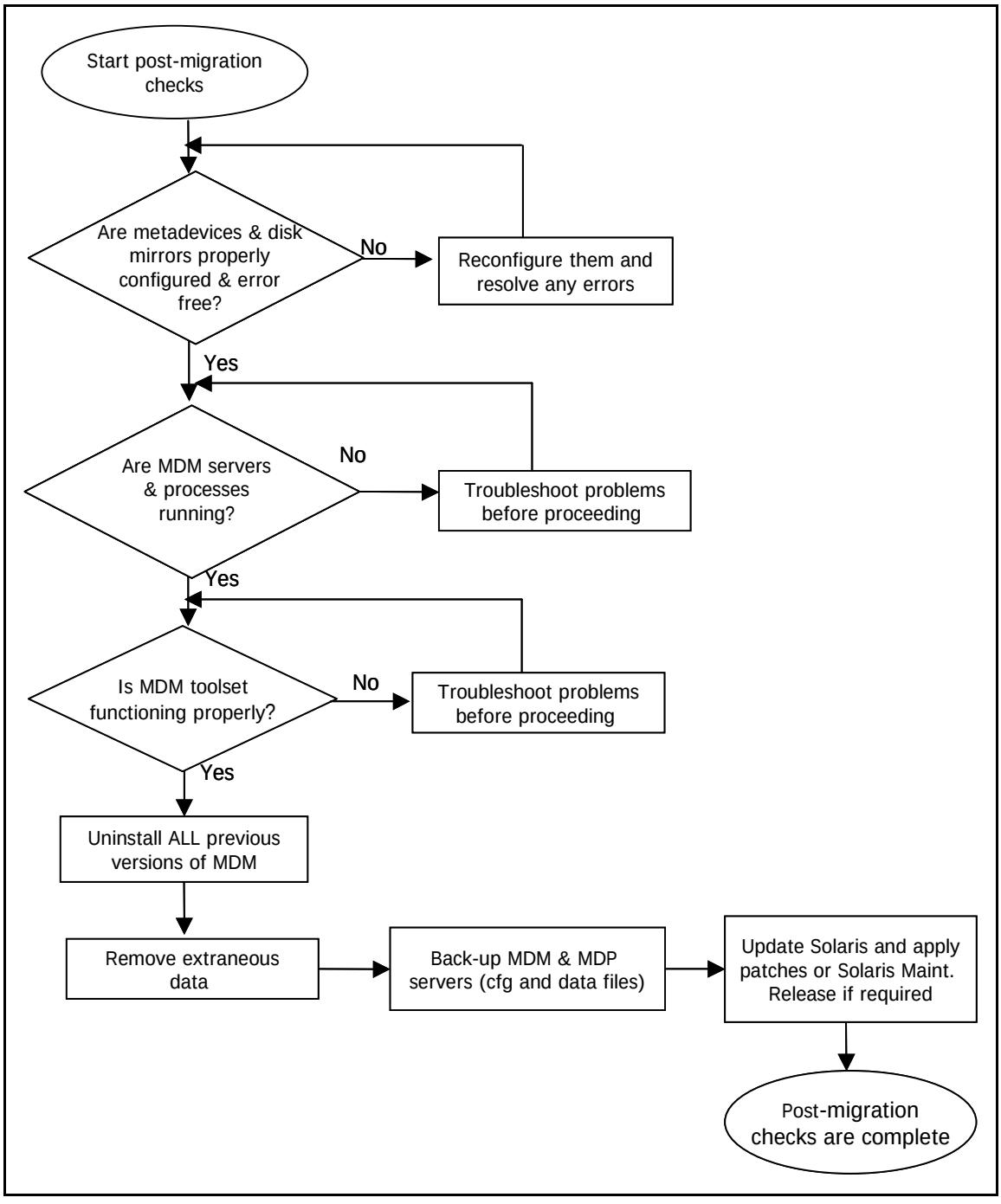
Prerequisites

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 MDM tools and software.

The figure MDM post-migration check task flow on page 297 shows you the sequence of procedures you must perform to determine the status of the servers after a migration.

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 263
- Verifying that MDM servers and processes are running post-migration on page 299
- Uninstalling MDM software on page 301
- Ensuring that there is enough disk space on the servers on page 250
- Performing a complete system backup on page 244
- Upgrading the Solaris operating system on page 232

Verifying that MDM servers and processes are running post-migration

From the MDM server

1 Log in — see Logging into MDM platform on page 295.

2 Open a MDM window — see Opening the MDM Toolset on page 295.

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 *Nortel Multiservice Data Manager Server Reference* 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 MDM window choose System -> Administration -> GMDR Administration.

Note: For more information, see Using the GMDR Administration tool in the 241-6001-303 *Nortel Multiservice Data Manager Customization and Administration*.

10 Ensure that there are two FMDR servers for every distinct Carrier Voice over IP office, and two OAMC 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 the MDP servers were installed, use the Server Administration tool to ensure the servers are running.

The servers must be listed in the following sequence:

- MDP Disk Manager (mdpdiskmgr)
- MDP File Mover Manager (mdpfmmgr)
- MDP Data Model Manager (mdpdmm)

- MDP MSS File Manager (mdpppmgr)
- MDP File Prober Manager (mdpfpmgr)

Note: Start the Server Administration tool using the "mdpadmin" userid used to start the MDP servers.

13 From the Toolset icon, select any tool and open its Help system to verify that the installation was successful.

If the installation was successful, follow these steps.

From the MDM server

1 If the software was downloaded successfully, remove the software download directory:

rm -r /MDM152

2 Remove the software patch directory:

rm -r /patch152

Uninstalling MDM software

To roll back MDM software from SN08 to a previous release, you must uninstall the software release, patches, remove several directories and then, restore the software. You must uninstall the MDM software and patches using the MDM Installer. Perform the following procedures in the order listed:

- Uninstalling MDM software on page 301
- Removing MDM software patch on page 302
- Removing directories before restoring MDM software on page 302

Uninstalling MDM software

From the MDM

1 Using the user ID root, open a UNIX xterm.

cd /opt/MDM<release>_INST

2 Change directories to the directory that contains the uninstall tool for the software release to be removed.

3 Start the software removal tool InstallAnywhere Uninstaller.

./uninstall_mdm[134 or 141] (for release 13.4 or 14.1)

./uninstall_mdm (for any release above 14.1)

The InstallAnywhere Uninstaller window opens.

4 Select **Uninstall**.

A window opens that indicates the MDM packages available for removal.

5 Select the MDM packages to remove and click **Uninstall Selected Packages**.

A progress bar indicates the stage of removal for each package.

A popup window indicates completion.

6 Click **Ok**.

7 Click **Done**.

The Uninstaller logs are located in the directory /opt/MagellanNMS/data/log/<release>_Install_logs.

8 If the Secure Shell (SSH) software was installed on this workstation, remove the SSH software. Type the following commands in sequence and respond to the prompts.

/bin/pkgrm MagSTRM

/bin/pkgrm SSHinit

If this workstation uses Solaris 8, type

/bin/pkgrm MagOSSH

9 If the software package cannot be successfully removed, contact GNTS.

Removing MDM software patch

From the MDM

1 Using the user ID root, open a UNIX xterm.

2 Run the Sun Microsystems Inc. patch removal utility.

patchrm <release>-<patch>

The software patch is removed. You are informed of a successful patch removal.

3 Review the *MDM 15.2 Release Supplement* or the README file included with the installed software patch. Determine the actions required to restore the MDM software to its previous state.

Before you restore MDM information, you must manually remove the following directories:

- /opt/nortel/data
- /opt/nortel/config
- /opt/nortel/log
- /opt/nortel/3rdparty

Removing directories before restoring MDM software

From the MDM

1 Using the user ID root, open a UNIX xterm.

2 Change directories to the directory to remove.

rm -R <directory_name>

3 Repeat this command until all of these four directories are removed.

CS 2000 Core Manager

Before upgrading the CS 2000 Core Manager

Perform the required prerequisite upgrade as follows:

Network	CS 2000 Core Manager applies to:	Previous Upgrade
ATM	PT-AAL1, UA-AAL1, and PT-AAL2	Multiservice Data Manager (MDM) on page 215
IP	IAC- International, CHS - International, IAW, PT-IP and UA-IP[1]	Multiservice Data Manager (MDM) on page 215
	IAC - North America and CHS - North America	Ethernet Routing Switch 8600 on page 94
Tri-Modal	all applications	Multiservice Data Manager (MDM) on page 215

1.Includes IP International: PT-IP and UA-IP

After upgrading the CS 2000 Core Manager

Perform the next required upgrade as follows:

Network	CS 2000 Core Manager applies to:	Next Upgrade
ATM	UA-AAL1 and PT-AAL2	Integrated Element Management System (IEMS) on page 487
	PT-AAL1	Multiservice Switch (MSS) 15000/20000 on page 820
IP	PT-IP, UA-IP, IAW, IAC, and CHS[1]	Integrated Element Management System (IEMS) on page 487
Tri-Modal	all applications	Integrated Element Management System (IEMS) on page 487

1.Includes IP International: CHS, IAC, PT-IP, and UA-IP

About the CS 2000 Core Manager

The Communication Server 2000 Core Manager manages the XA-Core and the subtending time division multiplexing (TDM) components of the

Communication Server 2000. It resides on the SuperNode Data Manager (SDM) platform and provides operations, administration, maintenance, and provisioning (OAM&P) functionality.

Filesets to solution mapping

This module provides information on the filesets included in the CS2E0080 load.

The following table lists CS2E0080 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 4)

Fileset	Description	Solutions					
		IAC	IAW	PT-AAL1	PT-IP	UA-AAL1	UA-IP
SDM_Version.info	CS2E0080	Y	Y	Y	Y	Y	Y
NT_SIM.tools	Patching tools	Y	Y	Y	Y	Y	Y
SDM_ACE.dist	SDM ACE distribution	Y	Y	Y	Y	Y	Y
SDM_AFT.DMS500	SBA Automatic File Transfertime	N	N	N	N	N	N
SDM_ATA.client	ASCII Terminal Access Client	Y	Y	Y	Y	Y	Y
SDM_BASE.base	Platform base	Y	Y	Y	Y	Y	Y
SDM_BASE.client	Client Common Resources	Y	Y	Y	Y	Y	Y
SDM_BASE.dfquery	Check disks and disk drives	Y	Y	Y	Y	Y	Y
SDM_BASE.fts	File Transfer Service	Y	Y	Y	Y	Y	Y
SDM_BASE.gdd	Generic Data Delivery	Y	Y	Y	Y	Y	Y
SDM_BASE.logs.client	Log Delivery Service Client	Y	Y	Y	Y	Y	Y
SDM_BASE.logs	Log Delivery Service	Y	Y	Y	Y	Y	Y
SDM_BASE.mtce	Platform Maintenance	Y	Y	Y	Y	Y	Y

Note: Y= required, N=not required, O=optional

Fileset-to-solution mapping (Sheet 2 of 4)

Fileset	Description	Solutions					
		IAC	IAW	PT-AAL1	PT-IP	UA-AAL1	UA-IP
SDM_BASE.omsl	OM Access Service	Y	Y	Y	Y	Y	Y
SDM_BASE.tasl	Table Access Service	Y	Y	Y	Y	Y	Y
SDM_BASE.util	Platform utilities	Y	Y	Y	Y	Y	Y
SDM_BMI.bmi	Base Maintenance Interface	Y	Y	N	Y	Y	Y
SDM_DDMS.ossaps	OSS and Application Svcs	Y	Y	N	Y	Y	Y
SDM_DDMS.osscomms	OSS Comms Svcs	Y	Y	N	Y	Y	Y
SDM_DMA.dma	DMS Maintenance Application	Y	Y	N	Y	Y	Y
SDM_DNBD.dnbd	DNBD Call Data Delivery	Y	Y	Y	Y	Y	Y
SDM_DNBD.osidp	ONE FTAM Software	Y	Y	Y	Y	Y	Y
SDM_DTS_PROVIDERS.dts	DCE DTS Time providers for global servers	Y	Y	Y	Y	Y	Y
SDM_ECR.ecr	SDM Expansion Chassis Removal tool	Y	Y	Y	Y	Y	Y
SDM_ESUP.esup	ESUP Tools	Y	Y	Y	Y	Y	Y
SDM_ETA.eta	Enhanced Terminal Access	Y	Y	Y	Y	Y	Y
SDM_ETA.client	Enhanced Terminal Access Client	Y	Y	Y	Y	Y	Y
SDM_FTP.proxy	FTP proxy	Y	Y	Y	Y	Y	Y
SDM_GR740PT.gr740pt	GR740 Pass Through	Y	Y	Y	Y	Y	Y
SDM_IMAGEDUMP.rte	Image Dump Service	Y	Y	Y	Y	Y	Y
SDM_INSTALL_inst	SDM Tools	Y	Y	Y	Y	Y	Y

Note: Y= required, N=not required, O=optional

Fileset-to-solution mapping (Sheet 3 of 4)

Fileset	Description	Solutions					
		IAC	IAW	PT-AAL1	PT-IP	UA-AAL1	UA-IP
SDM_LOGS.mdm	Passport Log Streamer	N	N	Y	Y	Y	N
SDM_OMDD.omdd	OM Delivery	Y	Y	Y	Y	Y	Y
SDM_OpenSSH.base	Open SSH ver. 3.4p1	Y	Y	Y	Y	Y	Y
SDM_OpenScreen.base	OpenScreen	Y	Y	Y	Y	Y	Y
SDM_PRECHECK.sysaudit	System pre-check tools	Y	Y	Y	Y	Y	Y
SDM_REACHTHRU.rttl1	Reach Through SPM	Y	Y	Y	Y	Y	Y
SDM_SBA.DMS500	SDM Billing Application	Y	Y	Y	Y	Y	Y
SDM_SCFT.scft	Secure Core File Transfer	Y	Y	Y	Y	Y	Y
SDM_SCM.scm	Succession SAM21 Manager ***Note:*** This fileset is only required for SN05 to SN08 upgrades.	Y	Y	N	Y	Y	Y
SDM_SFT.client	Secure File Transfer Client	Y	Y	Y	Y	Y	Y
SDM_SFT.sft	Secure File Transfer	Y	Y	Y	Y	Y	Y
SDM_SWLD.swld	BOOTP Loading Service	Y	Y	N	Y	Y	Y
SDM_UPGRADE.tools	UPGRADE Tools	Y	Y	Y	Y	Y	Y
SDM_BKM-CSU-00.tape 21.3.0.0	Succession Provisioning Data Sync Manager	N	Y	N	Y	Y	Y
SDM_GEM.dmsDataSrv-<version>.tape	CEM DMS Data Server	Y	Y	Y	Y	Y	Y

Note: Y= required, N=not required, O=optional

Fileset-to-solution mapping (Sheet 4 of 4)

Fileset	Description	Solutions					
		IAC	IAW	PT-AAL1	PT-IP	UA-AAL1	UA-IP
SDM_TntFTPHndl.TntFTPHndl-<version>.tape	CEM Telnet FTP Handler	Y	Y	Y	Y	Y	Y
SDM_CEM.SAF-<version>.tape	CEM Store and Forward	Y	Y	Y	Y	Y	Y

Note: Y= required, N=not required, O=optional

Preparing your system for upgrade using ESD

Purpose

Use this procedure to prepare the CS 2000 Core Manager for an Electronic Software Delivery (ESD) upgrade, which includes the following tasks:

- Applying the SDM_CERTS.Certs Package on page 309
- Preparing the CS 2000 Core Manager for file transfer from the repository server on page 310

Prerequisites

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.

Electronic Software Delivery (ESD) uses standard network connectivity methods into the software distribution process for the 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.

Action

Applying the SDM_CERTS.Certs Package

ATTENTION
Perform this procedure only if the SDM-based node requires software authentication for software delivery.

On the CS 2000 Core Manager

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 Verify that the SDM_CERTS.Certs package is already installed and listed in the available filesets on the system.

If the package is installed, continue with the next step.

If the package is not installed, skip the rest of this procedure and go to the next procedure.

5 Select the SDM_CERTS.Certs package

```
> select <n>
```

where <n> is the number next to the SDM_CERTS.Certs fileset.

6 Apply the SDM_CERTS.Certs fileset:

```
> apply
```

7 When prompted, confirm the apply command:

```
> y
```

8 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 Use the following table to determine your next step:

If	Do
you want to convert an existing logical volume	step 3
you do not want to convert an existing logical volume	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 Remove all archived filesets from the system, to free up disk space. Access the Details level:

```
sdmmtc details
```

7 Show all software:

```
filter off
```

8 Select all archived filesets:

```
select all
```

9 Remove all archived filesets:

```
remove all
```

Note: The system will automatically select appropriate files to remove.

10 Confirm the command:

```
y
```

11 After removing the archived filesets, ensure that /usr logical volume is less than 50% full. To check the "% full" value of /usr, enter the following command:

```
sdmmtc storage
```

Note: If /usr is more than 50% full, refer to procedure "Increasing the size of a logical volume" in NN10170-611, *CS 2000 Core Manager Security and Administration* to increase the /usr logical volume size as required. The /usr logical volume must have minimum size of 1050Mb.

12 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 14
do not want to convert an existing logical volume	press the Enter key and go to step 13

13 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.

14 Exit the maintenance interface:

```
quit all
```

15 Transfer the ISO image to the SDM-based node. Perform the procedure Transferring a compressed ISO image to an SDM-based node on page 314.

16 You have completed this procedure, and can now proceed to upgrade your system from disk.

Transferring a compressed ISO image to an SDM-based node

Application

Use this procedure to transfer a compressed ISO image file from the ESD load repository server to an SuperNode Data Manager (SDM-based) node.

Prerequisites

This procedure has the following prerequisites:

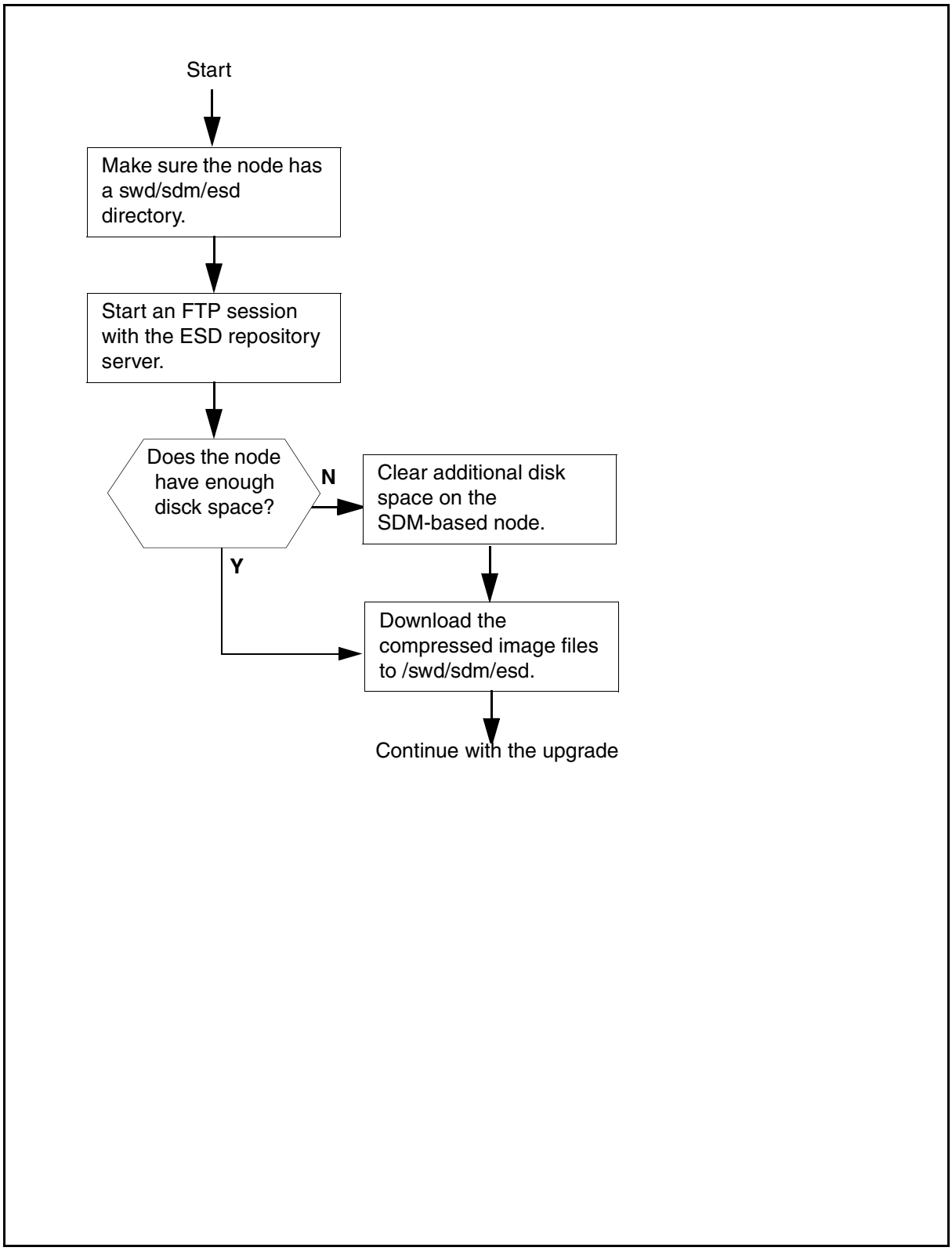
- The image file must be uncompressed and available on your ESD load repository server.
- You must know the name or IP address of the load repository server and the location of the dropbox directory on the server.
- You must know the name or IP address of the SDM-based node.
- You must know the root password to the SDM-based node.

This procedure requires you to confirm the availability of disk space on the SDM-based node. If the node does not have the required amount of available disk space, follow your local office policy to clear space. If you do not know your policy or cannot clear the required amount of available disk space, contact your next level of support.

Action

Use the flowchart as an overview of the tasks required to complete this procedure. Use the step-by-step instructions to complete the procedure.

Overview of steps to transfer a compressed ISO image to an SDM-based node



Transferring an ISO image to an SDM-based node

At your workstation

1 Log in as root to the SDM-based node.

Note: The SDM-based node supports a variety of secure and non-secure login options. Follow office policy or check the user documentation for your release.

2 Change to the data directory by typing

```
# cd /swd/sdm
```

and pressing the Enter key.

3 List the directories in /data by typing

```
# ls -d esd
```

and pressing the Enter key.

4 Use the following table to determine your next step.

If the response is	Do
`No such file or directory`	step 5
`esd`	step 6

5 Create the directory by typing

```
# mkdir esd
```

and pressing the Enter key.

6 Display the available disk space in the data directory by typing

```
# df -k /swd/sdm/esd
```

and pressing the Enter key.

7 Record the amount of available disk space. You will need the information later in this procedure.

8 Change to the esd directory by typing

```
# cd esd
```

and pressing the Enter key.

9 Start an FTP session with the ESD repository server by typing

```
# ftp <repository_server_ip>
```

and pressing the Enter key.

where

<repository_server_ip>
is the machine owned by the operating company that was selected to be the destination for ESD software.

10 List the directories on the ESD repository server by typing

```
ftp> ls
```

and pressing the Enter key.

11 Change directory to the drop box directory by typing

```
ftp> cd <dropbox_directory>
```

and pressing the Enter key.

where

<dropbox_directory>
is the name of the your dropbox directory.

12 List the contents of the drop box by typing

```
ftp> ls -l
```

and pressing the Enter key.

13 Locate the compressed image file you want to transfer and identify the size of the file.

14 Compare the size of the compressed image file with the amount of available space on your SDM-based node that you recorded in step 7. Use the following table to determine your next step.

If the SDM-based node	Do
does not have enough available disk space.	step 15
has enough available disk space	step 16

15 Clear additional disk space, following local office policy, before you continue with this procedure. If necessary, contact your next level of support.

16 Change the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

17 Transfer the ESD software load to the SDM-based node by typing

```
ftp> get <iso_image>
```

and pressing the Enter key.

where

<iso_image>
is the full name of the image file

18 End the FTP session by typing

```
ftp> bye
```

and pressing the Enter key.

19 Make sure the files the files successfully transferred to the SDM-based node. List the files in /swd/sdm/esd by typing

```
# ls -l
```

and pressing the Enter key.

20 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

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 347. The purpose of this procedure is to avoid any potential tape problems during the upgrade.

ATTENTION

Nortel 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 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, you will minimize potential disruption to the software upgrade, minimize any risk to the switch, and assist Nortel in providing full support on the upgrade, should assistance be required. Nortel 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.

Procedures

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

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 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	

Pre-check tasks	Time (min.)	Passed /Failed
CPU Stability pre-check	5	
DS512 fiber link pre-check	5	
Application/fileset status and configuration pre-check	2	
User configuration pre-check	2	
Ethernet configuration pre-check	5	
System dump device pre-check	1	

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 core and CS 2000 Core Manager.
- Obtain cell_admin password.
- Obtain the IP address for the CS 2000 Core Manager, the 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” 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.

- Ensure that all released DMS core-side patches have been applied and that the CS 2000 Core Manager is at patch current status
- Ensure that the modem is configured and operational in the event that Nortel 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. 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.

- Test the SDM for CNR (call notification record) Delivery and CIPC Provisioning (applies to GEM-only applications).
- 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 347 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 recommends that you upgrade your system directly from tape only if you are unable to complete the procedure Software upgrades from tape on page 347.

- 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.
- Obtain the OAM and CALLP Gateway IP addresses for the Ethernet configuration pre-check from the system administrator.
- List the loads installed on the CS 2000 Core Manager, by entering the following command at the command line:

  `querysdm loads`

  In response to this command, the system will display the loads and software fixes currently installed on the CS 2000 Core Manager, and the status of these software loads and fixes.
- Display the latest configured SBA schedule by entering the following command at the command line:

  `/sdm/sba/DMS500/bin/schedulelist`

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 the core manager is upgraded to the new software load, the system audit will run automatically on a daily basis.

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 327

2 Determine the fileset source.

If the fileset is	Do
on tape	insert the tape into slot 2, and continue with step 3 ***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 327.

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 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 “Upgrade Guidelines” in *Upgrading the CS 2000 Core Manager,* NN10060-461 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.

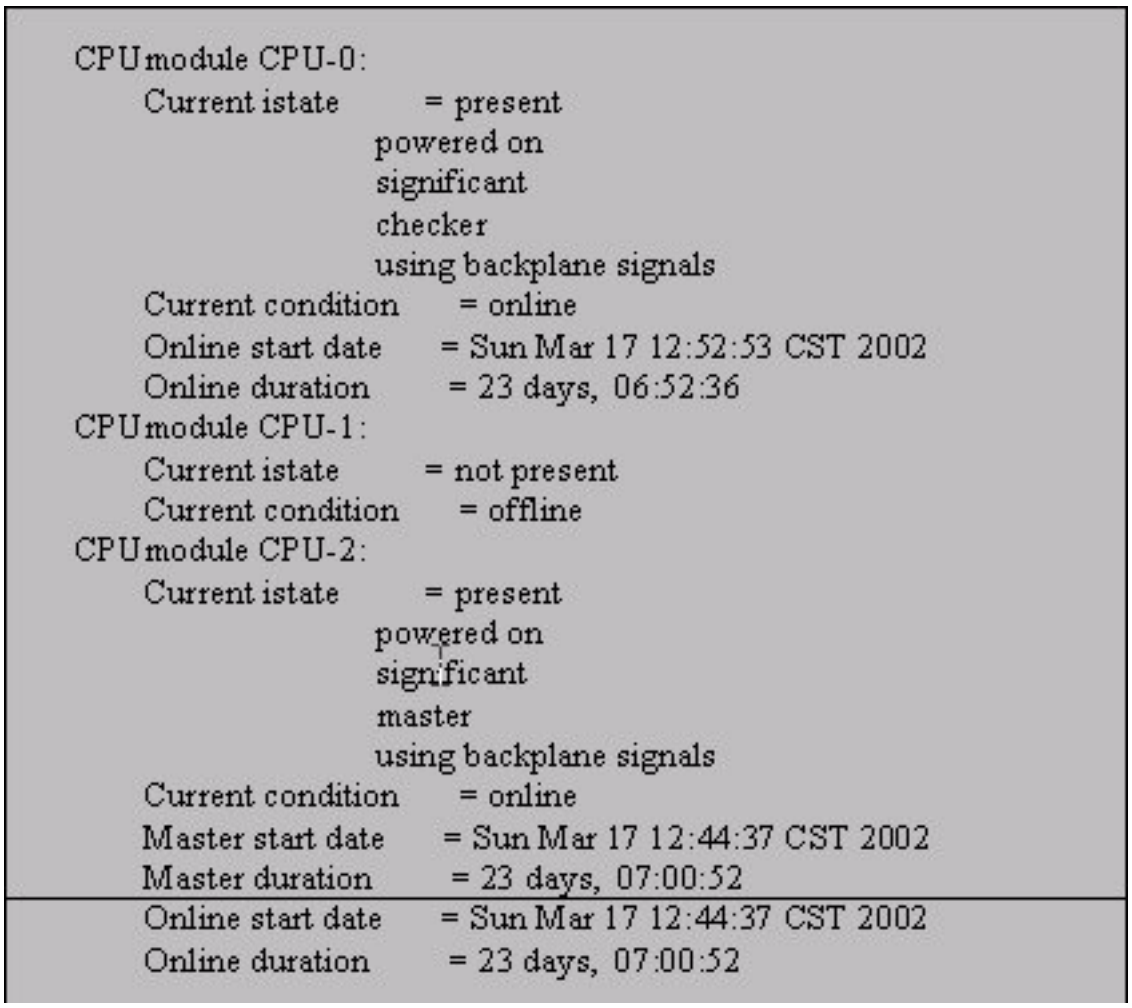
Performing the CPU stability pre-check

At the VT100 console

1 Determine which CPU is currently master:

```
ftctl -status
```

Example response:



Note: CPU 0 is installed in Domain 0. CPU 2 is installed in Domain 1.

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:

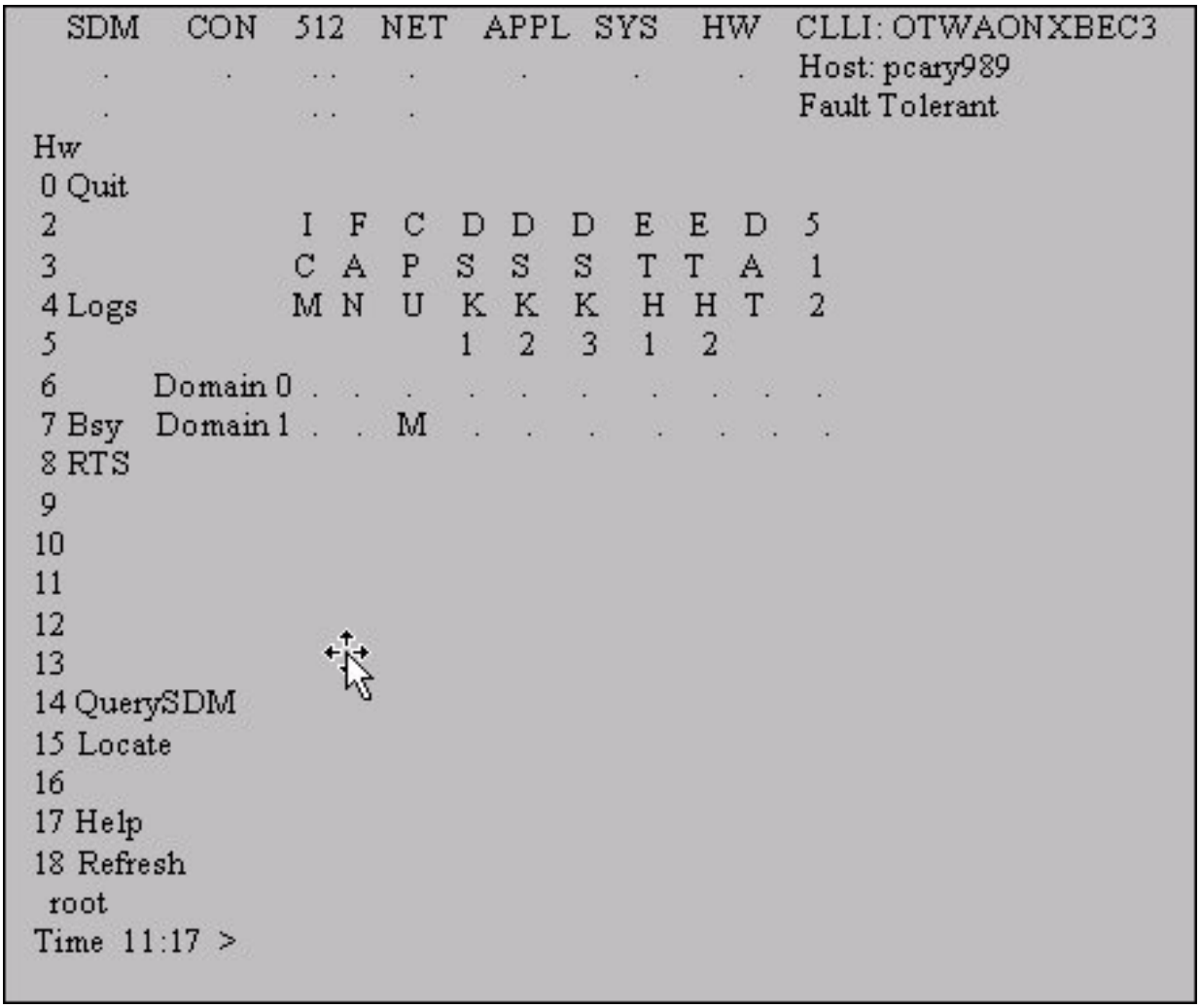
`bsy  <domain> cpu`

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

Note: CPU status changes from M (busy) to I (re-integration). Re-integration time will vary depending on system configuration.

Example

```
rts 1 cpu
```

If the rts command	Do
succeeds	step 6
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.

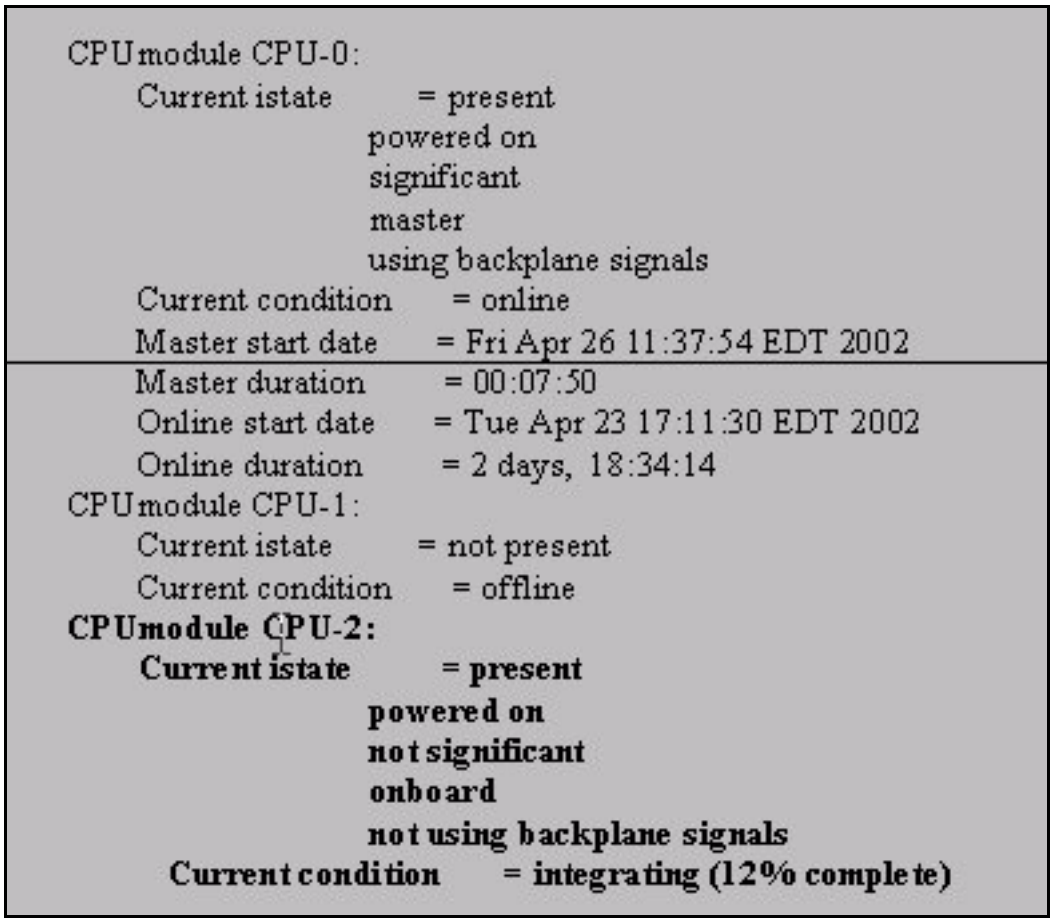
6 Exit the hardware level:

```
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 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 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 or 1)

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 or 1)

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 >
```

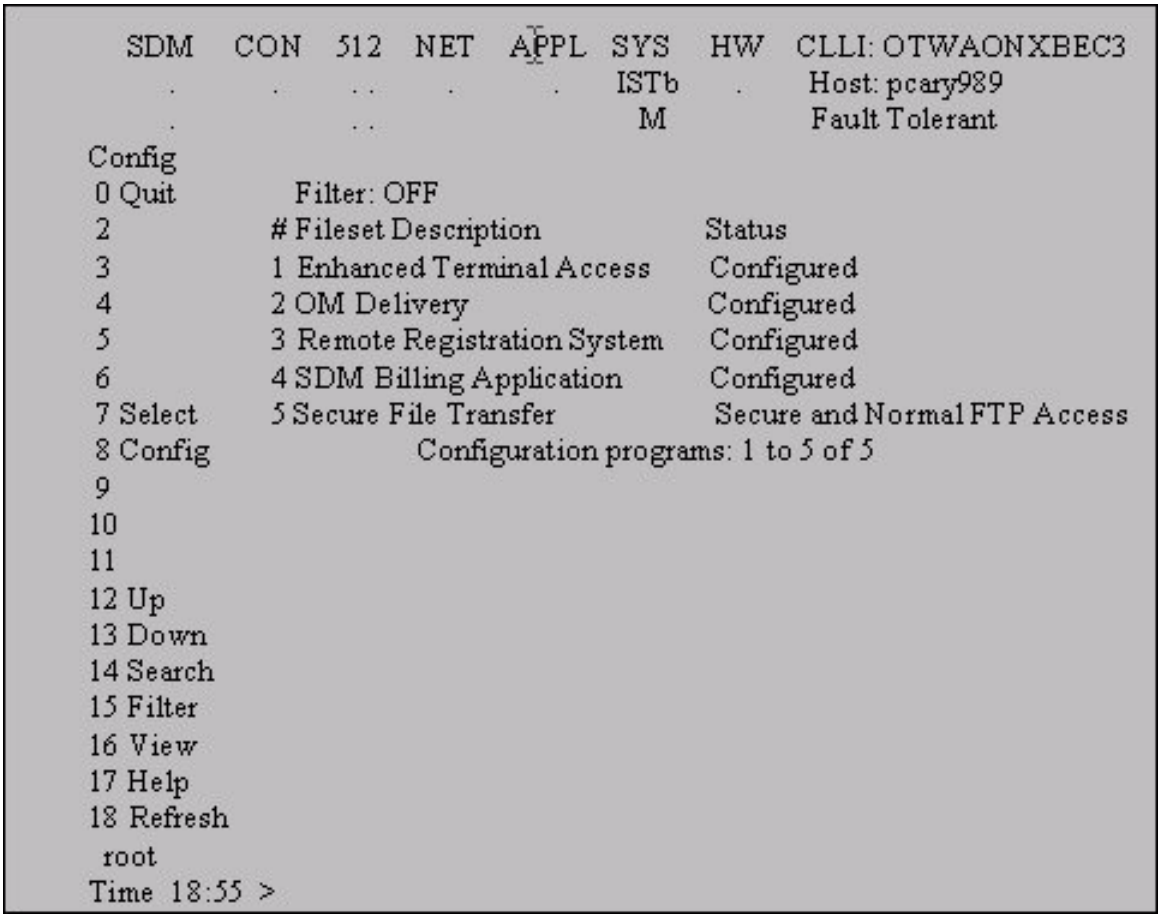
2 Verify that all applications used are in service (represented by a dot [.] under the “State” header). Use the up/down commands to scroll through the list of applications if necessary.

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 configuration, status, and transmission path to external network element(s).

Performing the Ethernet configuration pre-check

At the VT100 console

1 Obtain and record the IP gateway addresses for Ethernet interface ent0 and ent1.

2 Display the Ethernet configuration and status:

```
lsstate -s | grep ent
```

The system will display the Ethernet configuration. The following is an example of this kind of display:

Example response:

```
pent0  c1-f2   Available  online       Physical Ethernet Device
pent1  c1-f4   Available  online       Physical Ethernet Device
pent2  c1-f13  Available  online       Physical Ethernet Device
pent3  c1-f15  Available  online       Physical Ethernet Device
ent0           Available  online_both  FT Logical Ethernet
ent1           Available  online_both  FT Logical Ethernet
```

dbgent

The system will display the Ethernet status. The following is an example of this kind of display:

Example response:

```
ent1:

    member0  pent1  active    (08:00:3e:26:25:21)    PM: online
    member1  pent3  backup    (08:00:3e:26:25:25)    PM: online

ent0:

    member0  pent0  backup    (08:00:3e:26:25:24)    PM: online
    member1  pent2  active    (08:00:3e:26:25:20)    PM: online
```

3 Using the information obtained in step 1, verify that the selected external network element can be reached.

ping -c 3 <ip_address>

The following example shows a sample ping command used to ping the Gateway router for ent0 and the format of the results that the system displays in response:

Example

```
# ping -c 3 47.101.50.112
PING 47.101.50.112:(47.101.50.112): 56 data bytes
64 bytes from 47.101.50.112: icmp_seq=0 ttl=61 time=1 ms
64 bytes from 47.101.50.112: icmp_seq=1 ttl=61 time=1 ms
64 bytes from 47.101.50.112: icmp_seq=2 ttl=61 time=1ms

----47.101.50.112 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=1/1/1 ms
```

4 Switch the active and backup Ethernet interface members:

dbgent -sl ent*n*

where

n
is either 0 or 1

Example
dbgent -sl ent0

5 Verify that the switch occurred.

dbgent

The following example display shows that the active and backup Ethernet interface members for ent0 have switched. Compare the display for ent0 below with that for ent0 in step 2 in the example response to the dbgent command.

Example response:

```
ent1:

    member0  pent1  active    (08:00:3e:26:25:21)   PM: online
    member1  pent3  backup    (08:00:3e:26:25:25)   PM: online

ent0:

    member0  pent0  active    (08:00:3e:26:25:20)   PM: online
    member1  pent2  backup    (08:00:3e:26:25:24)   PM: online
```

6 Using the information obtained in step 1, verify that the selected external network element can still be reached.

ping -c 3 <ip_address>

The following example shows a sample ping command used to ping the Gateway router for ent0 and the format of the results that the system displays in response:

Example

```
# ping -c 3 47.101.50.112
PING 47.101.50.112:(47.101.50.112): 56 data bytes
64 bytes from 47.101.50.112: icmp_seq=0 ttl=61 time=1 ms
64 bytes from 47.101.50.112: icmp_seq=1 ttl=61 time=1 ms
64 bytes from 47.101.50.112: icmp_seq=2 ttl=61 time=1ms

----47.101.50.112 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=1/1/1 ms
```

7 Switch the active and backup Ethernet interfaces.

dbgent -sl ent*n*

where

n
is either 0 or 1

Example
dbgent -sl ent0

8 Verify that the switch occurred.

`dbgent`

The following example display shows that the active and backup Ethernet interface members for ent0 have switched. Compare the display for ent0 below with that for ent0 in step 5 in the example response to the dbgent command.

Example response:

ent1:

```
member0  pent1  active    (08:00:3e:26:25:21)   PM: online
member1  pent3  backup    (08:00:3e:26:25:25)   PM: online
```

ent0:

```
member0  pent0  backup    (08:00:3e:26:25:24)   PM: online
member1  pent2  active    (08:00:3e:26:25:20)   PM: online
```

9 Repeat steps 3 through 8 for the second Ethernet (ent0 or ent1).

10 You have completed this procedure.

System dump device pre-check

The purpose of the System dump device pre-check is to verify that the system dump devices are not in the “null” state. If either device is in the null state, your upgrade will fail.

Performing the system dump device pre-check

At the VT100 console

1 Verify the system dump (sysdump) devices by completing the following steps.

Start the verification:

```
sysdumpdev -l
```

Note: In the command above, the “**l**” is a lower-case letter L.

If the following message is displayed	Do
primary /dev/sysdump0 secondary /dev/sysdumpnull copy directory /var/adm/ras forced copy flag FALSE always allow dump FALSE dump compression OFF	step 2
primary /dev/sysdump0 secondary /dev/sysdump1 copy directory /var/adm/ras forced copy flag FALSE always allow dump FALSE dump compression OFF	step 3

2 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
```

3 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 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
```

Note: If this command fails because there are no patches applied on the CS 2000 Core Manager, the following message is displayed: "Create the FIXES filesystem from sdmmtc;fixes and retry this." You should, then, create the FIXES directory as requested in this message using the following procedure:

1. Create the fixes directory by entering the following command and responding to the prompts it displays:

   sdmmtc fixes

2. Exit from the maintenance interface:

   quit all

3. Enter the maintenance interface:

   sdmmtc

4. Return to step 6, above.

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
```

Note: If this command fails, the following message may be displayed: "Create the FIXES filesystem from sdmmtc;fixes and retry this." This message displays when the FIXES directory does not exist on the core manager. You should, then, create the FIXES directory as requested in this message using the following procedure:

1. Create the fixes directory:

   sdmmtc fixes

2. Exit from the maintenance interface:

   quit all

3. Enter the maintenance interface:

   sdmmtc

4. Return to step 6, above.

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: `Successfully deposited all filesets to <directory name>` **Record the directory path for reference.**	go to step 11
displays a failure message ***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.

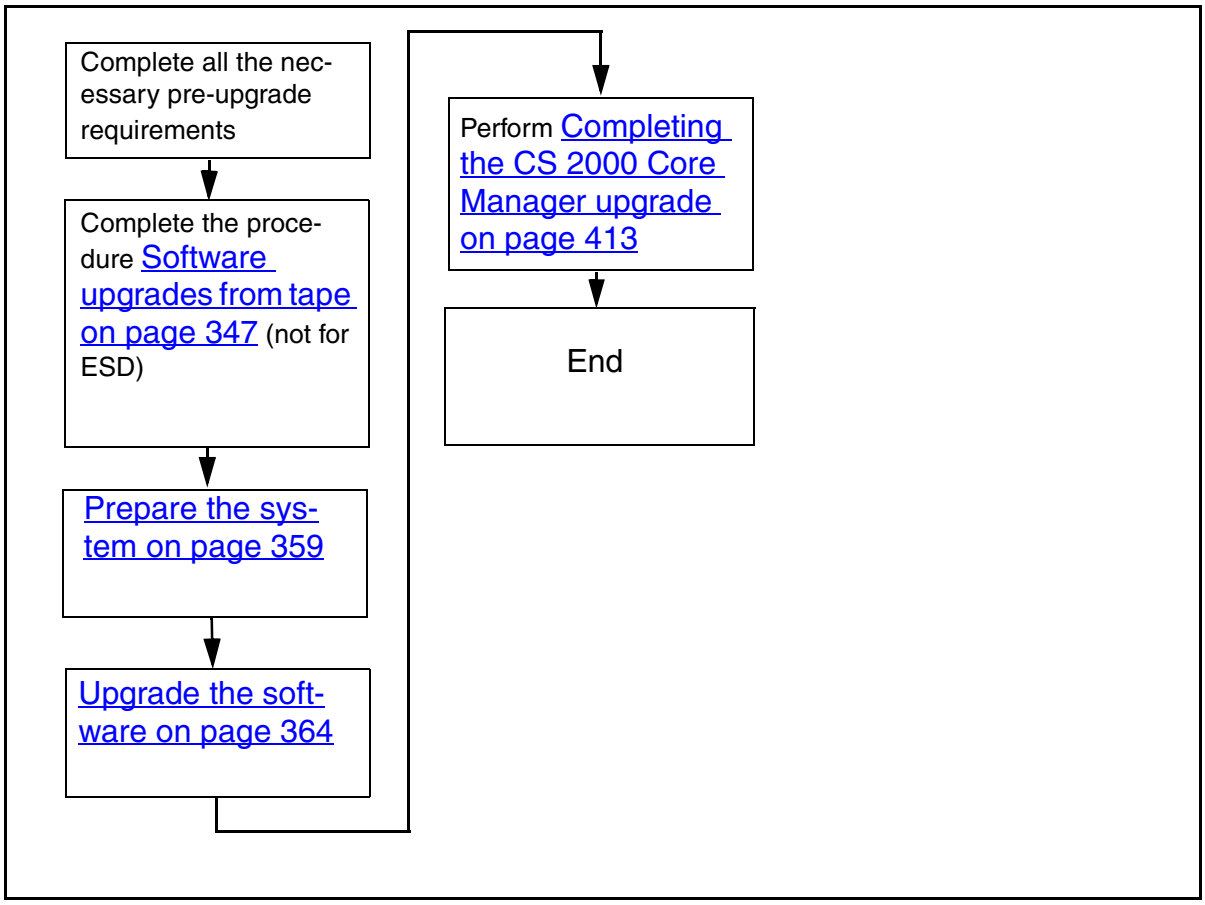
10 Once the DAT drive is clean, repeat steps 1 through 8.

11 You have completed this procedure. You are now ready to upgrade the CS 2000 Core Manager software.

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 to the new software 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 319 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 for the new software release.

  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 349.

- 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. Use the following commands to query AFT sessions: **`billmtc, appl, aft, aftconfg, list`**. To verify which billing files for each session are still pending, enter the following commands: **`billmtc, appl, aft, query <session_name>`**. ***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 the new software release.

ATTENTION
Some obsolete applications in SN07 are automatically removed. If Remote Registration system fileset is present, it is automatically removed when upgrading to the new software release.

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 on page 354 and Upgrade notices on page 358 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

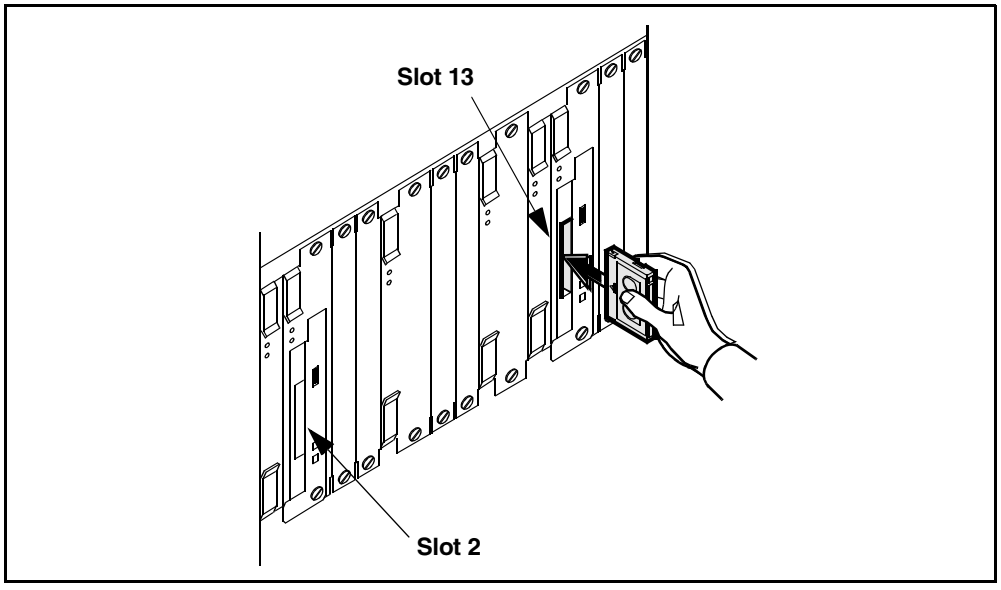
2 Log on to the CS 2000 Core Manager using the root user ID and password

3 If you are upgrading from tape (not from ESD), verify that the procedure Uploading the software from tape to a disk on page 349 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 ***Note:*** A directory created during ESD or during procedure Uploading the software from tape to a disk on page 349	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 for the new software load into the tape drive in slot 13 (DAT1) as shown in the following figure, and continue with step 5. ***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 349	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 secondary /dev/sysdumpnull copy directory /var/adm/ras forced copy flag FALSE always allow dump FALSE dump compression OFF	step 12
primary /dev/sysdump0 secondary /dev/sysdump1 copy directory /var/adm/ras forced copy flag FALSE always allow dump FALSE 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 for the new software release 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 for the new software release, 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 new software 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 349.	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 on page 349 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
```

Note: If there are Custom Log Devices defined in logroute, follow the steps in the appropriate Configuration Management NTP, such as, *CS 2000 Core Manager Configuration Management*, NN10104-511, or *SDM Configuration Management*, NN10103-511.

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 a new software load or from CS2E0006 to a new software load	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 380, 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 applications and services	step 50
do not need to install new applications and services	step 51

50 Install new 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 305.

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 352.

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 413.

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:

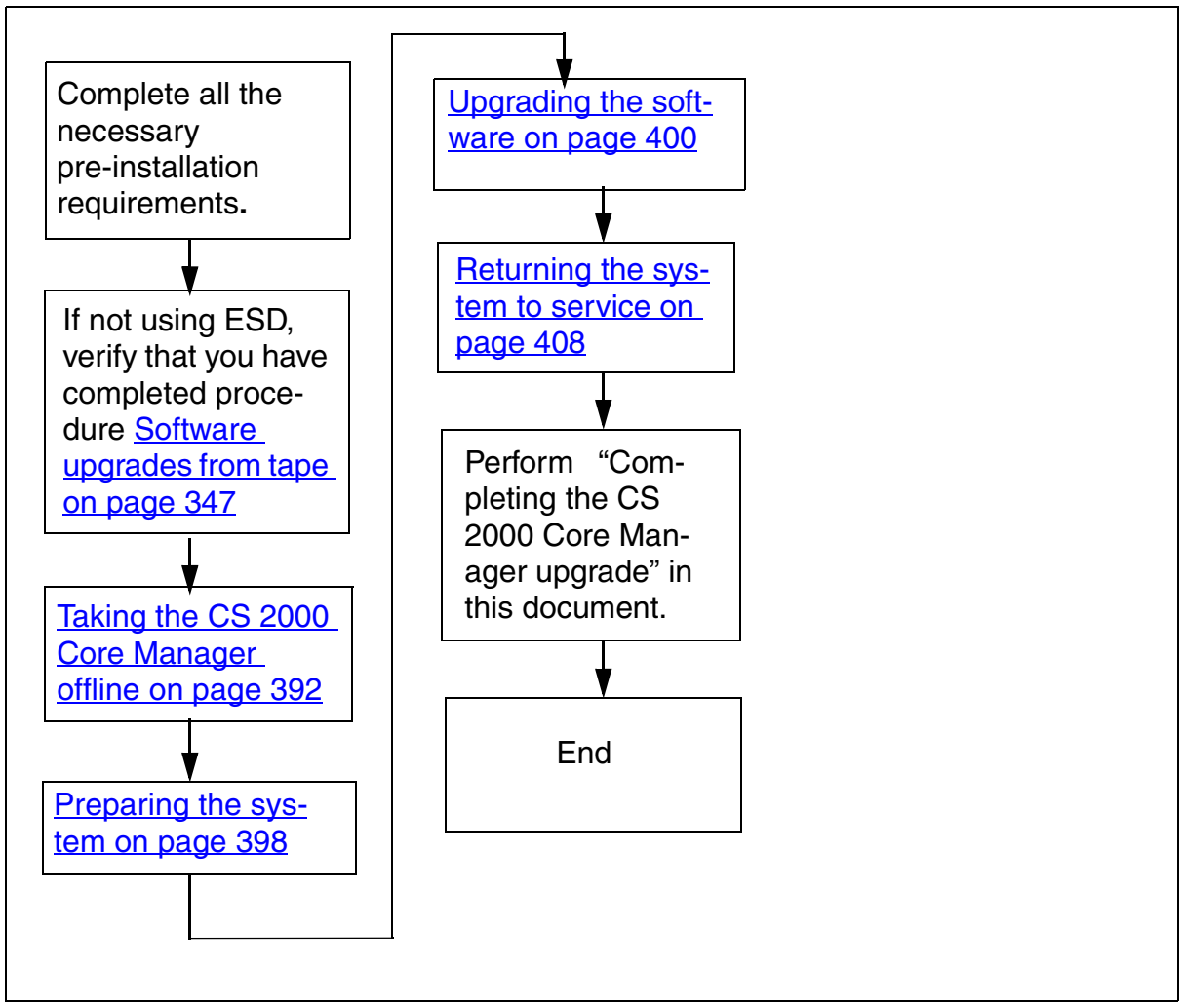
```
> quit all
```

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 describes the process to upgrade the CS 2000 Core Manager to the new software 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 319 procedure were successfully completed seven days before starting this upgrade.
- Perform a system image backup.

  ATTENTION

  Nortel 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 as the root user to perform the upgrade. 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 for the new software load.
- 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. The /usr logical volume must have a minimum size of 1050Mb.

Before starting the upgrade, ensure that /usr is less than 50% full. 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.
- If you are upgrading to SN07 or a higher release, offline and remove the application, “Ineo SSH Secure File Transfer” using the procedure Removing the “Ineo SSH Secure File Transfer” application on page 387

Removing the “Ineo SSH Secure File Transfer” application

At the VT100 console or telnet session

1 Log on to the CS 2000 Core Manager using the root user ID and password.

2 Access the application level of the SDMMTC interface:

```
# sdmmtc appl
```

3 In the display, locate the Ineo SSH Secure File Transfer application.

If	Do
Ineo SSH Secure File Transfer is installed on your system	step 4
Ineo SSH Secure File Transfer is not installed on your system	step 9

4 If the Ineo SSH Secure File Transfer application is in service, busy it and take it offline:

```
> bsy <number>
> offl <number>
```

where

<number>
is the number displayed on the screen that is associated with the Ineo SSH Secure File Transfer application

5 Access the details level:

```
> details
```

6 Remove the Ineo SSH Secure File Transfer application from the system:

```
> select <number>
> remove
```

where

<number>
is the number displayed on the screen that is associated with the Ineo SSH Secure File Transfer application

The system will provide output similar to that in the following example:

Example
WARNING: If you proceed with this action, all versions of the

following fileset will be removed from the system:

Ineo SSH Secure File Transfer

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, or “N”)

7 Confirm the removal of this application:

```
> Yes
```

8 Exit from the maintenance interface:

```
> quit all
```

9 You have completed this procedure.

Post-upgrade notes

You must be aware of the following information.

Note: If, after this upgrade, the “source” command (at the sdmmtc/apply level) fails, the following message is displayed: “Create the FIXES filesystem from sdmmtc;fixes and retry this.” This message displays when the FIXES directory does not exist on the core manager. You should, then, create the FIXES directory as requested in this message.

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 the new software load.

Procedures

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

ATTENTION

Read the instructions in Pre-upgrade requirements on page 384 and Upgrade notices on page 389, and complete any necessary activities before you proceed with the upgrade.

ATTENTION

Nortel recommends that you deliver unprocessed billing files downstream. Ensure that no unprocessed billing file remains on the system.

ATTENTION

Nortel 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 347 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. Use the following commands to query AFT sessions: **`billmtc, appl, aft, aftconfg, list`**. 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 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.

CAUTION: Before continuing with the upgrade, verify that there are no files in the /sba/ama/closedNotSent directory. Otherwise, the billing center may receive duplicate billing records. If files exist in the /sba/ama/closedNotSent directory, perform a manual backup. If files still exist in the /sba/ama/closedNotSent directory after manual backup, contact your next level of support.

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.

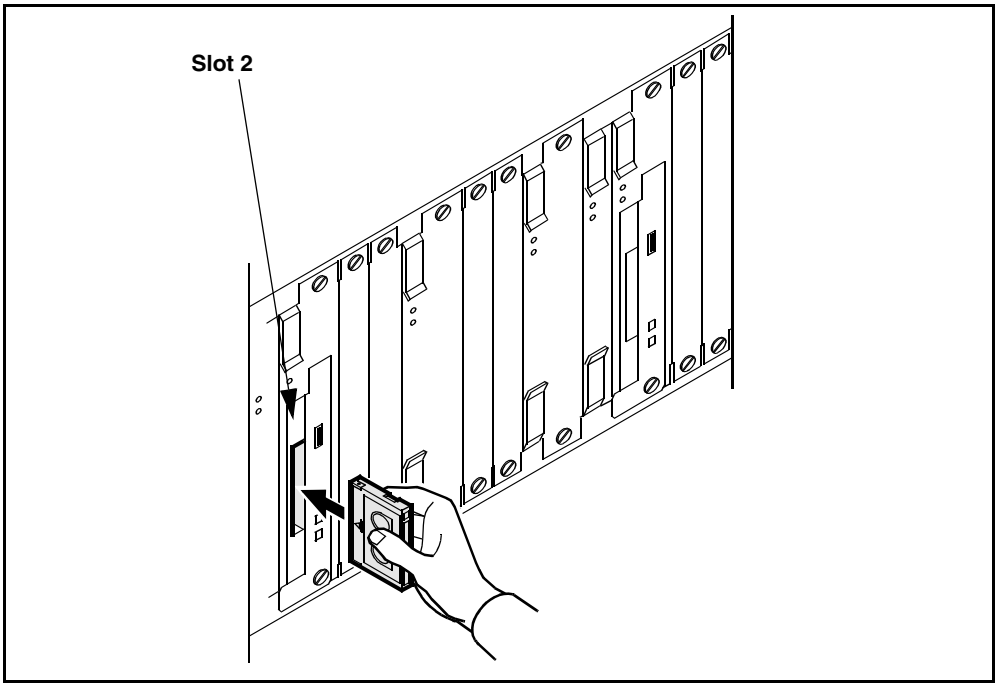
Preparing the system

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 347	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 for the new software load into the tape drive in slot 2 as shown in the following figure, and continue with step 2. ***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, or later, 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: CS2E0080.0 : 21.60.8.0
```

The displayed product name (in this example, CS2E0080.0) 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 After removing the archived filesets, ensure that /usr logical volume is less than 50% full. To check the "% full" value of /usr, enter the following command:

```
sdmmtc storage
```

Note: If /usr is more than 50% full, refer to procedure "Increasing the size of a logical volume" in NN10170-611, *CS 2000 Core Manager Security and Administration* to increase the /usr logical volume size as required. The /usr logical volume must have minimum size of 1050Mb.

9 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 347	list the filesets: **`apply <directory path>`** ***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” In the sdmmtc rmi window: OSS Comms Svcs MORE... (100%)	step 6
not prompted to configure “OSS Comms Svcs”	step 8

Note: If there are Custom Log Devices defined in logroute, follow the steps in the appropriate Configuration Management NTP, such as, *CS 2000 Core Manager Configuration Management*, NN10104-511, or *SDM Configuration Management*, NN10103-511.

6 Press the space bar to display the DDMS Clients Configuration menu.

```
##############################################
# Configuring 'SDM_DDMS.osscomms'.

##############################################


########################################
#     Configuring DDMS clients         #
########################################

           DDMS Clients Configuration


0. Quit

1. Add new clients

2. Remove existing client

3. List existing clients


Enter choice:
```

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 384 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
```

If	Do
faults are present	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 for installing the SDM bundle.

If you are upgrading	Do
from a directory created during ESD or during the procedure Software upgrades from tape on page 347	list the filesets: **`apply <directory path>`** ***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**

17 Install the “sdm” software:

```
apply bundle sdm
```

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 18
not prompted to confirm the apply command	step 24

18 Confirm the apply command:

```
y
```

Response

```
Command completed with no errors
```

If you are	Do
prompted to reboot the system	step 19
not prompted to reboot the system	press Enter and continue with step 24

19 Confirm the system reboot:

```
y
```

20 Once the system has finished rebooting, log into the CS 2000 Core Manager using the root user ID and password.

21 Wait until all cards at the hardware level are in service before you proceed. Monitor the status of the cards as described in steps 22 and 23.

22 Access the hardware level of the maintenance interface:

```
sdmmtc hw
```

23 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 NTP, and return to this procedure
no faults are present	step 24

24 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 319.

If you	Do
have X.25	step 25
do not have X.25	step 30

25 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 347	list the filesets: **apply <directory path>** ***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**

26 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 27
not prompted to confirm the apply command	step 30

27 Confirm the apply command:

y

Response

```
Command completed with no errors
```

If you are	Do
prompted to reboot the system	step 28
not prompted to reboot the system	press Enter and continue with step 30

28 Confirm the system reboot:

y

29 Once the system has finished rebooting, log into the CS 2000 Core Manager using the root user ID and password.

30 Wait until all cards at the hardware level are in service before you proceed. Monitor the status of the cards as described in steps 31 and 32.

31 Access the hardware level of the maintenance interface:

sdmmtc hw

32 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 NTP, and return to this procedure
no faults are present	step 33

33 If you have the DNBD Call Monitoring Application on your system, upgrade it by following the appropriate procedure in the International Lawful Interception NTP, and then return to step 34

34 You have completed this procedure.

Returning the system to service

35 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 392.

At the console connected to SP0 (VT100 or remote access)

36 Use the following table to determine your next step.

If your core manager	Do
is connected to the CS 2000 - Compact	step 37
is not connected to the CS 2000 - Compact	step 38

37 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 41

At the MAP display

38 Access the SDM level of the MAP display:

```
mapci;mtc;appl;sdm
```

39 Change the state of the CS 2000 Core Manager from offline to busy:

```
bsy
```

40 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)

41 Use the following table to determine your next step.

If the SBA application	Do
was not offline prior to the upgrade	step 42
was offline prior to the upgrade	step 55
is not installed on your system	step 55

42 Access the APPL level of the maintenance interface:

```
sdmmtc appl
```

43 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.

44 Busy the SBA:

```
bsy <application_number>
```

where

<application_number>
is the number next to the SuperNode Billing Application

45 Confirm the command:

```
y
```

If the SBA application	Do
was in service prior to the upgrade	step 46
was busy prior to the upgrade	step 55

46 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 47
is not installed on your system	step 51

47 Use the following table to determine your next step.

If the AFT application	Do
was not offline prior to the upgrade	step 48
was offline prior to the upgrade	step 51

48 Busy the AFT application:

```
bsy <application_number>
```

where

<application_number>
is the number next to the Automatic File Transfer application

49 Confirm the command:

```
y
```

If the AFT application	Do
was in service prior to the upgrade	step 50
was not in service prior to the upgrade	step 51

50 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

51 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

52 Return the posted stream to service:

```
rts
```

53 Repeat steps 51 and 52 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)

54 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 55
did not increase from the first query command (meaning billing is not working)	contact your next level of support

55 Use the following table to determine your next step.

If you	Do
need to install new applications and services	step 56
do not need to install new applications and services	step 57

56 Install new 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 57.

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 305 in the Upgrades section.

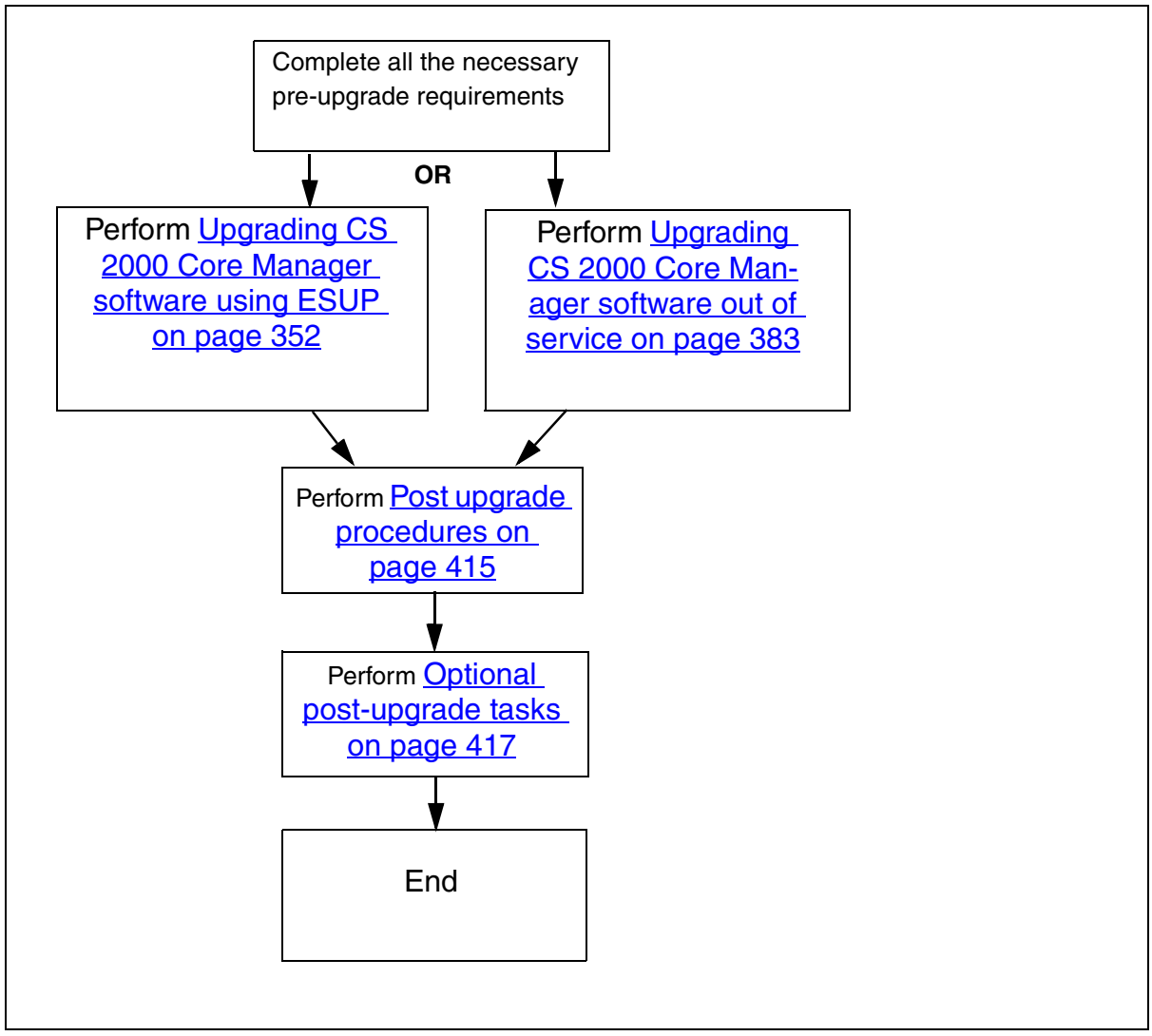
Note 2: Install new applications and services from the console connected to SP0 (local VT100 terminal or remote access).

57 You have completed this procedure. Go to “Completing the CS 2000 Core Manager upgrade”, in this document.

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 415.
- verify the current software load, to confirm that the upgrade was successful. Use the procedure Verifying the current software load on page 416.
- 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 418.

If you upgraded from tape, eject the tape 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 446. Carrier Voice over IP 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 417.
- 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 420. For more information, contact your next level of support.

Post upgrade procedures

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

Verifying the application state

At the VT100 console

1 Access the application level of the 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 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 416.

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 the release that you are upgrading to:

```
# querysdm loads
```

If the product code	Do
is the correct release	step 3
is not the correct release	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 Updating the CS 2000 Core Manager software version number on the Integrated EMS (IEMS) on page 416.

Updating the CS 2000 Core Manager software version number on the Integrated EMS (IEMS)

At the IEMS

1 Edit the object properties in the IEMS for the CS 2000 Core element manager you just upgraded to reflect the new software

version. Refer to either of the procedures that follow to update the software version in the Device Version field.

- Editing and viewing object properties using Web Client on page 1846
- Editing and viewing object properties using Java Web Client on page 1841

2 You have completed this procedure. Proceed to Optional post-upgrade tasks on page 417.

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.

Note: You may need to contact your system administrator, as client-side upgrades require secure access to the workstations.

2 After your CS 2000 Core Manager is upgraded to the new software 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 Stopping and starting the DDMS proxy on page 450.

b Stop and start the Tomcat Servlet Container component on the CS 2000 Management Tools server. Refer to Stopping and starting the Apache Web Server and Tomcat Servlet Container on page 452.

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 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.

Upgrading the CS 2000 Core Manager with software patches

Purpose

Use this procedure to upgrade your CS 2000 Core Manager with software patches.

Prerequisites

ATTENTION

Before continuing with patch application, verify that there are no files in the /sba/ama/closedNotSent directory. Otherwise, the billing center may receive duplicate billing records. If files exist in the /sba/ama/closedNotSent directory, perform a manual backup. If files still exist in the /sba/ama/closedNotSent directory after manual backup, contact your next level of support.

Application

The information that follows indicates how to upgrade your CS 2000 Core Manager with software patches, and includes the following procedures:

- Applying the SDM_CERTS.Certs Package on page 309
- Setting the schedule to apply fixes automatically on page 425
- Applying fix filesets manually on page 424
- Changing the default fixes directory on page 426

ATTENTIONAttention

Before applying the fixes fileset you should capture the session file. See Capturing the pre-check session file on page 320.

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 1: Patches for the CS 2000 Core Manager are referred to in this document as fix filesets.

Note 2: To utilize the software authentication feature, the SDM_CERTS.Certs package must be applied.

Note 3: If software authentication has been enabled on your system, monitor the maintenance interface for any logs or alarms respecting software authentication failures.

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 424 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 configured 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 the Security and Administration document.

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 423. Fix filesets that require user intervention need to be applied manually. Refer to Manual installation of fix filesets on page 424.

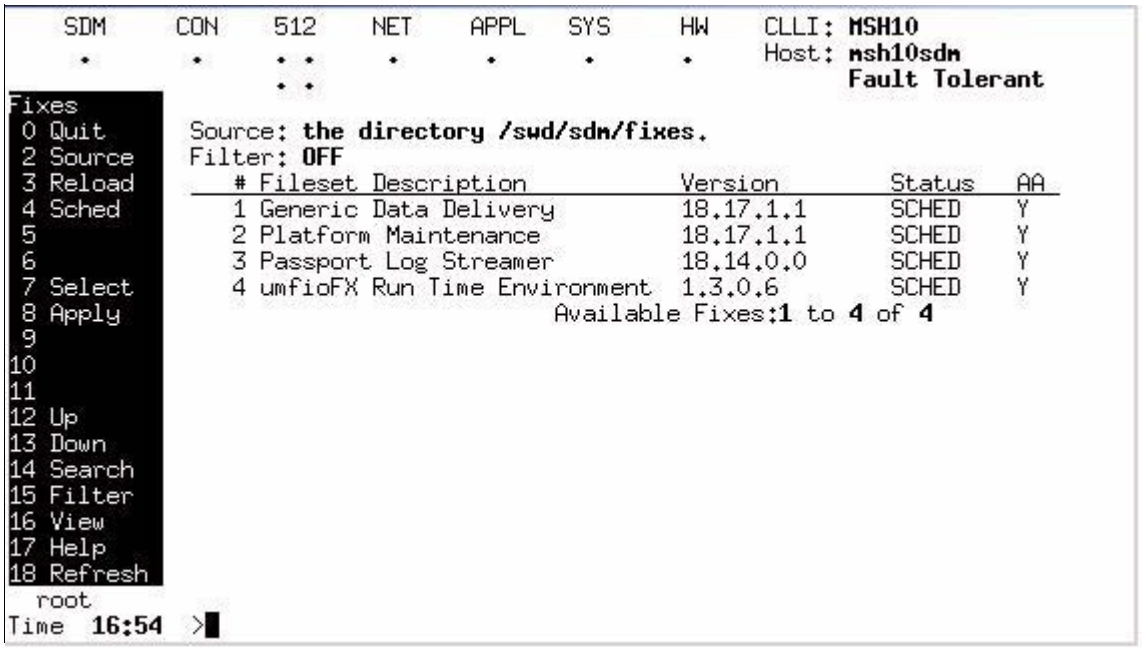
Once the fix filesets have been successfully applied, they are deleted from the configured directory. The associated release notes, if present, are also deleted.

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), the fix fileset has dependencies that have not been installed and are not available. Contact your Nortel 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 424 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 424.

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 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 1: 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.

Note 2: Beginning with release SDM20, the SDM maintenance interface (sdmmtc) expects a filesystem, rather than a directory, that contains patches. Prior to the SDM20 release, sdmmtc could list patches from any directory, whether or not the directory was a filesystem.

Procedures

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

Applying fix filesets manually

ATTENTION

Before continuing with patch application, verify that there are no files in the /sba/ama/closedNotSent directory. Otherwise, the billing center may receive duplicate billing records. If files exist in the /sba/ama/closedNotSent directory, perform a manual backup. If files still exist in the /sba/ama/closedNotSent directory after manual backup, contact your next level of support.

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 on page 424 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

ATTENTION
Before continuing with patch application, verify that there are no files in the /sba/ama/closedNotSent directory. Otherwise, the billing center may receive duplicate billing records. If files exist in the /sba/ama/closedNotSent directory, perform a manual backup. If files still exist in the /sba/ama/closedNotSent directory after manual backup, contact your next level of support.

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.

Example 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, and complete the prompts for the specified interval.

7 When prompted, confirm your entry:

`y`

Example 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.

Note: Enter the full directory path when specifying a directory.

Example 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 DCE

Purpose

Use this procedure to upgrade your Distributed Computing Environment (DCE).

Application

ATTENTION
This procedure will upgrade the DCE system files and provide the cell_admin user with sdm_admin sub administrator account access permissions.

These access 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 must be specified when performing subsequent CS 2000 Core Manager DCE administration and upgrade tasks.

For more information about DCE, refer to the following procedures:

- “Creating a DCE user” in the Security and Administration document
- “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 the Security and Administration document
- “Updating DCE principal names” in the Security and Administration document

Procedure

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

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.

Example 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).

Example response:

```
DCE administrator password:
```

3 At the prompt, enter the password for the DCE cell_admin user ID.

Example 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.

Installing or upgrading OpenSSH

Purpose

Use this procedure 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.

If the software is	Do
on tape	step 2
in a directory	step 3

2 Insert the tape labeled for the new release into the tape drive in slot 2, and continue with step 3

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

3 Access the maintenance interface:

```
# sdmmtc
```

If the software is	Do
on tape	list the filesets: **`apply 0`**
in a directory	list the filesets: **`apply <directory_path>`**

4 Select the latest version of the OpenSSH fileset:

```
> select <x>
```

where

<x> is the number next to the OpenSSH fileset.

5 Apply the selected fileset:

```
> apply
```

6 Confirm the apply command:

```
> y
```

7 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.

If the software is	Do
on tape	step 2
in a directory	step 3

2 insert the new software load tape into slot 2 of the tape drive, and go to step 3

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

3 Access the maintenance interface:

```
# sdmmtc
```

If the software is	Do
on tape	list the filesets: apply 0
in a directory	list the filesets: apply <directory path>

4 Select the Reach Through SPM fileset:

```
> select <n>
```

where

<n> is the number next to the Remote Registration System fileset.

5 Apply the selected fileset:

```
> apply
```

6 Confirm the apply command:

```
> y
```

7 You have completed this procedure.

Installing or upgrading the GR740PT application server

Purpose

Use this procedure to install or upgrade the GR740 Pass Through (PT) application server on the core manager.

Prerequisites

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

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

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

CM EADAS TCP/IP configurations

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

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

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

EADAS channel assignments

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

Procedure

Installing the GR740PT application server

At the core manager

1 Log in to the CS 2000 Core Manager as the root user.

If the NCL filesets are	Do
on tape	step 2
in a directory	step 3

2 Insert the new software tape in slot 2 of the tape drive.

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

3 Access the maintenance interface:

```
# sdmmtc
```

The 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

```
GR740PT application server Installation

Command in Progress, x filesets to process.
Processing fileset x.

APPLYING GR740PT 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 the configuration. Use the following table to determine your next step.

If	Do
you are configuring GR740PT in non-secure mode	Go to step 9
you are configuring GR740PT in local secure mode	Go to step 10
you are configuring GR740PT in DCE secure mode	Go step 11

9 Use the following table to determine your next step.

If	Do
your system is configured for DCE	Step a
your system is not configured for DCE	Step b

a In response to the prompt that asks whether you want to configure the GR740PT fileset using DCE, respond with “N” or “No”.

b In response to the prompt, “Enter mode of security”, select **1** (Non-secure).

c After the configuration is complete, the system displays a response indicating successful installation. Go to step 12

10 Use the following table to determine your next step.

If	Do
your system is configured for DCE	Step a
your system is not configured for DCE	Step b

a In response to the prompt that asks whether you want to configure the GR740PT fileset using DCE, respond with “N” or “No”.

b In response to the prompt, “Enter mode of security”, select **2** (Local [SSH] security).

c After the configuration is complete, the system displays a response indicating successful installation. Go to step 12

11 In response to the prompt that asks whether you want to configure the GR740PT fileset using DCE, respond with “Y” or “Yes”.

You will then be prompted for DCE administrator’s ID (sdm_admin) and password. You must then select **3** (DCE security Secure mode) in response to the prompt to enter the mode of security.

After the configuration is complete, the system displays a response indicating successful installation.

Note: If you choose not to configure GR740PT in DCE secure mode, you must then choose either **1** (non-secure mode) or **2** (local secure mode) in order to complete the configuration.

12 You have completed this procedure.

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

Purpose

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

Application

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

Procedures

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

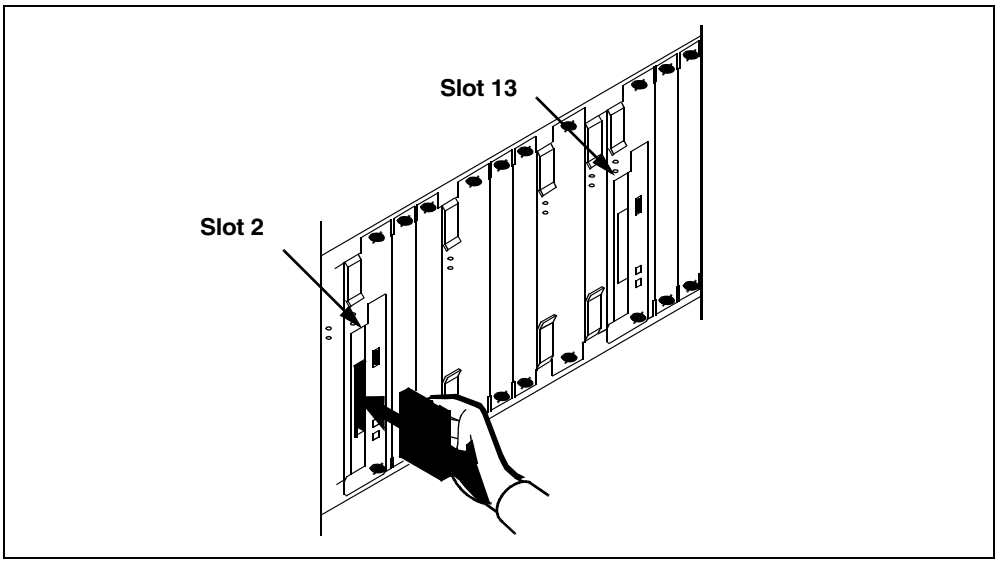
Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager

At the CS 2000 Core Manager

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

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

Tape drive in main chassis



At the maintenance interface

2 Determine the installation method.

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

If you choose to install OM Data Delivery by	Do
using telnet from a remote UNIX workstation to the CS 2000 Core Manager	step 3

3 Open a VT-100 compatible terminal window at the remote UNIX workstation.

4 Log onto the CS 2000 Core Manager from the terminal window prompt:

telnet <ip_address>

where

<ip_address> is the IP address of the CS 2000 Core Manager you want to install the Backup Restore Manager application on.

5 When prompted, enter the login ID and password for the root user.

6 Access the maintenance interface level:

sdmmtc

7 Access the software inventory manager (SWIM) level:

swim

The CS 2000 Core Manager lists the software applications currently installed.

8 List the contents of the tape you previously inserted:

apply <n>

where

<n>
is either 0 (slot 2) or 1 (slot 13).

9 Locate the Java Runtime Environment (JRE) 1.3 packages.

Note: If necessary, use the up (enter 12, u, or up) and down (enter 13, d, or down) commands to locate the JRE 1.3 packages.

10 Select and install the Java Runtime Environment Executables 1.3.0.0 package:

apply <n>

where

<n>
is the number next to the Java Runtime Environment Executables 1.3.0.0 package.

11 Confirm the apply command:

y

12 Select and install the Java Runtime Environment Libraries 1.3.0.0 package:

apply <n>

where

<n>
is the number next to the Java Runtime Environment Libraries 1.3.0.0 package.

13 Confirm the apply command:

y

14 Select and install the Java Runtime Environment Executables 1.3.0.15 package:

apply <n>

where

<n>
is the number next to the Java Runtime Environment Executables 1.3.0.15 package.

15 Confirm the apply command:

y

16 Select and install the Java Runtime Environment Libraries 1.3.0.15 package:

apply <n>

where

<n>
is the number next to the Java Runtime Environment Libraries 1.3.0.15 package.

17 Confirm the apply command:

y

18 Select and install Succession Provisioning Data Sync Manager (or Backup Restore Manager fileset, SDM_BKM.bkm).

```
apply <n>
```

where

<n>
is the number next to the Backup Restore Manager fileset, SDM_BKM.bkm (or Succession Prov Data Sync Manager)

19 Confirm the apply command:

```
y
```

20 As part of the Backup Restore Manager application installation, a script runs that enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). As the script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, “Creating the backup user ID on the core for SBRM” in *CS 2000 Core Manager Configuration Management*, NN10104-511, or in *ATM/IP Solution-level Security and Administration*, NN10402-600.

21 As the script continues to run, you are then prompted for the password of the user you entered (in step 20). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, “Creating the backup user ID on the core for SBRM” in *CS 2000 Core Manager Configuration Management*, NN10104-511, or in *ATM/IP Solution-level Security and Administration*, NN10402-600.

22 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.

23 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.

24 If, at any time after the installation is complete, you wish to re-configure the access to the core for the SBRM, perform the following steps:

a Access the config level of the SDM maintenance interface:

```
sdmmtc config
```

b From the list of filesets that displays, select the Succession Provisioning Data Sync Manager fileset (or Backup Restore Manager fileset, SDM_BKM.bkm) and then type **config**.

You will then be prompted again for the information that you supplied earlier in steps 20 through 23.

25 You have completed this procedure.

Purpose

Use this procedure to install the following filesets:

- AX4<release>-dmsDataSrv-CSU-000.tape
- AX4-<release.-TntFTPHndl-CSU-000.tape
- AX4-<release>-SAF-CSU-000.tape

Note: These filesets must be installed in the order listed above.

For more information about the CEM filesets, refer to NN10018-111, *CS 2000 Core Manager Basics*.

Procedure

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

At the CS 2000 Core Manager

1 Log on to the CS 2000 Core Manager as the root user.

If the software is	Do
on tape	step 2
in a directory	step 3

2 Insert the tape labeled for the new software load into the tape drive in slot 2, and continue with step 3

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

3 Access the maintenance interface:

```
sdmmtc
```

If the software is	Do
on tape	list the filesets: **`apply 0`**
in a directory	list the filesets: **`apply <directory_path>`**

4 Select the latest version of one of the CEM filesets:

`select <x>`

where

<x> is the number next to the fileset.

Note: The filesets must be installed in the order shown below:

- AX4<release>-dmsDataSrv-CSU-000.tape
- AX4-<release.-TntFTPHndl-CSU-000.tape
- AX4-<release>-SAF-CSU-000.tape

5 Apply the selected fileset:

`apply`

6 Confirm the apply command:

`y`

7 Return to step 4 and select another CEM fileset. If you have completed installing all of the CEM filesets, go to step 8

8 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.

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 Log in 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 -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Stop the DDMS proxy by typing

```
# /opt/nortel/NTsesm/admin/scripts/ddmsproxy stop
```

and pressing the Enter key.

6 Start the DDMS proxy by typing

```
# /opt/nortel/NTsesm/admin/scripts/ddmsproxy start
```

and pressing the Enter key.

7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to 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.

Core and Billing Manager (CBM) 850

ATTENTION

Upgrade the SSPFS software before upgrading any application software on the server.

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. If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.

Before upgrading the Core and Billing Manager 850

The Core and Billing Manager 850 component was introduced in the SN07 software release, therefore only SN07 to SN08 upgrades are supported.

Perform the required prerequisite upgrade as follows:

Network	CBM applies to:	Previous Upgrade
ATM	UA-AAL1 and PT-AAL2	Multiservice Data Manager (MDM) on page 215
IP	IAC- International, CHS - International, IAW, PT-IP and UA-IP[1]	Multiservice Data Manager (MDM) on page 215
	IAC - North America and CHS - North America	Ethernet Routing Switch 8600 on page 94
Tri-Modal	all applications	Multiservice Data Manager (MDM) on page 215

1.Includes IP International: PT-IP and UA-IP

After upgrading the Core and Billing Manager 850

Perform the next required upgrade as follows:

Network	CBM applies to:	Next Upgrade
ATM	UA-AAL1 and PT-AAL2	Integrated Element Management System (IEMS) on page 487
IP	PT-IP, UA-IP, IAW, IAC, and CHS[1]	Integrated Element Management System (IEMS) on page 487
Tri-Modal	all applications	Integrated Element Management System (IEMS) on page 487

1.Includes IP International: CHS, PT-IP, IAC, and UA-IP

About the Core and Billing Manager 850

The Core and Billing Manager 850 (CBM 850) offers terminal access to the core, the ability to transfer files to and from the core, log delivery service, and applications for managing accounting data and operational measurement (OM) data.

The CBM 850 enhances OAM&P functionality by enabling service providers to use their existing LAN resources to create an “operations intranet”, with Ethernet connectivity from the core to upstream OSSs, off-loading OAM&P responsibilities from the core.

Upgrading the CBM 850

Upgrade strategy

Upgrading the CBM 850 involves upgrading both the SSPFS platform and software, and upgrading the CBM 850 software. The SSPFS upgrade consists of two processes:

- upgrading the Solaris operating system
- upgrading the SSPFS software

The CBM upgrade also consists of two processes:

- preparing the CBM upgrade media
- applying and patching the new CBM software

The CBM upgrade is automatically initiated during the SSPFS upgrade.

ATTENTION
For a successful CBM 850 upgrade, all CBM software applications must be either in-service or offline.

ATTENTION
In order to perform the CBM 850 upgrade, the two nodes of the CBM 850 cluster must be in service.

ATTENTION
Before starting the upgrade, ensure that the currently-running CBM node is patch-current.

Procedures

Upgrading the CBM 850 consists of the following tasks:

- Preparing to upgrade the CBM 850 on page 457
- Upgrading the CBM 850 on page 461
- Completing the CBM 850 upgrade on page 476

Preparing to upgrade the CBM 850

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)SN08 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
1	Ensure that no SBA alarms are currently raised.		Use procedure “SBA alarm troubleshooting” in NN10351-911, *Core and Billing Manager 850 Fault Management* to check for alarms.
2	Ensure that adequate backup space is available on the core. During the CBM 850 upgrade, the billing application will go into backup.		To determine the amount of backup disk space required, see “Disk Space Requirements” in “Preparing for SBA installation and configuration” in NN10363-811, *Core and Billing Manager 850 Accounting*. To reconfigure backup volumes, refer to the procedure “Configuring SBA backup volumes on the core” in NN10363-811, *Core and Billing Manager 850 Accounting*.

(I)SN07 to (I)SN08 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
3	Ensure that the SN07 CBM 850 system is patch-current.		1. Launch your web browser. 2. Search for www.nortelnetworks.com 3. Under the pulldown menu labeled “Support and Training”, select “software downloads”. 4. In the “Find Products” box at the right side of the screen, click “Families” 5. In the “Product Families” list that displays, click “DMS” 6. In the “DMS: General Availability” list that displays, click “Software” under the “Core and Billing Manager” entry. 7. At the top of the list of software entries that displays, click “Filter and Sort” 8. Make the appropriate selections (such as CBM00070) in the sort boxes and then click “GO” 9. Create a directory in the “root” directory (/) on the CBM 850 to hold the patches that you have selected: **mkdir /<directory name>** 10. Download the patches from the RPS ftp site to an intermediary location. Then, ftp the patches from this location to the directory on your CBM 850 that you created in step 9. 11. Apply the patches on the CBM 850 by first logging in to the CBM 850 as the root user and then entering the following command: **patchctrl -d <directory name>** where <directory name> is the full pathname of the directory containing the patches.

(I)SN07 to (I)SN08 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
4	Prior to the upgrade, determine if the system has the necessary 9 GB unallocated disk space execute the following command as the root user: /opt/nortel/sspfs/fs/meta.pl fs The displayed value must be larger then "19000000" (19,000,000) for the upgrade to succeed. Note: If it is determined that there is not enough unallocated disk space to perform the upgrade, contact Nortel Technical Support.		If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in the *ATM/IP Security and Administration document*, NN10402-600.

Upgrading the CBM 850

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)SN08 CBM 850 upgrade checklist

	Activities	√	Procedures
1	Start the SSPFS platform and software upgrade.		Perform the steps in the procedure Upgrading SSPFS software on page 666 to the point at which you are prompted by the system to select the media used for the CBM upgrade.
2	Upgrade the CBM 850 software and applications.		The CBM 850 software and application upgrade occurs automatically as part of the SSPFS upgrade. When, during that upgrade, you are prompted to select the media used for the CBM upgrade, perform Procedure for upgrading a CBM 850 on page 462

Procedure for upgrading a CBM 850

ATTENTION

If errors are encountered during the CBM 850 upgrade, you have the choice of accessing a maintenance shell command line prompt or performing a fallback to the previous release. The maintenance shell provides the ability to correct the issue causing the error. Upon exiting the maintenance shell, the operation that failed will be re-executed. A fallback causes a return to the previous SSPFS and CBM 850 release.

At your workstation

1 The CBM 850 upgrade process is automatically initiated during the SSPFS upgrade process. When the program that runs the CBM 850 upgrade starts, the following banner displays:

```
============================================================
                    CBM Upgrade Media Setup
============================================================
========= Verify SSPFS Boot Environment (est. 2 sec) ... Completed.
======== Verify Remote Node communication (est. 3 sec) ... Completed.
Please select the software delivery method that is being used for the CBM
load?
  - enter 'esd' if Electronic Software Delivery is being used
  - enter 'cdrom' if CDROM is being used
  - enter 'shell' to suspend the upgrade and enter a Maintenance Shell.
  - enter 'fallback' to cancel the entire UPGRADE procedure
choice (esd | cdrom | shell | fallback):
```

In response to the prompt you may:

- enter “cdrom” to start the upgrade
- enter “shell” to suspend the upgrade and enter a Maintenance shell before continuing the upgrade
- enter “fallback” to cancel the entire upgrade procedure

Note: In release (I)SN08, ‘esd’ is only supported for emergency use when the cdrom media is defective. Therefore, ‘esd’ cannot be entered as the initial media for the

upgrade; only ‘cdrom’ can be entered as the initial media for the upgrade.

Use the following table to determine your next step.

If	Action
you entered “shell”	Go to step 2
you entered “fallback”	Go to step 3
you entered “cdrom”	Go to step 4

2 The system displays the following:

You have selected to enter a Maintenance Shell. Please contact next level of support to determine the proper course of action.

During the first part of the CBM 850 upgrade, that is, preparing the CBM upgrade media, the system informs you about what you will be prompted for when you exit the shell.

Proceed with shell? (yes | no):

Once the action has been completed, enter ‘exit’ at the command line prompt to return to the upgrade.

If	System response
you entered “yes”	A maintenance shell prompt appears. You may then either: - enter commands to perform some action or - enter “exit”. When you enter “exit”, the system will re-perform the last action it performed before you entered the maintenance shell. Go back to the step that you were performing when you selected to enter a maintenance shell.When you enter “exit”, you are re-prompted to enter either “cdrom”, “shell”, or “fallback”.
you entered “no”	When you enter “no”, the system will re-perform the last action it performed before you entered the maintenance shell. Go back to the step that you were performing when you selected to enter a maintenance shell.

3 The system displays the following:

```
You have selected to perform a fallback. This choice will cancel the entire
UPGRADE.
Proceed with fallback? (yes|no):
```

If	System response
you entered “yes”	The CBM 850 upgrade is cancelled and the node is brought to the ok prompt. Perform the procedure “Executing a fallback during an SSPFS-based server upgrade” in NN10408-900, *ATM/IP Fault Management* for more information.
you entered “no”	When you enter “no”, the system will re-perform the last action it performed before you selected to fallback. Go back to the step that you were performing when you selected to fallback.

4 The system displays the following:

```
Please insert the CBM CD disk into the CDROM drive.
Once the CD has been inserted, please select one of the following:
  - enter ‘continue’ to start the CBM portion of the upgrade.
  - enter ‘shell’ to suspend the upgrade and enter a Maintenance Shell.
  - enter ‘media’ to select a different CBM software delivery method.
  - enter ‘fallback’ to cancel the entire UPGRADE procedure.
Choice (continue | shell | media | fallback):
```

Insert the CBM CD disk into the CDROM drive and then respond to the system prompt.

If	Action
you entered “shell”	See step 2 for the system response.
you entered “fallback”	See step 3 for the system response.
you entered “continue”	See step 5 for the system response.

5 Use the following table to determine your next step:

If	Action
problems were encountered after you inserted the CD	Go to step 7.
no problems were encountered after you inserted the CD	Go to step 6

6 The system displays the following:

```
====== Allowing time for CD media to automount (est. 10 sec) ... Completed.
====== Checking CD media (est. 2 sec) ... Completed.
====== Preparing CBM CD Media for use (est. 5 min.) ... Completed
NOTIFICATION: ejecting cdrom (est. 1 sec) ... Completed.
============================================================
=== Invoking cbm_setup script to invoke the CBM portion of the Upgrade.
============================================================
```

Go to step 10.

7 The system displays the following:

```
====== Allowing time for CD media to automount (est. 10 sec) ... Completed.
====== Checking CD media (est. 2 sec) ... ERROR:
    The system displays the text for the particular error that was
    encountered.
Please insert the CBM CD disk into the CDROM drive.
Once the CD has been inserted, please select one of the following:
  - enter 'continue' to start the CBM portion of the upgrade.
  - enter 'shell' to suspend the upgrade and enter a Maintenance Shell.
  - enter 'media' to select a different CBM software delivery method.
  - enter 'fallback' to cancel the entire UPGRADE procedure.
Choice (continue | shell | media | fallback):
```

If	Action
you entered “shell”	See step 2 for the system response.
you entered “fallback”	See step 3 for the system response.

If	Action
you entered “media”	See step 8 for the system response.
you entered “continue”	See step 5 for the system response.

8 The system displays the following:

```
Please select the software delivery method that is being used for the CBM
load?
  - enter ‘esd’ if Electronic Software Delivery is being used
  - enter ‘cdrom’ if CDROM is being used
  - enter ‘shell’ to suspend the upgrade and enter a Maintenance Shell.
  - enter ‘fallback’ to cancel the entire UPGRADE procedure
choice (esd | cdrom | shell | fallback):
```

In response to the prompt you may:

- enter “esd” to select an ESD image to be used for the upgrade

  Note: The “esd” selection is only available when the cdrom media is defective and when an esd media has been prepared by Nortel for recovery purposes. Therefore, you should contact your next level of support before proceeding with the upgrade.

- enter “shell” to suspend the upgrade and enter a Maintenance shell before continuing the upgrade
- enter “fallback” to cancel the entire upgrade procedure

Use the following table to determine your next step.

If	Action
you entered “shell”	Go to step 2
you entered “fallback”	Go to step 3
you entered “esd”	Go to step 9
you entered “cdrom”	Go to step 4

9 If only one ESD image is found in the /swd/sdm directory, that image is selected by the system, by default, and you will not receive any additional prompts. If more than one ESD image is

found in the /swd/sdm directory, the system will display the list of images and a series of prompts for selecting the image to use as shown in the following example:

There appears to be more than one ESD image located within the /swd/sdm directory.

Please choose which ESD file you would like to use:

The system displays a list of ESD files from which to choose, for example:
1: CBM08_21.57.2.99.iso.gz.tape
2: CBM08_21.99.99.99.iso.gz.tape
3: CBM08_22.57.6.0.iso.gz.tape

- enter 'shell' to suspend the upgrade and enter a Maintenance Shell to retrieve the ESD image if it is not available.

- enter 'media' to re-select the CBM software delivery method.

- enter 'fallback' to cancel the entire UPGRADE procedure

choice (1-4 | esd | shell | media | fallback):

Once you have chosen a valid ESD image from the list, the system displays the following:

======== Verifying that this is a CBM ISO image (est. 2 sec) ... Completed.

======== Verifying disk space (est. 2 sec) ... Completed.

======== Preparing the CBM ESD Media for use (est. 3 min) ... Working

10 When the CBM upgrade begins, the upgrade program checks for any Major or Critical alarms on either node of the CBM 850 cluster and notifies you with information about any alarms that have been found. If alarms are found by the program, you may:

- enter 'shell' to suspend the upgrade and enter a Maintenance shell in order to address the problems indicated by the alarms
- enter 'fallback' to cancel the entire upgrade and fall back to the previous release
- enter 'continue' to continue the upgrade if the level or severity of the alarm does not warrant correction at this time

The following examples show samples of system displays when errors are discovered.

Example 1

The following example shows a sample upgrade display when alarms have been discovered and you choose to suspend the upgrade by entering 'shell' and address the alarms. This sample

does not show any commands entered to perform an alarm correction activity, but it does show exiting from the shell:

```
================================================
===     CBM Setup Program - UPGRADE procedure
================================================
======== Examine CBM Alarms (est. 1 min)...Warning:
================================================
        Detected MAJOR and/or CRITICAL alarms
Local Node:
Major:1
  ** SPFS340  MSH:  Cluster nodes out of sync.
Please investigate the alarms and/or contact your next level of support to
determine the next course of action.
 - enter 'shell' to suspend the upgrade and enter a Maintenance Shell
 - enter 'fallback' to cancel the entire UPGRADE procedure
 - enter 'continue' to proceed with the UPGRADE
NOTE:
During the upgrade, it is expected that the Cluster Nodes be out of Sync (i.e.
SPFS340 MSH: Cluster nodes out of Sync). This is the only alarm that may
be ignored - ALL OTHER ALARMS should be investigated before continuing.
Choice (shell/fallback/continue):shell
You have selected to enter a Maintenance Shell. Please contact next level of
support to determine the proper course of action.
Proceed with shell? (yes|no):yes
Once the action has been completed, enter 'exit' at the command line prompt
to return to the upgrade.
cbm_upgrade_shell:>
```

In response to the Maintenance Shell prompt, you may examine the alarms and perform any required actions. When you have completed any alarm examination and correction, you may enter "exit" to exit from the Maintenance Shell and resume the upgrade.

```
cbm_upgrade_shell:>exit
```

If you have resolved all of the alarms that have been discovered, the upgrade resumes. If you have not resolved all of the alarms that have been discovered, you will be prompted as to whether to continue the upgrade.

Example 2

The following example shows a sample upgrade display when alarms have been discovered and you choose to continue the upgrade without first correcting any alarms:

```
================================================
===     CBM Setup Program - UPGRADE procedure
================================================
======== Examine CBM Alarms (est. 1 min)...Warning:
================================================
        Detected MAJOR and/or CRITICAL alarms
Local Node:
Major:1
  ** SPFS340  MSH:  Cluster nodes out of sync.
Please investigate the alarms and/or contact your next level of support to
determine the next course of action.
 - enter 'shell' to suspend the upgrade and enter a Maintenance Shell
 - enter 'fallback' to cancel the entire UPGRADE procedure
 - enter 'continue' to proceed with the UPGRADE
NOTE:
During the upgrade, it is expected that the Cluster Nodes be out of Sync (i.e.
SPFS340 MSH: Cluster nodes out of Sync). This is the only alarm that may
be ignored - ALL OTHER ALARMS should be investigated before continuing.
Choice (shell/fallback/continue):continue
You have selected to proceed with the upgrade. Please confirm that you wish
to proceed with the upgrade.
Proceed with upgrade? (yes|no):yes
```

11 The CBM upgrade program examines the upgrade environment and prepares the system for the CBM upgrade.

Example

The following example shows a sample of the display that occurs as the upgrade environment is being examined:

```
======= Verify the CBM base directory (est. 5 sec) ... Completed
======= Verify disk space (est. 10 sec) ... Completed.
==== Preinstall CBM software management tools (est. 10 sec) ... Completed.
======= Prepare upgrade filesystem (est. 10 sec) ... Completed.
```

If problems are encountered during this portion of the upgrade, you will be prompted to enter either “shell” to suspend the upgrade and enter a Maintenance Shell or “fallback” to cancel the entire upgrade procedure. For a sample of the system response when you enter “shell”, see step 2. For a sample of the system response when you enter “fallback”, see step 3.

12 After the upgrade environment is prepared, any required CBM packages are applied.

Example 1

The following example shows a sample of the kind of display that occurs when any required CBM packages are applied:

```
======= Examine installed software (est. 15 sec) ... Completed.
======= UPGRADE required packages (est. 5 min) ...
  NT Software Inventory Manager   COMPLETELY INSTALLED
  SDM/CBM Debug Helper tools      REQUIRED - Applying - Completed.
  CBM version Info Files          REQUIRED - Applying - Completed.
  Platform Maintenance Common     REQUIRED - Applying - Completed.
  CBMMTCE Interface               REQUIRED - Applying - Completed.
  Platform Utilities              REQUIRED - Applying - Completed.
  Generic Data Delivery           REQUIRED - Applying - Completed.
  Log Delivery Service            REQUIRED - Applying - Completed.
  Table Access Service            REQUIRED - Applying - Completed.
  OM Access Service               REQUIRED - Applying - Completed.
  GNU Debugger                    COMPLETELY INSTALLED
```

Example 2

The following example shows a sample of the kind of display that occurs when a problem prevents a required CBM package from being applied. The display shows the dialog that would normally occur when a recovery procedure is performed.

```
======= Examine installed software (est. 15 sec) ... Completed.
======= UPGRADE required packages (est. 5 min) ...
  NT Software Inventory Manager   COMPLETELY INSTALLED
  SDM/CBM Debug Helper tools      REQUIRED - Applying - Completed.
  CBM version Info Files          REQUIRED - Applying - Completed.
  Platform Maintenance Common     REQUIRED - Applying - Failed


Please see the log file [log file path specified by the system] for more
information on the failure.

Please contact your next level of support to determine the next course of
action.
  - enter 'shell' to suspend the upgrade and enter a Maintenance Shell.
```

```
 - enter 'fallback' to cancel the entire UPGRADE procedure
choice (shell | fallback): shell
You have selected to enter a Maintenance Shell. Please contact next level of
support to determine the proper course of action.
Proceed with shell? (yes | no): yes
Once the action has been completed, enter 'exit' at the command line prompt
to return to the upgrade.
```

At this point, your next level of support is helping you to replace the faulty package.

```
cbm_upgrade_shell: exit
======Removing package Platform Maintenance Common (est. 10 sec) ...
Completed.
  Platform Maintenance Common     REQUIRED - Applying - Completed.
  CBMMTCE Interface               REQUIRED - Applying - Completed.
  Platform Utilities              REQUIRED - Applying - Completed.
  Generic Data Delivery           REQUIRED - Applying - Completed.
  Log Delivery Service            REQUIRED - Applying - Completed.
  Table Access Service            REQUIRED - Applying - Completed.
  OM Access Service               REQUIRED - Applying - Completed.
  GNU Debugger                    COMPLETELY INSTALLED
```

13 After the required CBM packages have been applied, the SWIM tool applies any upgrade software packages for applications installed on the system. If any of the software upgrade packages require configuration, the configuration is initiated by the system. You are prompted to press the Return key to start each of the individual configuration programs that run.

> ***Note:*** If any of the packages have a SWIM UPGRADE configuration script, you are notified by the system and prompted to start their execution.

Example

The following example shows a sample of the kind of display that occurs when upgrade packages for applications installed on the system are applied:

```
==== UPGRADE value added software using the CBM SWIM tool (est. NA) ...
The following new packages have been selected.
  NTswd21 'Bootpd and tftpd' 21.44.4.0
  NTscrt21 'SSH Core File Transfer' 21.44.4.0
  .
```

.
.
NTaft21 ‘SBA Automatic File Transfer’ 21.4..4.0

APPLYING Package NTpls21 Version 21.44.4.0
APPLIED Package NTpls21 Version 21.44.4.0
APPLYING Package NTace21 Version 21.44.4.0
APPLIED Package NTace21 Version 21.44.4.0
.
.
.
APPLIED Package NTaft21 Version 21.44.4.0

14 After any upgrade packages for applications installed on the system have been applied and after any required configurations have been performed, the upgrade program applies any patches that are present in the ISO image on the CBM CD.

Example

The following example shows a sample of the kind of display that would occur when patches are applied by the SIM patching tool:

======= Verify and Apply Patches using the SIM patching tool ...
############## Starting: COPYING FILES #############
This may take a moment depending on how many files there are.
############## Completed: COPYING FILES ##############
############## Starting: INTEGRITY CHECK ##############
Notification: Checking integrity of: NTBMI214404-01.
Success: Integrity confirmed for NTBMI214404.01.
############## Completed: INTEGRITY CHECK ##############
############## Starting: PREREQUISITE CHECK ##############
Determining if all requisites are installed or available.
Please note: This stage may take a few moments to complete.
############## Completed: PREREQUISITE CHECK ##############
########### Starting: APPLICATION PHASE (for active) ############
Applying NTBMI214404-01 ...
Success: NTBMI214404-01 applied successfully.
Please see the log file: /opt/nortel/sim/logs/PatchLog for additional details.
======= UPGRADE - CBM SIM patching tool end.

15 After the new patches have been applied, the upgrade program performs some additional tasks to complete the upgrade, including preserving logs, preparing data formatting, removing the old release from the upgrade environment, creating load baseline information, and checking the system for alarms. After the CBM upgrade is complete, control of the upgrade process is returned to the SSPFS upgrade.

Example

The following example shows a sample display that occurs at this point in the upgrade:

```
===== Preserve Logs (est. 5 sec) ... Completed.
===== Prepare Dataformatting (est. 5 sec) ... Completed.
===== Removing Old Release [20] From Upgrade Environment (est. NA) ...
The system displays the names of software packages as they are removed from the system.
===== Creating Load Baseline Information (est. 10 sec) ... Completed.
The upgrade procedure will now return control to the SSPFS portion of the upgrade. CBM Alarms will once again be examined for Major or Critical alarms.
======= Examine CBM Alarms (est. 1 min) ...
```

If any alarms exist, an alarm summary will be displayed and you will be prompted to enter ‘shell’ , ‘fallback’, or ‘continue’. For information about how to respond to any alarms that are discovered, see step 10.

16 When the CBM upgrade is complete, control will be returned to the SSPFS upgrade program.

> ***Note:*** At this time you should make sure that you have inserted the correct SSPFS upgrade CDROM disk into the CDROM drive. When you have entered “OK” in response to the system prompt, you will not have control over the system for approximately five minutes.

The SSPFS upgrade program resumes and activates the SOLARIS_9 upgraded environment. The inactive node of the cluster then reboots.

> ***Note:*** This reboot will take considerably longer than a regular system reboot.

At this point, the automatic portion of the upgrade is complete and manual steps must be performed to complete the upgrade process. Perform the following steps to ensure that the inactive node has been successfully rebooted:

a Enter the following command to determine whether the inactive node is in “ClusterIndicatorSTBY” (standby) state:

```
ubmstat
```

Re-run this command until the inactive node is shown to be in the standby state.

b Enter the following command to determine whether all filesystems are in “STANDBY normal UP clean” (standby) state:

```
udstat
```

Re-run this command until all filesystems are shown to be in the standby state.

c Enter the following command to determine whether SAM is running:

```
appctrl -p
```

In response the system should display “Command Complete”. Re-run this command until this response is displayed, indicating that SAM is running.

Use the following table to determine your next step.

If	Do
you wish to fall back at this point to cancel the upgrade procedure because something is unsatisfactory	Perform the procedure “Executing a fallback during an SSPFS-based server upgrade” in NN10408-900, *ATM/IP Fault Management* for more information.
you wish to complete the upgrade	Go on to section Completing the CBM 850 upgrade on page 476

Completing the CBM 850 upgrade

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)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
1	Ensure that no SBA alarms are currently raised.		Use procedure “SBA alarm troubleshooting” in NN10351-911, *Core and Billing Manager 850 Fault Management* to check for alarms.
2	Deliver any unprocessed billing files to the downstream destination. No more than one unprocessed billing file should remain on the system.		On the active node of the CBM 850 cluster, close any billing files that will be sent downstream by performing “Closing billing files” in NN10363-811, *Core and Billing Manager 850 Accounting*. Send the billing files downstream by performing procedure “Sending billing files from disk” in NN10363-811, *Core and Billing Manager 850 Accounting*. If you are unable to send billing files to a downstream destination, Nortel recommends that you back up the billing files to DVD, using the procedure “Copying billing files to DVD using SBADVDWRITE” in NN10363-811, *Core and Billing Manager 850 Accounting*.
3	If your system contains billing streams that meet all of the following qualifications, you must take the AFT and SBA applications offline: - use file format type DIRP - use stream record format BC - validate the SENSOR_TYPE, SENSOR_ID, RECORD_OFFICE_TYPE, RECORD_OFFICE_ID fields in the header and trailer records.		On the active node of the CBM 850 cluster, perform Procedure for taking the AFT and SBA applications offline on page 482

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
4	Complete the SSPFS platform and software upgrade procedure.		Complete the procedure Upgrading SSPFS software on page 666 starting with step 12.
5	Bring up the upgraded services on the newly-upgraded unit, making it the newly-active unit.		On the active node of the cluster, perform a swact by entering the following command: **`init 6`** When the swact completes, continue with step 6.
6	If you took the SBA and AFT offline in step 3 of this table, you must now return these applications to service.		To return the SBA and AFT to service, perform Procedure for returning SBA and AFT to service on page 484
7	Verify that the billing system is collecting billing records and verify the billing streams.		To verify that the billing system is collecting billing records and to verify the billing stream, perform Procedure for determining whether the billing system is collecting billing records and to verify a billing stream on page 486

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
8	Ensure that any SN08 CBM 850 patches have been applied.		1. Launch your web browser. 2. Search for www.nortelnetworks.com 3. Under the pulldown menu labeled “Support and Training”, select “software downloads”. 4. In the “Find Products” box at the right side of the screen, click “Families” 5. In the “Product Families” list that displays, click “DMS” 6. In the “DMS: General Availability” list that displays, click “Software” under the “Core and Billing Manager” entry. 7. At the top of the list of software entries that displays, click “Filter and Sort” 8. Make the appropriate selections (such as CBM00080) in the sort boxes and then click “GO” 9. Create a directory in the “root” directory (/) on the CBM 850 to hold the patches that you have selected: **mkdir /<directory name>** 10. Download the patches from the RPS ftp site to an intermediary location. Then, ftp the patches from this location to the directory on your CBM 850 that you created in step 9. 11. Apply the patches on the CBM 850 by first logging in to the CBM 850 as the root user and then entering the following command: **patchctrl -d <directory name>** where <directory name> is the full pathname of the directory containing the patches.

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
9	At this point, you must decide whether things look well with both the SSPFS and CBM upgrades. You can choose either to accept the new environment permanently, or you can choose to roll back to the state prior to the upgrade and lose all upgrade work.		If you have decided to fall back to the state prior to the upgrade, go to step 10 in this table. If you have decided to accept the new environment, go to step 11 in this table.

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
10	If you have decided to fall back to the state prior to the update, perform this step.		1. Log in to the inactive unit (the unit on which the “init 6” command was performed) and enter the following command: **`GetRunningClusterNodeNames`** Ensure that the system returns TWO nodes. If it doesn’t, wait for one minute and retry the command. If the system still doesn’t return TWO nodes, contact your next level of support before proceeding with this upgrade. 2. If your system contains billing streams that meet all of the following qualifications, you must take the AFT and SBA applications offline: - use file format type DIRP - use stream record format BC - validate the SENSOR_TYPE, SENSOR_ID, RECORD_OFFICE_TYPE, RECORD_OFFICE_ID fields in the header and trailer records. To take the SBA and AFT offline, perform the procedure, Procedure for taking the AFT and SBA applications offline on page 482.
	Note: Step 3 allows you to fall back to the state prior to the update. After a fallback, file systems gradually become fully-active on the newly-active unit. While file systems are becoming fully-active, you may see applications going into system-busy state. After the file systems have become fully-active, however, the applications will come into service automatically.		3. Perform the procedure Confirming the upgrade on an SSPFS-based server on page 764 and follow the steps to rollback to the state prior to the upgrade. Perform steps 1, 4, 6, and 8-9. Then return to this step in this table. 4. Return the SBA and AFT to service by performing the procedure, Procedure for returning SBA and AFT to service on page 484. After performing this step, you have completed the upgrade procedure.

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
11	If you have decided to accept permanently the new environment, perform this step.		Perform the procedure Confirming the upgrade on an SSPFS-based server on page 764 and follow the steps to accept the upgraded environment.
12	Edit the object properties in the IEMS for the CBM SSPFS platform you just upgraded to reflect the new software version.		Refer to either of the procedures that follow to update the software version in the Device Version field. - Editing and viewing object properties using Java Web Client on page 1841 -Editing and viewing object properties using Web Client on page 1846

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

Procedure for taking the AFT and SBA applications offline

At your workstation

1 From the command line, access the APPL level of the maintenance interface:

```
cbmmtc appl
```

If AFT application	Do
is installed on your system	step 2
is not installed on your system	step 5

2 Busy the AFT application:

```
bsy <application_number>
```

where

<application_number>
is the number next to the Automatic File Transfer application

3 Confirm the command:

```
y
```

4 Offline the AFT application:

```
offl <application_number>
```

where

<application_number>
is the number next to the Automatic File Transfer application

5 Busy the SuperNode Billing Application (SBA):

```
bsy <application_number>
```

where

<application_number>
is the number next to the SuperNode Billing Application

6 Confirm the command:

```
y
```

7 Take the SBA offline:

```
offl <application_number>
```

where

<application_number>
is the number next to the SuperNode Billing Application

8 You have completed this procedure. Return to the table (I)SN07 to (I)SN08 CBM 850 upgrade completion checklist on page 476

Procedure for returning SBA and AFT to service

At your workstation

1 Access the APPL level of the maintenance interface:

```
cbmmtc appl
```

2 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.

3 Busy the SBA:

```
bsy <application_number>
```

where

<application_number>
is the number next to the SuperNode Billing Application

4 Confirm the command:

```
y
```

5 Return the SBA to service:

```
rts <application_number>
```

where

<application_number>
is the number next to the SuperNode Billing Application

Note: Check to ensure that all billing streams are either in-service or in recovery on the core side before continuing.

If AFT application	Do
is installed on your system	step 6
is not installed on your system	step 8

6 Busy the AFT application:

```
bsy <application_number>
```

where

<application_number>
is the number next to the Automatic File Transfer application

7 Confirm the command:

```
y
```

8 Return the AFT application to service:

```
rts <application_number>
```

where

<application_number>
is the number next to the Automatic File Transfer application

9 Exit from SDMMTC:

```
quit all
```

10 Access the BILLMTC level:

```
billmtc
```

11 Access the APPL level:

```
appl
```

12 Access the AFT level:

```
aft
```

13 Restart the AFT session:

```
start <session_name>
```

Example response:

*** WARNING: Started AFT session: <session_name>

14 You have complete this procedure. Return to the table (I)SN07 to (I)SN08 CBM 850 upgrade completion checklist on page 476

Procedure for determining whether the billing system is collecting billing records and to verify a billing stream

At your workstation

1 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 2
did not increase from the first query command (meaning billing is not working)	contact your next level of support

2 You have completed this procedure. Return to the table (I)SN07 to (I)SN08 CBM 850 upgrade completion checklist on page 476

Integrated Element Management System (IEMS)

ATTENTION

All Media Server 2000 Series commissioned offices must also contain a commissioned IEMS network application in order to complete an upgrade to software release SN08 or greater.

An IEMS can be commissioned on a stand alone server or on the same SSPFS-based server as the CS 2000 Management Tools and Clients (CMT) application.

Offices that do not contain an IEMS prior to the upgrade must schedule to commission an IEMS during the upgrade.

ATTENTION

Upgrade the SSPFS software before upgrading any application software on the server.

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. If required, refer to procedure "Verifying disk utilization on an SSPFS-based server" in *ATM/IP Security and Administration*, NN10402-600.

Use this section to upgrade the IEMS on a standalone SSPFS-based server.

Note: If the IEMS resides on the same SSPFS-based server as the CS 2000 Management Tools, then use section CS 2000 Management Tools and Clients (CMT) on page 523).

Before upgrading Integrated Element Management Systems

Perform the required prerequisite upgrade as follows:

Network	IEMS applies to:	Previous Upgrade
ATM	UA-AAL1 and PT-AAL2	Depending on configuration: CS 2000 Core Manager on page 303 Core and Billing Manager (CBM) 850 on page 455 (only if upgrading from SN07)
IP	PT-IP, UA-IP. CHS, IAW and IAC[1]	Depending on configuration: CS 2000 Core Manager on page 303 Core and Billing Manager (CBM) 850 on page 455 (only if upgrading from SN07)
Tri-Modal	all applications	Depending on configuration: CS 2000 Core Manager on page 303 Core and Billing Manager (CBM) 850 on page 455

1.Includes IP International: CHS, IAC, PT-IP, and UA-IP

After upgrading Integrated Element Management System

Perform the next required upgrade as follows:

Network	IEMS supported in:	Next Upgrade
ATM	UA-AAL1 and PT-AAL2	CS 2000 Management Tools and Clients (CMT) on page 523
IP	PT-IP, UA-IP, CHS, IAW, and IAC[1]	CS 2000 Management Tools and Clients (CMT) on page 523
Tri-Modal	all applications	CS 2000 Management Tools and Clients (CMT) on page 523

1.Includes IP International: CHS, IAC, PT-IP, and UA-IP

About the Integrated Element Management System

Integrated Element Manager System (IEMS) interface manages the output used by external OSS systems to monitor network element and alarm conditions. The IEMS uses a Graphical User Interface (GUI), that interacts with the manager GUIs, which provides access to network element alarms and logs. In a stand alone configuration, the IEMS server includes the following software packages:

- Succession Server Platform Foundation (SSPFS)
- Integrated Element Manager System (IEMS)
- Network Patch Manager (NPM)
- Patching Server Element (PSE)

Upgrading the Integrated EMS

Upgrading the Integrated EMS involves upgrading the Succession Server Platform Foundation Software (SSPFS) and the Integrated EMS software. Use this procedure to upgrade the Integrated EMS on an SSPFS-based server in a simplex or HA configuration.

Note: If the upgrade of Integrated EMS to the newly installed version of software fails before the upgrade is completed, all the changes done for migrating the data of Integrated EMS revert to the original state.

Prerequisites

This procedure has the following prerequisites:

- Ensure all console and telnet sessions used during the upgrade are recorded to a file.
- Ensure all users are logged out of the server prior to the upgrade.

Upgrade checklists

Follow the link associated with your configuration.

- Simplex server on page 490
- HA server pair on page 494

Simplex server

Use the table that follows as a checklist to upgrade a simplex server. Place a check (√) in the √column as you complete each procedure.

Upgrade checklist for a simplex server

	Activities	√	Procedures
1	Check the hardware requirements.		Refer to "Hardware requirements" in *Integrated EMS Basics*, NN10329-111
2	Verify whether an HTTPS certificate is installed on the server, and whether it is valid.		Perform procedure Verifying the presence and validity of an HTTPS certificate on an SSPFS-based server on page 545.
3	Ensure the (I)SN07 Integrated EMS is installed with all patches.		Refer to Ensuring (I)SN07 Integrated EMS is installed.

Upgrade checklist for a simplex server

	Activities	√	Procedures
4	Perform a full system backup. It is recommended that you take a backup image for restore in case the upgrade fails.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.
			Perform procedure Saving user-defined NPM data using the NPM on page 576.
			Perform procedure Saving the NPM patch files on page 589.
5	Ensure the devices supported by Integrated EMS are upgraded to (I)SN07.		Refer to the Upgrade document for the device.
6	Determine if a third-party security application is used.		Refer to Determining if a third-party security application is used on page 558.
7	Ensure the user names in (I)SN07 are compliant to (I)SN08 restrictions.		All user names in (I)SN07 must be compliant to the (I)SN08 restrictions. Refer to "Adding New Users" of (I)SN08 *Integrated EMS Security and Administration*, NN10336-611. If the user names are not compliant to these rules they may be deleted without notice during upgrade.
8	Validate the order of upgrade.		Refer to Component upgrade order on page 9.
9	Ensure the domain name service (DNS) is enabled on the server.		Refer to procedure "Configuring Domain Name Service" in *ATM/IP Solution-level Configuration Management*, NN10409-500.
10	Upgrade the Succession Server Platform Foundation Software (SSPFS).		Perform procedure Upgrading SSPFS software.

Upgrade checklist for a simplex server

	Activities	√	Procedures
11	Install any SSPFS MNCLs. ***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.
12	Obtain any patches applicable to components on the Integrated EMS server (PSE, NPM, SSPFS, IEMS, IEMSCSS, COREM).		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
13	Apply all SSPFS patches.		Perform procedure Applying patches using the NPM on page 1895.
14	Apply all NPM patches and restart NPM.		Perform procedure Applying patches using the NPM on page 1895.
15	If you have a large office, abort any NPM tasks that are queued ahead of the NPM restart task. ***Note:*** In a large office, the list of NPM tasks queued ahead of the NPM restart task, can be long and can take many hours to complete. Therefore, aborting NPM tasks is recommended in large offices to shorten the upgrade time.		Perform procedure Prioritizing a patching maintenance request using the NPM on page 2000.
16	Apply all PSE patches and restart PSE.		Perform procedure Applying patches using the NPM on page 1895.

Upgrade checklist for a simplex server

	Activities	√	Procedures
17	Upgrade the Integrated EMS software on this server.		If you are upgrading through Electronic Software Delivery (ESD), transfer the Integrated EMS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading Integrated EMS software in a simplex configuration on page 496

HA server pair

Use the table that follows as a checklist to upgrade an HA server pair. Place a check (√) in the √column as you complete each procedure.

Upgrade checklist for an HA server pair

	Activities	√	Procedures
On the ACTIVE server			
1	Check the hardware requirements.		Refer to "Hardware requirements" in *Integrated EMS Basics*, NN10329-111
2	Verify whether an HTTPS certificate is installed on the server, and whether it is valid.		Perform procedure Verifying the presence and validity of an HTTPS certificate on an SSPFS-based server on page 545.
3	Ensure the (I)SN07 Integrated EMS is installed with all patches.		Refer to Ensuring (I)SN07 Integrated EMS is installed.
4	Perform a full system backup. It is recommended that you take a backup image for restore in case the upgrade fails.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.
			Perform procedure Saving user-defined NPM data using the NPM on page 576.
			Perform procedure Saving the NPM patch files on page 589.
5	Ensure the devices supported by Integrated EMS are upgraded to (I)SN07.		Refer to the Upgrade document for the device.
6	Determine if a third-party security application is used.		Refer to Determining if a third-party security application is used on page 558.

Upgrade checklist for an HA server pair

	Activities	√	Procedures
7	Ensure the user names in (I)SN07 are compliant to (I)SN08 restrictions.		All user names in (I)SN07 must be compliant to the (I)SN08 restrictions. Refer to "Adding New Users" of (I)SN08 *Integrated EMS Security and Administration*, NN10336-611. If the user names are not compliant to these rules they may be deleted without notice during upgrade.
8	Validate the order of upgrade.		Refer to Component upgrade order on page 9.
9	Ensure the domain name service (DNS) is enabled on the server .		Refer to procedure "Configuring Domain Name Service" in *ATM/IP Solution-level Configuration Management*, NN10409-500.
On the INACTIVE server			
10	Verify the state of the cluster.		Perform procedure Verifying the state of a cluster on page 629.
11	Upgrade the Succession Server Platform Foundation Software (SSPFS).		Perform procedure Upgrading SSPFS software.
12	Install any SSPFS MNCLs. ***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.
On the ACTIVE server			
13	Obtain any patches applicable to components on the Integrated EMS server (PSE, NPM, SSPFS, IEMS, IEMSCSS, COREM).		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889

Upgrade checklist for an HA server pair

	Activities	√	Procedures
On the INACTIVE server			
14	Apply all SSPFS patches.		Perform procedure Patching the inactive node of a cluster during an upgrade on page 737.
15	Apply all NPM patches.		Perform procedure Patching the inactive node of a cluster during an upgrade on page 737.
16	Apply all PSE patches.		Perform procedure Patching the inactive node of a cluster during an upgrade on page 737.
17	Upgrade the Integrated EMS software on this server.		If you are upgrading through Electronic Software Delivery (ESD), transfer the Integrated EMS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading Integrated EMS software in an HA configuration on page 505

Ensuring (I)SN07 Integrated EMS is installed

The Integrated EMS (I)SN07 Maintenance Release software or Integrated EMS (I)SN07 software with complete patch must be installed in the system or set must be installed. If you want to install Integrated EMS patches, refer to Carrier Voice over IP Network patching.

Upgrading Integrated EMS software in a simplex configuration

Use the following procedure to upgrade Integrated EMS software in a simplex configuration.

Upgrading Integrated EMS software in a simplex configuration

At the Integrated EMS Server system

1 Obtain the password for user nortel prior to the upgrade, as the password will be changed during the upgrade, and you will need to reset it following the upgrade.

2 Log in at the console port as the root user at the server where the Integrated EMS Server needs to be upgraded.

3 Verify the status of the Integrated EMS server by typing

```
# servquery -status all
```

The output shows the services running on the unit.

```
APP NAME                    STATUS
=========                   ======

CINOTIFIER                  RUNNING
DATABASE                    RUNNING
IS                          RUNNING
BOOTP                       RUNNING
WEBSERVER                   RUNNING
CORBA                       RUNNING
OMPUSH                      RUNNING
WEBSERVICES                 RUNNING
ORA_AUTO_BACKUP             RUNNING
DELEGATE                    RUNNING
ORA_ARCHIVE_ROTATOR         RUNNING
PROP_SRV                    RUNNING
IEMS                        RUNNING
SNMP_POLLER               RUNNING
RADSVR                      RUNNING
```

4 Use the following table to determine your next step.

If you are upgrading from	Do
a CD	step 5
electronic software delivery (ESD)	step 7

At the server

5 Insert the CD that contains the Integrated EMS software into the drive.

At the server console

6 Upgrade the IEMS software using a CD as follows:

a Access the upgrade script by typing

```
# cd /cdrom/cdrom0/bin/
```

and pressing the Enter key.

b Run the upgrade script by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

The screen output lists the currently installed packages and confirms the upgrade.

The screen output then lists the contents of the IEMS software package to be installed, similar to the following screen shot:

```
NNaxl          VERSION:  3.25,v1
NNedu          VERSION:  1.3.2,v1
NNjre          VERSION:  1.4.2_04,v1
NNlog4cpp             VERSION:  0.3.4b,v1
NNlog4j        VERSION:  1.2.8,v1
NNnds          VERSION:  5.1_SP2_HF2,v1
NNnsssaml             VERSION:  1.1.0,mip0400ac38
NNoro          VERSION:  2.0.7,v1
NNrad          VERSION:  1.1.0,mip0400ac38
NNrogwave             VERSION:  sourcePro_6.0,v1
NNs1isext             VERSION:  1.1.0,mip0400ac38
NNs1is         VERSION:  6.0_SP1,v1
NNseccore             VERSION:  1.1.0,mip0400ac38
NNsecui        VERSION:  1.1.0,mip0400ac38
NNsisclt              VERSION:  1.1.0,mip0400ac38
NNswmgmt              VERSION:  MIP4.0.0,mip0400ac38
NNxercesc             VERSION:  2.3.0,v1
IEMS             IEMS_8_45_0
NNCEMS180        18.0.165.0
```

c Proceed to step 8.

7 Upgrade the IEMS software using ESD as follows:

a Access the upgrade script by typing

```
# cd /tmpmnt/bin/
```

and pressing the Enter key.

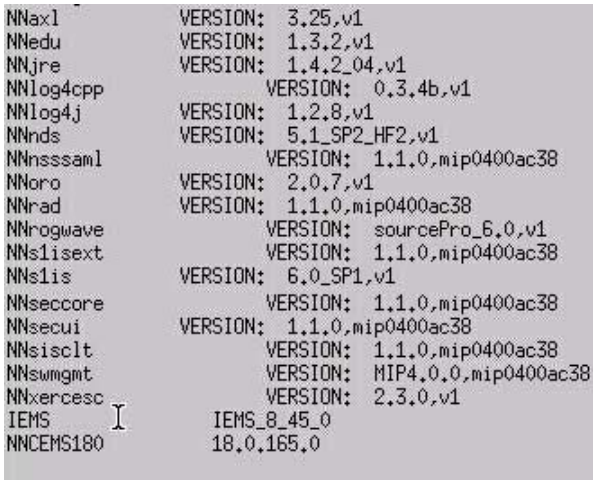
b Run the upgrade script by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

The screen output lists the currently installed packages and confirms the upgrade.

The screen output then lists the contents of the IEMS software package to be installed, similar to the following screen shot:



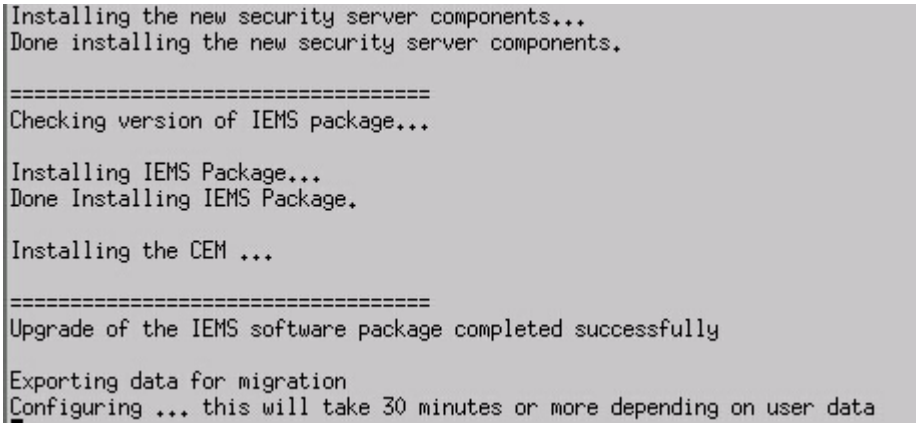
8 When prompted, confirm you want to upgrade by typing

`y`

and pressing the Enter key.

A message appears, similar to the following screen shot:

Note: The upgrade can take 30 minutes or more depending on the user data. If one or more error or failure messages are generated during the software upgrade, contact your next level of support.



9 Ensure you are at the root directory level by typing

`# cd /`

and pressing the Enter key.

10 Reset the password for user nortel by typing

```
# passwd -r files nortel
```

and pressing the Enter key.

11 When prompted, enter the password for user nortel that you obtained prior to the upgrade.

12 When prompted, enter the password again to confirm it.

13 Use the following table to determine your next step.

If you upgraded from a	Do
CD	step 14
directory	step 16

14 Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

 # /etc/init.d/volmgt stop

 # /etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

15 Remove the CD or DVD from the drive.

16 Apply all IEMS, IEMSCSS, COREM patches using procedure Patching procedures checklist for the IEMS, COREM, and IEMS security components on page 1856.

17 Ensure the IEMS is running by typing

```
# servquery -status -group IEMS
```

and pressing the Enter key.

18 Use the following table to determine your next step.

If you upgraded from a	Do
CD	step 19
directory	step 20

19 If you upgraded from a CD, run the Config File Swap script as follows:

a Insert the CD that contains the IEMS software into the drive.

b Run the script by typing

```
# /cdrom/cdrom0/bin/switch08conf.ksh
```

and pressing the Enter key.

c When prompted, confirm you want to continue by typing

```
y
```

and pressing the Enter key.

d Proceed to step step 21.

20 If you upgraded from a directory, run the Config File Swap script as follows:

a Run the script by typing

```
# /tmpmnt/bin/switch08conf.ksh
```

and pressing the Enter key.

b When prompted, confirm you want to continue by typing

```
y
```

and pressing the Enter key.

21 Use the following table to determine your next step.

If	Do
the Media Server 2000 is in the network	step 22
otherwise	step 25

22 Determine if the bootptab file is present on the server by typing

```
# ls -l /data/sspfs/etc/bootp/bootptab
```

and pressing the Enter key.

23 Use the following table to determine your next step.

If the bootptab is	Do
not present	step 24
present	step 25

24 Set up the BootP file using procedure Setting up the BootP file on SSPFS on page 516.

25 If you determined at the beginning of the upgrade that the server was using a third-party security application, the special edits that were in the NSCD, PAM and NSSwitch configuration files (nscd.conf, pam.conf and nsswitch.conf), need to be put back since during the IEMS software upgrade, the configuration files were replaced with new configuration files that use the IEMS security application.

Contact your system administrator.

26 If you upgraded from SN07, run the Integrated EMS cleanup script using the following commands:

cd /opt/nortel/iems/current/bin

and pressing the Enter key.

./CleanUpSN07Data.sh

and pressing the Enter key.

27 Use the following table to determine your next step.

If you upgraded from a	Do
CD	step 28
directory	step 29

28 If you ugraded from a CD, eject the CD from the drive as follows:

a Ensure you are at the root directory level by typing

cd /

and pressing the Enter key.

b Eject the CD by typing

eject cdrom

and pressing the Enter key.

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

/etc/init.d/volmgt stop

/etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

d Proceed to step 30.

29 If you upgraded from a directory, unmount and remove the ISO image file from the server using procedure Unmounting and removing an ISO image from an SSPFS-based server.

30 Update the CEM documentation.

If you are upgrading from	Do
a CD	step 31
electronic software delivery (ESD)	step 34

31 Insert the CD that contains the CEM documentation into the drive.

32 Upgrade the CEM documentation by typing

```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.

33 Eject the CD from the drive as follows:

a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

 # /etc/init.d/volmgt stop

 # /etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

d Proceed to step 36.

34 Mount the CEM help file. See Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server.

35 Upgrade the CEM documentation by typing

```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.

Note: To configure CEM, see Integration of Core Element Manager with Integrated EMS in *Integrated EMS Basics*, NN10329-111.

36 Start the Integrated EMS Server by entering the following command:

```
# servstart IEMS
```

and pressing the Enter key.

37 After 3 minutes, issue the following command and check that Integrated EMS Server has started.

```
# servquery -status -group IEMS
```

and pressing the Enter key.

If the Integrated Server has started, the following message is displayed to indicate that the upgrade was successful and Integrated EMS is in service:

```
IEMS Instance is UP
```

After installing the (I)SN08 version of Integrated EMS, the migration is done when the Integrated EMS Server is started for the first time. The order of migration is mentioned in Integrated EMS data migration order section. If the migration fails, all the changes done for migrating the data of Integrated EMS alone revert to the original state.

If the migration fails, you can check for error messages the file IEMSDataMigration.log located under /home/opt/nortel/iems/current/logs.

38 Start the Core Element Manager (CEM). Refer to procedure Starting and stopping the Core Element Manager (CEM) on page 817.

39 Accept the upgraded environment by typing

```
# /SSPFS_Upgrade.accept
```

and pressing the Enter key.

The execution of this step takes approximately 20 minutes to complete depending on system configuration.

40 Proceed to Completing the Integrated EMS upgrade on page 515.

Upgrading Integrated EMS software in an HA configuration

Use the following procedure to upgrade Integrated EMS software in a an HA configuration.

Upgrading Integrated EMS software in an HA configuration

At the Integrated EMS Server system

1 Obtain the password for user nortel prior to the upgrade, as the password will be changed during the upgrade, and you will need to reset it following the upgrade.

2 Determine which unit in the cluster is in standby mode so it can be upgraded. Log into either of the units from the console port as the root user and type the following command:

```
# ubmstat
```

and pressing the Enter key.

The state of the ClusterIndicator is either active (ACT) or standby (STBY).

If the unit you have logged into is active, log out and log in to the other unit. Upgrade the unit in STBY mode first.

```
Group State
---------------
ClusterIndicator STBY
```

3 Determine whether any applications are running on the STBY unit by typing

```
# servquery -status all
```

The output shows the services running on the unit.

```
APP NAME                          STATUS
=========                         ======

CINOTIFIER                        NOT RUNNING
DATABASE                          NOT RUNNING
IS                                NOT RUNNING
BOOTP                             NOT RUNNING
WEBSERVER                         NOT RUNNING
CORBA                             NOT RUNNING
OMPUSH                            NOT RUNNING
WEBSERVICES                       NOT RUNNING
ORA_AUTO_BACKUP                   NOT RUNNING
DELEGATE                          NOT RUNNING
ORA_ARCHIVE_ROTATOR               NOT RUNNING
NPM                               NOT RUNNING
PROP_SRV                          NOT RUNNING
```

```
IEMS                                    NOT RUNNING
SNMP_POLLER                             NOT RUNNING
RADSVR                                  NOT RUNNING
```

4 If any of the applications are running, stop the application by typing

```
# servstop <application>
```

and pressing the Enter key.

where

application
is the name of the application, for example IEMS

5 Remove the inactive unit from the cluster using procedure Removing a server from a cluster.

6 Use the following table to determine your next step.

If you are upgrading from a	Do
CD	step 7
directory	step 9

At the server

7 Insert the CD that contains the Integrated EMS software into the drive of the inactive server.

At the server console

8 Upgrade the IEMS software using a CD as follows:

a Access the upgrade script by typing

```
# cd /cdrom/cdrom0/bin/
```

and pressing the Enter key.

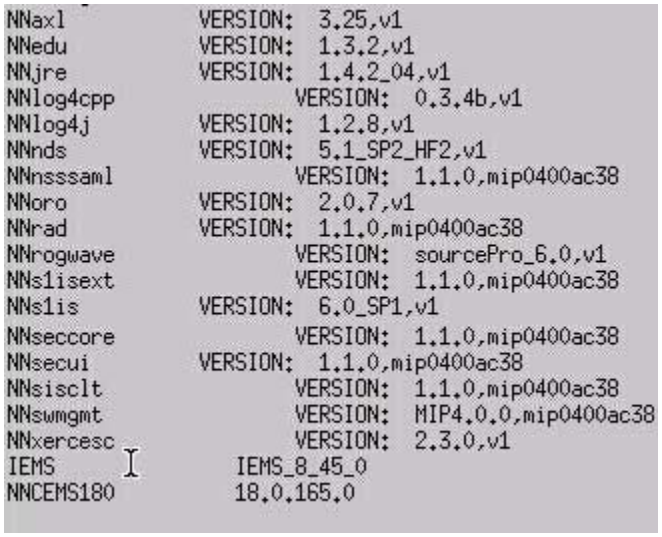
b Run the upgrade script by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

The screen output lists the currently installed packages and confirms the upgrade.

The screen output then lists the contents of the IEMS software package to be installed, similar to the following screen shot:



c Proceed to step 10.

9 Upgrade the IEMS software using ESD as follows:

a Access the upgrade script by typing

```
# cd /tmpmnt/bin/
```

and pressing the Enter key.

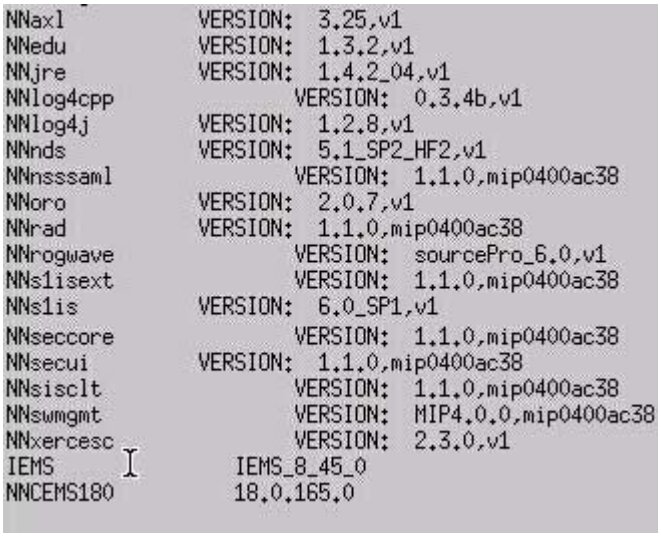
b Run the upgrade script by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

The screen output lists the currently installed packages and confirms the upgrade.

The screen output then lists the contents of the IEMS software package to be installed, similar to the following screen shot:



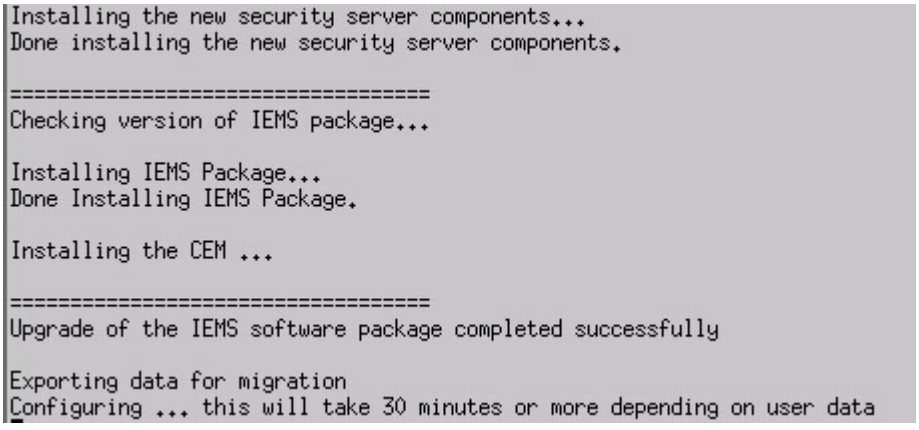
10 When prompted, confirm you want to upgrade by typing

y

and pressing the Enter key.

A message appears, similar to the following screen shot:

Note: The upgrade can take 30 minutes or more depending on the user data. If one or more error or failure messages are generated during the software upgrade, contact your next level of support.



11 Ensure you are at the root directory level by typing

cd /

and pressing the Enter key.

12 Reset the password for user nortel by typing

```
# passwd -r files nortel
```

and pressing the Enter key.

13 When prompted, enter the password for user nortel that you obtained prior to the upgrade.

14 When prompted, enter the password again to confirm it.

15 Use the following table to determine your next step.

If you upgraded from a	Do
CD	step 16
directory	step 18

16 Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

 # /etc/init.d/volmgt stop

 # /etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

17 Remove the CD or DVD from the drive.

18 Apply all IEMS, IEMSCSS, COREM patches using procedure Patching the inactive node of a cluster during an upgrade on page 737.

19 Return the inactive unit to the cluster using procedure Returning a server to a cluster.

20 Verify the state of cluster. Refer to Verifying the state of a cluster on page 629.

If any error messages are returned, you must contact your next level of support.

21 Stop the cluster using procedure Stopping a cluster .

22 Use the following table to determine your next step.

If you upgraded from a	Do
CD	step 23
directory	step 24

23 If you upgraded from a CD, run the Config File Swap script as follows:

a Insert the CD that contains the IEMS software into the drive.

b Run the script by typing

```
# /cdrom/cdrom0/bin/switch08conf.ksh
```

and pressing the Enter key.

c When prompted, confirm you want to continue by typing

```
y
```

and pressing the Enter key.

d Proceed to step 25.

24 If you upgraded from a directory, run the Config File Swap script as follows:

a Run the script by typing

```
# /tmpmnt/bin/switch08conf.ksh
```

and pressing the Enter key.

b When prompted, confirm you want to continue by typing

```
y
```

and pressing the Enter key.

25 Use the following table to determine your next step.

If	Do
the Media Server 2000 is in the network	step 26
otherwise	step 29

26 Determine if the bootptab file is present on the server by typing

```
# ls -l /data/sspfs/etc/bootp/bootptab
```

and pressing the Enter key.

27 Use the following table to determine your next step.

If the bootptab file is	Do
not present	step 28
present	step 29

28 Set up the BootP file using procedure Setting up the BootP file on SSPFS on page 516.

29 If you determined at the beginning of the upgrade that the server was using a third-party security application, the special edits that were in the NSCD, PAM and NSSwitch configuration files (nscd.conf, pam.conf and nsswitch.conf), need to be put back since during the IEMS software upgrade, the configuration files were replaced with new configuration files that use the IEMS security application. This needs to be done on the active and inactive unit.

Contact your system administrator.

30 If you upgraded from SN07, run the Integrated EMS cleanup script on the active unit using the following commands:

```
cd /opt/nortel/iems/current/bin
```

and pressing the Enter key.

```
./CleanUpSN07Data.sh
```

and pressing the Enter key.

31 Remove the CD or ISO images associated with the (I)SN08 load installation. Select your next step:

If	Do
you are using a CD	step 32
you are using an ISO image	step 33

32 Eject the CD from the drive as follows:

a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the CD by typing

eject cdrom

and pressing the Enter key.

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

/etc/init.d/volmgt stop

/etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

d Proceed to step 34.

33 If you upgraded from ESD, unmount and remove the ISO image file from the server using procedure Unmounting and removing an ISO image from an SSPFS-based server.

34 Update the CEM documentation.

If you are upgrading from	Do
a CD	step 35
electronic software delivery (ESD)	step 38

35 Insert the CD that contains the CEM documentation into the drive.

36 Upgrade the CEM documentation by typing

 # pkgadd -d SScemhelp.pds

and pressing the Enter key.

37 Eject the CD from the drive as follows:

a Ensure you are at the root directory level by typing

cd /

and pressing the Enter key.

b Eject the CD by typing

eject cdrom

and pressing the Enter key.

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

/etc/init.d/volmgt stop

/etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

d Proceed to step 41.

38 Mount the CEM help file. See Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server.

39 Upgrade the CEM documentation by typing

 # pkgadd -d SScemhelp.pds

and pressing the Enter key.

Note: To configure CEM, see Integration of Core Element Manager with Integrated EMS in *Integrated EMS Basics*, NN10329-111.

40 Accept the upgraded environment by typing

```
# /SSPFS_Upgrade.accept
```

and pressing the Enter key.

The execution of this step takes approximately 20 minutes to complete depending on system configuration.

41 Clone the inactive node to the active node so both nodes have same image. Refer to procedure Cloning the image of one node in a cluster to the other node on page 766 .

Note: Ensure no provisioning activities are in progress, or are scheduled to take place during this step. This includes Integrated EMS Security administration actions that involve changes to the security database.

Example
Adding or changing user account information and adding or changing group information.

After installing the (I)SN08 version of Integrated EMS, the migration is done when the Integrated EMS Server is started for the first time in the upgraded (I)SN08 unit becomes active. The order of migration is mentioned in Integrated EMS data migration order section. If the migration fails, all the changes done for migrating the data of Integrated EMS alone revert to the original state as specified in the note on page 490.

If the migration fails, you can check for error messages the file IEMSDataMigration.log located under /home/opt/nortel/iems/current/logs.

42 Proceed to Completing the Integrated EMS upgrade on page 515.

Integrated EMS data migration order

Integrated EMS data migration occurs in the following order:

- Security data migration
- Integrated EMS data migration
  - — Database schema migration
  - — Data migration
  - — Configuration migration

Completing the Integrated EMS upgrade

The following table contains a summary of required post-upgrade procedures that has to be followed after upgrading to (I)SN08 Integrated EMS.

Required post-upgrade procedures

Requirement	Procedure
1. Clear the Java Web Start Client cache on client workstation.	Clear the Java Web Start Client cache to properly launch the Integrated EMS Client. To clear the Java Web Start Client cache, refer to “Clearing the JWS cache on a client workstation" in the *ATM/IP Solution-level Configuration Management* document, NN10409-500.
2. Check whether the user group and user list are imported correctly.	Verify that the user group and user lists have been imported correctly in the Integrated EMS Security and Administration GUI. Refer to "Listing all groups and users" of *Integrated EMS Security and Administration guide*, NN10336-611.
3. Edit the object properties in the Integrated EMS for the IEMS SSPFS platform that you just upgraded to reflect the new software version.	Refer to either of the procedures that follow to update the software version in the Device Version field: • Editing and viewing object properties using Java Web Client on page 1841 • Editing and viewing object properties using Web Client on page 1846

Setting up the BootP file on SSPFS

Application

Use this procedure to set up the Succession Server Platform Foundation Software (SSPFS-based server as the bootp master and migrate the bootp entries from the core manager to the SSPFS-based server.

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 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.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the SSPFS-based server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the SSPFS-based server on which you want to set up the bootp file

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the 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 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 -
```

b 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)
 2 - sdm_unconf (Unconfigure SDM IP Address)
 3 - sdmuser_conf (Configure SDM User)
 4 - sdmuser_unconf (Unconfigure SDM User)
 5 - cmClli_rediscovery (Re-discover the CM
     CLLI by SDM IP)
 6 - cmClli_conf (Configure CM_CLLI Address)
 7 - cmClli_unconf (Unconfigure CM_CLLI IP
     Address)
 8 - cm_conf (Configure CM IP Address)
 9 - cm_unconf (Unconfigure CM IP Address)

 X - exit

select -
```

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

Example response

```
===Executing “sdm_conf”

Enter the ip address of the SDM []
```

d When prompted, enter the IP address of the core manager (SDM).

Example response

```
Retrieving CM CLLI. Please wait...

SDM IP: 47.152.34.56
CM CLLI: OFFICE3

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 Generate the ssh key pair needed for data transmission between the SSPFS-based server and the core manager by typing

```
# keygen.sh sam21em
```

and pressing the Enter key.

Note: The keygen.sh sam21em script is used to generate the ssh key pair on any SSFPS-based server and is not specific to sam21em.

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, access to the needed directories and files on the core manager will be provided.

You have completed this procedure.

CS 2000 Management Tools and Clients (CMT)

ATTENTION

All Media Server 2000 Series commissioned offices must also contain a commissioned Integrated Element Management System (IEMS) network application in order to complete an upgrade to software release SN08 or greater.

An IEMS can be commissioned on a stand alone server or on the same SSPFS-based server as the CS 2000 Management Tools and Clients (CMT) application.

Offices that do not contain an IEMS prior to the upgrade must schedule to commission an IEMS during the upgrade.

ATTENTION

Upgrade the SSPFS software before upgrading any application software on the server.

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. If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.

For IEMS co-resident configurations, upgrade an existing IEMS application or commission a new IEMS application during the CMT upgrade.

If the IEMS resides on a separate SSPFS-based server, refer to Integrated Element Management System (IEMS) on page 487.

Before upgrading CS 2000 Management Tools and Clients

Perform the required prerequisite upgrade as follows:

Network	CMT applies to:	Previous Upgrade
ATM	UA-AAL1 and PT-AAL2	Integrated Element Management System (IEMS) on page 487
IP	PT-IP, UA-IP, IAW, CHS, and IAC[1]	Integrated Element Management System (IEMS) on page 487
Tri-Modal	all applications	Integrated Element Management System (IEMS) on page 487

1.Includes IP International: PT-IP, IAC, CHS, and UA-IP

After upgrading CS 2000 Management Tools and Clients

Perform the next required upgrade as follows:

Network	CMT applies to:	Next Upgrade
ATM	UA-AAL1 and PT-AAL2	Multiservice Switch (MSS) 15000/20000 on page 820
IP	UA-IP and PT-IP[1]	Multiservice Switch (MSS) 15000/20000 on page 820
	IAC - North America	Peripheral Modules on page 1065
	IAC - International, IAW and CHS[2]	SAM21 Shelf Controller on page 1280
Tri-Modal	all applications	Multiservice Switch (MSS) 15000/20000 on page 820

1.Includes IP International: UA-IP and PT-IP
2.Includes IP International: CHS

About CS 2000 Management Tools and Clients

CS 2000 Management Tools is a collection of software packages that contain a set of tools used to manage elements and sub-elements in a Succession network. This set of tools can run on a single server, multiple servers, or be split to run on different servers. Deployment depends on the size of the network being managed and operational needs and preferences. Depending on the configuration, CS 2000 Management Tools can consist of the following software packages:

- Succession Server Platform Foundation (SSPFS)
- Network Patch Manager (NPM)
- Patching Server Element (PSE)
- Integrated Element Manager System (IEMS)
- CS 2000 Management Tools (CS2M)
- Audio Provisioning Server (APS)

Upgrading the CS 2000 Management Tools

Upgrading the CS 2000 Management Tools on an SSPFS-based server, consists of the following tasks:

- Preparing to upgrade the CS 2000 Management Tools software on page 527
- Upgrading the CS 2000 Management Tools software on page 633
- Completing the CS 2000 Management Tools upgrade on page 782

In the event you need or want to downgrade the CS 2000 Management Tools, refer to procedure “Downgrading the CS 2000 Management Tools software” in *ATM/IP Fault Management*, NN10408-900.

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. If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in the ATM/IP Security and Administration document, NN10402-600.

The supported upgrade paths to the (I)SN08 release are listed below. Follow the link associated with the release you are upgrading from.

- Preparing to upgrade from (I)SN06.2 to (I)SN08 on page 527
- Preparing to upgrade from (I)SN07 to (I)SN08 on page 535

Preparing to upgrade from (I)SN06.2 to (I)SN08

The configurations that support an upgrade from (I)SN06.2 to (I)SN08 are listed below. Follow the link associated with your configuration.

- Sun Netra t1400 on page 527
- Sun Netra 240 one-server configuration on page 530
- Sun Netra 240 two-server configuration on page 532

ATTENTION
The SSPFS and all applications on the server 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

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)SN08 (Sun Netra t1400) Preparation checklist

	Activities	√	Procedures
1	Verify whether an HTTPS certificate is installed on the server, and whether it is valid.		Perform procedure Verifying the presence and validity of an HTTPS certificate on an SSPFS-based server on page 545.
2	Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade.		Refer to procedure Verifying group IDs and user IDs on an SSPFS-based server on page 563.
3	Prior to the upgrade, determine if the system has the necessary 9 GB unallocated disk space execute the following command as the root user: /opt/nortel/sspfs/fs/meta.pl fs The displayed value must be larger then "19000000" (19,000,000) for the upgrade to succeed. Note: If it is determined that there is not enough unallocated disk space to perform the upgrade, contact Nortel Technical Support.		If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in the *ATM/IP Security and Administration document*, NN10402-600.
4	Perform an audit with the CS 2000 Management Tools.		Refer to Performing an audit on page 596.
5	Perform a full system backup.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.
			Perform procedure Performing a backup of APS audio files to tape on page 619. ***Note:*** Only perform this procedure if the APS is present on the server.

(I)SN06.2 to (I)SN08 (Sun Netra t1400) Preparation checklist

	Activities	√	Procedures
			Perform procedure Performing a backup of APS oracle data to tape on page 624. ***Note:*** Only perform this procedure if the APS is present on the server.
			Perform procedure Saving user-defined NPM data using the NPM on page 576. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
			Perform procedure Saving the NPM patch files on page 589. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
6	Proceed to upgrade the CS 2000 Management Tools software.		Refer to Upgrading the CS 2000 Management Tools software on page 633.

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)SN08 (Sun Netra 240 one-server) Preparation checklist

	Activities	√	Procedures
1	Verify whether an HTTPS certificate is installed on the server, and whether it is valid.		Perform procedure Verifying the presence and validity of an HTTPS certificate on an SSPFS-based server on page 545.
2	Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade.		Refer to procedure Verifying group IDs and user IDs on an SSPFS-based server on page 563.
3	Prior to the upgrade, determine if the system has the necessary 9 GB unallocated disk space execute the following command as the root user: /opt/nortel/sspfs/fs/meta.pl fs The displayed value must be larger then "19000000" (19,000,000) for the upgrade to succeed. Note: If it is determined that there is not enough unallocated disk space to perform the upgrade, contact Nortel Technical Support.		If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in the *ATM/IP Security and Administration document*, NN10402-600.
4	Perform an audit with the CS 2000 Management Tools.		Refer to Performing an audit on page 596.
5	Perform a full system backup.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.

(I)SN06.2 to (I)SN08 (Sun Netra 240 one-server) Preparation checklist

Activities	√	Procedures
		Perform procedure Performing a backup of APS audio files to CD or DVD on page 621. ***Note:*** Only perform this procedure if the APS is present on the server.
		Perform procedure Performing a backup of APS oracle data to CD or DVD on page 626. ***Note:*** Only perform this procedure if the APS is present on the server.
		Perform procedure Saving user-defined NPM data using the NPM on page 576. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
		Perform procedure Saving the NPM patch files on page 589. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
6 Proceed to upgrade the CS 2000 Management Tools software.		Refer to Upgrading the CS 2000 Management Tools software on page 633.

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)SN08 (Sun Netra 240 two-server) Preparation checklist

	Activities	√	Procedures
On the INACTIVE node			
1	Verify the state of the cluster.		Perform procedure Verifying the state of a cluster on page 629.
2	Determine through your system administrator whether QCA properties were modified on the Active server at any given time. If they were modified, ensure the Inactive server reflects those modifications. ***Note:*** The properties on the Inactive server will override the properties on the Active server during the upgrade.		Perform procedure “Modifying the QoS Collector Application” in the ATM/IP Configuration Management document, NN10409-500 if required.

(I)SN06.2 to (I)SN08 (Sun Netra 240 two-server) Preparation checklist

	Activities	√	Procedures
On the ACTIVE node			
3	Verify whether an HTTPS certificate is installed on the server, and whether it is valid.		Perform procedure Verifying the presence and validity of an HTTPS certificate on an SSPFS-based server on page 545.
4	Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade.		Refer to procedure Verifying group IDs and user IDs on an SSPFS-based server on page 563.
5	Obtain any patches applicable to components on this server (PSE, CS 2000 SAM21 Manager, NPM, SESM, QCA, SSPFS, IEMS).		Perform procedure Transferring patches delivered on CD to the NPM database on page 1884.
6	Prior to the upgrade, determine if the system has the necessary 9 GB unallocated disk space execute the following command as the root user: /opt/nortel/sspfs/fs/meta.pl fs The displayed value must be larger then "19000000" (19,000,000) for the upgrade to succeed. Note: If it is determined that there is not enough unallocated disk space to perform the upgrade, contact Nortel Technical Support.		If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in the *ATM/IP Security and Administration document*, NN10402-600.
7	Perform an audit with the CS 2000 Management Tools.		Refer to Performing an audit on page 596.

(I)SN06.2 to (I)SN08 (Sun Netra 240 two-server) Preparation checklist

	Activities	√	Procedures
8	Perform a full system backup. ***Note:*** Although a full system 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.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.
			Perform procedure Performing a backup of APS audio files to CD or DVD on page 621. ***Note:*** Only perform this procedure if the APS is present on the server.
			Perform procedure Performing a backup of APS oracle data to CD or DVD on page 626. ***Note:*** Only perform this procedure if the APS is present on the server.
			Perform procedure Saving user-defined NPM data using the NPM on page 576. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
			Perform procedure Saving the NPM patch files on page 589. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
9	Proceed to upgrade the CS 2000 Management Tools software.		Refer to Upgrading the CS 2000 Management Tools software on page 633.

Preparing to upgrade from (I)SN07 to (I)SN08

The configurations that support an upgrade from (I)SN07 to (I)SN08 are listed below. Follow the link associated with your configuration.

- Sun Netra t1400 on page 535
- Sun Netra 240 one-server configuration on page 538
- Sun Netra 240 two-server configuration on page 541

ATTENTION
The SSPFS and all applications on the server 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.

ATTENTION
In an office configuration where the Integrated Element Management System (EMS) and the CS 2000 Management Tools (CS2M) software reside on different servers, ensure the Network Patch Manager (NPM) has already been migrated to the server where the Integrated EMS software resides before proceeding with the upgrade from (I)SN07 to (I)SN08.

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)SN08 (Sun Netra t1400) Preparation checklist

	Activities	√	Procedures
1	Verify whether an HTTPS certificate is installed on the server, and whether it is valid.		Perform procedure Verifying the presence and validity of an HTTPS certificate on an SSPFS-based server on page 545.
2	Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade.		Refer to procedure Verifying group IDs and user IDs on an SSPFS-based server on page 563.

(I)SN07 to (I)SN08 (Sun Netra t1400) Preparation checklist

	Activities	√	Procedures
3	Prior to the upgrade, determine if the system has the necessary 9 GB unallocated disk space execute the following command as the root user: /opt/nortel/sspfs/fs/meta.pl fs The displayed value must be larger then "19000000" (19,000,000) for the upgrade to succeed. Note: If it is determined that there is not enough unallocated disk space to perform the upgrade, contact Nortel Technical Support.		If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in the *ATM/IP Security and Administration document*, NN10402-600.
4	Perform an audit with the CS 2000 Management Tools.		Refer to Performing an audit on page 596.
5	Perform a full system backup.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.
			Perform procedure Performing a backup of APS audio files to tape on page 619. ***Note:*** Only perform this procedure if the APS is present on the server.
			Perform procedure Performing a backup of APS oracle data to tape on page 624. ***Note:*** Only perform this procedure if the APS is present on the server.

(I)SN07 to (I)SN08 (Sun Netra t1400) Preparation checklist

	Activities	√	Procedures
			Perform procedure Saving user-defined NPM data using the NPM on page 576. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
			Perform procedure Saving the NPM patch files on page 589. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
6	If IEMS is present on this server, run the IEMS pre-check script. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Refer to Running the IEMS pre-check script on page 561.
7	If IEMS is present on this server, determine if a third-party security application is used. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Refer to Determining if a third-party security application is used on page 558.
8	Proceed to upgrade the CS 2000 Management Tools software.		Refer to Upgrading the CS 2000 Management Tools software on page 633.

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)SN08 (Sun Netra 240 one-server) Preparation checklist

	Activities	√	Procedures
1	Verify whether an HTTPS certificate is installed on the server, and whether it is valid.		Perform procedure Verifying the presence and validity of an HTTPS certificate on an SSPFS-based server on page 545.
2	Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade.		Refer to procedure Verifying group IDs and user IDs on an SSPFS-based server on page 563.
3	Prior to the upgrade, determine if the system has the necessary 9 GB unallocated disk space execute the following command as the root user: /opt/nortel/sspfs/fs/meta.pl fs The displayed value must be larger then "19000000" (19,000,000) for the upgrade to succeed. Note: If it is determined that there is not enough unallocated disk space to perform the upgrade, contact Nortel Technical Support.		If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in the *ATM/IP Security and Administration document*, NN10402-600.
4	Perform an audit with the CS 2000 Management Tools.		Refer to Performing an audit on page 596.

(I)SN07 to (I)SN08 (Sun Netra 240 one-server) Preparation checklist

	Activities	√	Procedures
5	Perform a full system backup.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.
			Perform procedure Performing a backup of APS audio files to CD or DVD on page 621. ***Note:*** Only perform this procedure if the APS is present on the server.
			Perform procedure Performing a backup of APS oracle data to CD or DVD on page 626. ***Note:*** Only perform this procedure if the APS is present on the server.
			Perform procedure Saving user-defined NPM data using the NPM on page 576. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
			Perform procedure Saving the NPM patch files on page 589. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
6	If IEMS is present on this server, run the IEMS pre-check script. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Refer to Running the IEMS pre-check script on page 561.

(I)SN07 to (I)SN08 (Sun Netra 240 one-server) Preparation checklist

	Activities	√	Procedures
7	If IEMS is present on this server, determine if a third-party security application is used. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Refer to Determining if a third-party security application is used on page 558.
8	Proceed to upgrade the CS 2000 Management Tools software.		Refer to Upgrading the CS 2000 Management Tools software on page 633.

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)SN08 (Sun Netra 240 two-server) Preparation checklist

	Activities	√	Procedures
On the INACTIVE node			
1	Verify the state of the cluster.		Perform procedure Verifying the state of a cluster on page 629.
2	Determine through your system administrator whether QCA properties were modified on the Active server at any given time. If they were modified, ensure the Inactive server reflects those modifications. ***Note:*** The properties on the Inactive server will override the properties on the Active server during the upgrade.		Perform procedure “Modifying the QoS Collector Application” in the ATM/IP Configuration Management document, NN10409-500 if required.

(I)SN07 to (I)SN08 (Sun Netra 240 two-server) Preparation checklist

	Activities	√	Procedures
On the ACTIVE node			
1	Verify whether an HTTPS certificate is installed on the server, and whether it is valid.		Perform procedure Verifying the presence and validity of an HTTPS certificate on an SSPFS-based server on page 545.
2	Verify none of the user-defined GIDs and UIDs conflict with the GIDs and UIDs SSPFS uses during the upgrade.		Refer to procedure Verifying group IDs and user IDs on an SSPFS-based server on page 563.
3	Obtain any patches applicable to components on this server (PSE, CS 2000 SAM21 Manager, NPM, SESM, QCA, SSPFS, IEMS).		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
4	Prior to the upgrade, determine if the system has the necessary 9 GB unallocated disk space execute the following command as the root user: /opt/nortel/sspfs/fs/meta.pl fs The displayed value must be larger then "19000000" (19,000,000) for the upgrade to succeed. Note: If it is determined that there is not enough unallocated disk space to perform the upgrade, contact Nortel Technical Support.		If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in the *ATM/IP Security and Administration document*, NN10402-600.
5	Perform an audit with the CS 2000 Management Tools.		Refer to Performing an audit on page 596.

(I)SN07 to (I)SN08 (Sun Netra 240 two-server) Preparation checklist

	Activities	√	Procedures
6	Perform a full system backup. ***Note:*** Although a full system 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.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.
			Perform procedure Performing a backup of APS audio files to CD or DVD on page 621. ***Note:*** Only perform this procedure if the APS is present on the server.
			Perform procedure Performing a backup of APS oracle data to CD or DVD on page 626. ***Note:*** Only perform this procedure if the APS is present on the server.
			Perform procedure Saving user-defined NPM data using the NPM on page 576. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.
			Perform procedure Saving the NPM patch files on page 589. ***Note:*** Only perform this procedure if the NPM is on the same server as the CS 2000 Management Tools.

(I)SN07 to (I)SN08 (Sun Netra 240 two-server) Preparation checklist

	Activities	√	Procedures
7	If IEMS is present on this server, run the IEMS pre-check script. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Refer to Running the IEMS pre-check script on page 561.
8	If IEMS is present on this server, determine if a third-party security application is used. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Refer to Determining if a third-party security application is used on page 558.
9	Proceed to upgrade the CS 2000 Management Tools software.		Refer to Upgrading the CS 2000 Management Tools software on page 633.

Verifying the presence and validity of an HTTPS certificate on an SSPFS-based server

Application

Use this procedure to verify whether an HTTPS certificate is installed on the server, and if one is installed, ensuring it has not expired.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

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

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

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

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

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

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

b When prompted, enter the root password.

4 Access the apache directory by typing

```
# cd /opt/apache
```

and pressing the Enter key.

5 Determine whether a certificat file (.crt) and a key file (.key) exist on the server by typing the following commands:

```
# find conf -name *.crt
```

and pressing the Enter key.

```
# find conf -name *.key
```

and pressing the Enter key.

6 Use the following table to determine your next step.

If	Do
the response to the commands in the previous step (step 5) displayed a .crt and a .key file, then an HTTPS certificate exists on the server	step 7
otherwise, you need to install a certificate	step 11

7 Change directories by typing

```
# cd conf
```

and pressing the Enter key.

8 Verify the certificate dates by typing

```
# keytool -printcert -file ssl.crt/server.crt
```

and pressing the Enter key.

Example response

```
Owner: EMAILADDRESS=znc0s0jh.us.nortel.com,
CN=znc0s0jh.us.nortel.com, OU=
jh.us.nortel.com, O=Nortel, L=RTP, ST=NC, C=US
Issuer: EMAILADDRESS=znc0s0jh.us.nortel.com,
CN=znc0s0jh.us.nortel.com, OU
0jh.us.nortel.com, O=Nortel, L=RTP, ST=NC, C=US
Serial number: c5aa63a60d80bf96
Valid from: Thu Oct 27 02:51:50 EDT 2005 until: Sun
Oct 26 01:51:50 EST 2008
Certificate fingerprints:
         MD5:
B1:1D:F6:17:7B:95:3D:7C:61:48:9E:78:6A:D5:22:29
         SHA1:
D8:06:0B:73:9A:46:76:A3:E9:52:65:96:16:95:E6:A5:E6
:54:53:BC
```

9 From the response, locate the certificate dates next to Valid from.

10 Use the following table to determine your next step.

If	Do
the certicate has reached its expiry date	step 11
otherwise	step 12

11 Install or replace the HTTPS certificate.

For detailed steps, refer to procedure Installing or replacing an HTTPS certificate on an SSPFS-based server on page 548.

12 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Installing or replacing an HTTPS certificate on an SSPFS-based server

Application

Use this procedure to install an HTTPS certificate on a Succession Server Platform Foundation Software (SSPFS)-based server. An HTTPS certificate enables secure transmission of communications, and is required from the SN07 release onward.

The steps to create a self-signed certificate are included in this procedure if you choose to use a self-signed certificate (see Types of certificates).

Types of certificates

Following, are the three types of security certificates that can be used. These certificates differ in the level of trust that needs to be assigned to a server.

- a certificate granted from a well known certificate authority (CA): used when the server is used in a public way, such as for e-commerce web sites
- a company-generated certificate: used when the server is used internally, and the operating company has its own internal CA
- a self-signed certificate created locally on the server: used when the server is used in a more restricted manner.

Note: When a server with a self-signed certificate is accessed, the browser presents the certificate and asks whether the certificate can be trusted. If the user answers “yes”, the server can be accessed. If the user answers “no”, nothing further will be received from the server.

Prerequisites

This procedure has the following prerequisites:

- The domain name service (DNS) must be enabled on the server to allow the security certificate to work, and must be enabled prior to the installation of the certificate. Refer to procedure “Configuring Domain Name Service” in the ATM/IP Solution-level Configuration Management document, NN10409-500.
- If purchasing a certificate from a third-party certificate authority (CA), such as VeriSign, obtain a PEM-encoded X.509 certificate, but without a passcode.

  Note: The name of the certificate should match the host name of the server. Nortel Networks recommends the installation of a unique certificate for each host. A separate file contains the key, and should not have an associated password.

- Make sure all GUI screens are closed before you install the certificate.
- The RSA key for the HTTPS certificate must not have a password.
- The certificate must be created with the fully qualified domain name (FQDN) of the server on which the certificate will be installed.
- Sub-directories “ssl.crt” and “ssl.key” must already exist in the “/opt/apache/conf” directory.

Action

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

- Simplex configuration (one server) on page 549
- High-availability configuration (two servers) on page 554

Simplex configuration (one server)

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server on which you want to install the HTTPS certificate

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

If you are	Do
using a self-signed certificate	step 5
not using a self-signed certificate	step 6

5 Create the self-signed certificate as follows:

a Access the “conf” directory by typing

```
# cd /opt/apache/conf
```

and pressing the Enter key.

b Generate the key file (server.key) by typing

```
# /opt/openssl/bin/openssl genrsa -rand
/var/log/sspfslog 1024 > server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -rand and /var/log/sspfslog entries.

c Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -key and server.key entries.

Example response:

```
You are about to be asked to enter information
that will be incorporated into your
certificate request.
What you are about to enter is what is called
a Distinguished Name or a DN.
There are quite a few fields but you can leave
some blank.
For some fields there will be a default value.
If you enter '.',the field will be left blank.
------

Country Name (2 letter code) [AU]:
```

d When prompted, enter a two letter code for the country where the server is located.

Example response:

```
State or Province Name (full name)
[Some-State]:
```

e When prompted, enter the full name of the State or Province where the server is located.

Example response:

```
Locality Name (eg, city) []:
```

f When prompted, enter the city where the server is located.

Example response:

```
Organization Name (eg, company) [Internet
Widgits Pty Ltd]:
```

g When prompted, enter the name of the company that owns the server.

Example response:

```
Organizational Unit Name (eg, section) []:
```

h When prompted, enter the name of the department that owns the server.

Example response:

```
Common Name (eg, YOUR name []:
```

i When prompted, enter the fully qualified domain name (FQDN) of the server.

Example response:

```
Email Address []:
```

j When prompted, enter the email address of the organization that owns the server.

6 Place the certificate file (server.crt) you obtained in "/opt/apache/conf/ssl.crt".

Note: If directory "ssl.crt" does not exist, you need to create it.

7 Place the key file (server.key) you obtained in "/opt/apache/conf/ssl.key".

Note: If directory "ssl.key" does not exist, you need to create it.

8 Change the certificate's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between "other" and the directory path.

9 Change the key file's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between "other" and the directory path.

10 Set the certificate permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

11 Set the key file permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

12 Restart the WEBSERVER as follows:

a Stop the WEBSERVER by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.

b Start the WEBSERVER by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.

13 Restart the WEBSERVICES as follows:

a Stop the WEBSERVICES by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.

b Start the WEBSERVICES by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

14 If you installed an HTTPS certificate on an existing SSPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure “Clearing the JWS cache on a client workstation” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

15 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

High-availability configuration (two servers)

At your workstation

1 Log in to the active server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the active server on which you want to install the HTTPS certificate

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

If you are	Do
using a self-signed certificate	step 5
not using a self-signed certificate	step 6

5 Create the self-signed certificate as follows:

a Access the “conf” directory by typing

```
# cd /opt/apache/conf
```

and pressing the Enter key.

b Generate the key file (server.key) by typing

```
# /opt/openssl/bin/openssl genrsa -rand
/var/log/sspfslog 1024 > server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -rand and /var/log/sspfslog entries.

c Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -key and server.key entries.

Example response:

```
You are about to be asked to enter information
that will be incorporated into your
certificate request.
What you are about to enter is what is called
a Distinguished Name or a DN.
There are quite a few fields but you can leave
some blank.
For some fields there will be a default value.
If you enter '.',the field will be left blank.
------

Country Name (2 letter code) [AU]:
```

d When prompted, enter a two letter code for the country where the server is located.

Example response:

```
State or Province Name (full name)
[Some-State]:
```

e When prompted, enter the full name of the State or Province where the server is located.

Example response:

```
Locality Name (eg, city) []:
```

f When prompted, enter the city where the server is located.

Example response:

```
Organization Name (eg, company) [Internet
Widgits Pty Ltd]:
```

g When prompted, enter the name of the company that owns the server.

Example response:

```
Organizational Unit Name (eg, section) []:
```

h When prompted, enter the name of the department that owns the server.

Example response:

```
Common Name (eg, YOUR name []:
```

i When prompted, enter the fully qualified domain name (FQDN) of the server.

Example response:

```
Email Address []:
```

j When prompted, enter the email address of the organization that owns the server.

6 Place the certificate file (server.crt) you obtained in "/opt/apache/conf/ssl.crt".

Note: If directory "ssl.crt" does not exist, you need to create it.

7 Place the key file (server.key) in"/opt/apache/conf/ssl.key".

Note: If directory "ssl.key" does not exist, you need to create it.

8 Change the certificate's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between "other" and the directory path.

9 Change the key file's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between "other" and the directory path.

10 Set the certificate permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

11 Set the key file permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

12 Restart the WEBSERVER as follows:

a Stop the WEBSERVER by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.

b Start the WEBSERVER by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.

13 Restart the WEBSERVICES as follows:

a Stop the WEBSERVICES by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.

b Start the WEBSERVICES by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

14 Clone the image of the node with the HTTPS certificate onto the other node using procedure Cloning the image of one node in a cluster to the other node on page 766.

15 If you installed an HTTPS certificate on an existing SSPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure “Clearing the JWS cache on a client workstation” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

16 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Determining if a third-party security application is used

Application

Use this procedure when directed to do so to determine if a third-party security application is used.

If the server is using a third-party security application, the NSCD, PAM and NSSwitch configuration files (nscd.conf, pam.conf and nsswitch.conf) will have special edits in them. Those special edits will need to be put back following the upgrade, since during the IEMS software upgrade, the configuration files are replaced with new configuration files that use the IEMS security application.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the host name of IP address of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

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

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server
is the host name of IP address of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

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

b When prompted, enter the root password.

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

4 Determine if a third-party security application is used on this server by typing

```
$ grep pam_dce /etc/pam.conf
```

and pressing the Enter key.

```
$ grep pam_ldap /etc/pam.conf
```

and pressing the Enter key.

5 Use the following table to determine your next step.

If	Do
you received a response from either of the commands in step 4	step 6
otherwise	step 7

6 This server is using a third-party security application, and the NSCD, PAM and NSSwitch configuration files (nscd.conf, pam.conf and nsswitch.conf) have special edits in them. Those special edits will need to be put back following the upgrade, since during the upgrade, the configuration files are replaced with new configuration files that use the IEMS security application.

Inform your system administrator before you proceed with the upgrade.

7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Running the IEMS pre-check script

This procedure applies only to IEMS software upgrades from (I)SN07 or (I)SN08 to a higher version. Run the script prior to upgrading the SSPFS or IEMS software on an IEMS server. Upgrading from (I)SN07 to a higher version ,the script determines which groups defined by IEMS in (I)SN07 conflict with groups defined by the higher version and which devices are not supported with the higher version. Upgrading from (I)SN08 to a higher version ,the script determines which devices are not supported with the higher version.

ATTENTION
The upgrade should not proceed until the IEMS pre-check test passes and indicates that the upgrade can proceed. If unsupported device versions are configured in the IEMS inventory, the IEMS upgrade will fail.

At the server:

1 Run the IEMS pre-check script by entering:

Note: In a two-server configuration, enter the command on the active server.

```
# /opt/nortel/iems/current/bin/IEMSUpgradePreCheck.sh
8.0 7.0 6.2
```

2 Use the following table to determine your next step.

If	Do
the pre-check test passes	step 5
the pre-check test fails	step 3

3 If any device versions are not supported by the version you are upgrading to, the pre-check step fails, and the following warning message appears.

Example response

```
IEMS Upgrade Pre-Check Test:
**********************************
The IEMS upgrade pre-check test Failed. The IEMS
upgrade should not proceed.
```

```
Device version check failed. The following
devices must be upgraded prior to proceeding
with the IEMS Upgrade to SN08.0:-

====================================
|S.No.| Device Name       | Version |
====================================
| 1     wcars1qf-MDM-Mgr      6.0
| 2     wcars1jk-MG9K-Mgr_9   6.0
------------------------------------
```

If the IEMS pre-check upgrade fails, upgrade the device version in the IEMS, for the devices that appear in the list, before proceeding with the IEMS upgrade.

Note: Any devices that appear in the list must be running the target software version. If they are not, the devices must be upgraded to the target software version.

4 Repeat this procedure to run the IEMS pre-check script.

If	Do
the IEMS pre-check test passes	step 5
the IEMS pre-check test fails	contact your next level of support

5 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to 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, nortel

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, coadm, Administrator, and nt120 through to nt220.

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.

Performing a backup of oracle data on an SSPFS-based server

Application

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

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

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

  Note: If the server is hosting the Integrated EMS, it is highly recommended to purge the Integrated EMS event and performance data prior to executing the data backup. This reduces the size of the oracle space used by the Integrated EMS, and therefore, reduces the backup time, and can avoid a backup failure. The purge capability is only available in (I)SN07 onward.

- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core and Billing Manager (CBM)

  Note: If the server is hosting the Core and Billing Manager (CBM), an oracle data backup is not required.

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

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater
- for a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- for a Sun Netra 240, you need one or more blank DVD-R or DVD-RW to store the data

Note 1: The backup utility limits the storage to 2 GB on aDVD-R and DVD-RW.

Note 2: If you are using a newDVD-RW, or want to use a used DVD-RW andneed to erase the contents, refer to procedure "Preparing a DVD-RW for use" in the *ATM/IP Security and Administration*, NN10402-600.

ATTENTION

The database must be in sync with the Communication Server 2000 and the MG 9000 Manager (if present). Therefore, ensure you have an image of both before you proceed. Performing a restore from the Oracle database alone can cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

Action

ATTENTION

In a two-sever configuration, execute this procedure on the active server.

At the server

1 Insert the blank tape or DVD into the drive. In a two-server configuration, insert the blank DVD into the drive of the active server.

At your workstation

2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the SSPFS-based server on which you want to perform the backup

Enter the physical IP address of the active server in a two-server configuration.

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 If the server is hosting the Integrated EMS, and you want to purge the event and performance data, do step 7, otherwise proceed to step 8.

7 Purge the Integrated EMS event and performance data as follows:

Note: Purging the Integrated EMS event and performance data prior to executing the data backup, reduces the size of the oracle space used by the Integrated EMS, and therefore, reduces the backup time, and can avoid backup failure. The purge capability is only available in (I)SN07 onward.

a

ATTENTION
This step stops the Integrated EMS server, therefore, ensure it is acceptable at this time to stop the Integrated EMS server.

Stop the Integrated EMS server by typing

```
# servstop IEMS
```

and pressing the Enter key.

b Run the script to purge the data by typing

```
# /opt/nortel/iems/current/bin/purgeTempData.sh
```

and pressing the Enter key.

c Start the Integrated EMS server by typing

```
# servstart IEMS
```

and pressing the Enter key.

8 Use the following table to determine your next step.

If you are using	Do
a tape	step 9
a DVD	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	step 12

11 Verify the backup to tape was successful as follows:

a List the content of the tape by typing

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

and pressing the Enter key.

Example response:

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:16 2005
opt/oracle.dmp.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:16 2005
opt/critdata.cpio
```

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

You have completed this procedure.

Note: To restore the data from this tape, refer to procedure “Restoring the oracle data on an SSPFS-based server” in the *ATM/IP Security and Administration*, NN10402-600.

12 Verify the backup to DVD was successful as follows:

a Reinsert the backup DVD into the drive.

b List the content of the DVD by typing

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

and pressing the Enter key.

Example response:

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:17 2005
opt/oracle.dmp.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:17 2005
opt/critdata.cpio
```

Note: When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

13 Eject the DVD from the drive as follows:

a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

 # /etc/init.d/volmgt stop

 # /etc/init.d/volmgt start

Then press the eject button located on the front of the DVD drive.

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

You have completed this procedure.

Note: To restore the data from this DVD, refer to procedure “Restoring the oracle data on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.

Performing a backup of file systems on an SSPFS-based server

Application

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

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

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

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater
- you must perform a data backup prior to performing this procedure (refer to procedure Performing a backup of oracle data on an SSPFS-based server on page 566, if required)

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

- for a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- for Sun Netra 240, you need one or more blank DVD-R or DVD-RW to store the data

  Note 1: The backup utility limits the storage to 2 GB on a DVD-R and DVD-RW.

  Note 2: If you are using a new DVD-RW, or want to use a used DVD-RW and need to erase the contents, refer to procedure “Preparing a DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

Action

ATTENTION
In a two-sever configuration, execute this procedure on the active server.

At the server

1 Insert the blank tape or DVD into the drive. In a two-server configuration, insert the blank DVD into the Active server.

At your workstation

2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server on which you are performing the backup

Enter the physical IP address of the Active server in a two-server configuration.

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

If you are using	Do
a tape	step 6
a DVD	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, the system will prompt you to insert another blank DVD if more than one is needed.

If you are using	Do
a tape	step 8
a DVD	step 9

8 Verify the backup to tape was successful as follows:

a List the content of the tape by typing

```
# gtar -tvMf /dev/rmt/0
```

and pressing the Enter key.

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

You have completed this procedure.

9 Verify the backup to DVD was successful as follows:

a Reinsert the backup DVD into the drive.

b List the content of the DVD by typing

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

and pressing the Enter key.

Note: When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

10 Eject the DVD from the drive as follows:

a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

 # /etc/init.d/volmgt stop

 # /etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

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

You have completed this procedure.

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 are user-defined sets, reports, alarms, and tasks. These procedures do not include steps for saving system defined data, which will be re-created during the NPM upgrade. All user-defined information will be removed during the NPM upgrade. These procedures contain 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 576
- Using the NPM GUI on page 582

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.

ATTENTION
In a two-server configuration, execute this procedure on the active server.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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 need to 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, DEVICE_ONHOLD, DEVICE_AUDITFAIL, DISABLED_APPLIED, ENABLED_REMOVED, REL-GEN_NOT_APP, PFRSGETPATCH, and PFRSGENREPORT.

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, AUDIT, PFRSGETPATCH, PFRSGENREPORT, and DELETEREPORTS.

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 Generate and save a copy of the PATCHLIST report for later reference, as follows:

a Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

b Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

c When prompted, enter the password for the root user.

d Change directory to /data/npm by typing

```
# cd /data/npm
```

and pressing the Enter key.

e Determine if a tmp directory exists in the npm directory by typing

```
# ls -l
```

and pressing the Enter key.

f Use the following table to determine your next step.

If	Do
a tmp directory exists	substep h
otherwise	substep g

g Create a tmp directory by typing

```
# mkdir tmp
```

and pressing the Enter key.

h Change directory to the tmp directory by typing

```
# cd tmp
```

and pressing the Enter key.

i Generate the patchlist report by typing

```
$ npm q patchlist output <filename>.list
```

and pressing the Enter key.

where

filename
is the name you want to give to the patchlist report

Example
npm q patchlist output aug032004.list

Example response

```
Enter the NPM Succession user id and
password.
Login
```

j When prompted, enter the NPM user ID.

Example response

```
password
```

k 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
```

l Display the file by typing

```
$ ls
```

and pressing the Enter key.

Example response

```
aug032004.list
local.login
local.cshrc
local.profile
```

m If required, display the contents of the file by typing

```
$ cat <filename> |more
```

and pressing the Enter key.

where

filename
is the name you gave to the patchlist report file

Example
cat aug032004.list

Example response

```
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
```

19 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

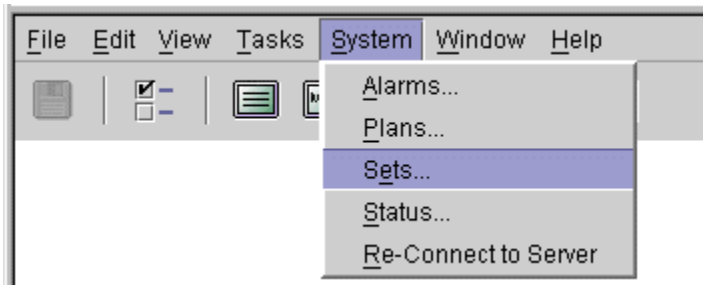
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

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 Select one of the user-defined sets, then click **Edit** to display its details.

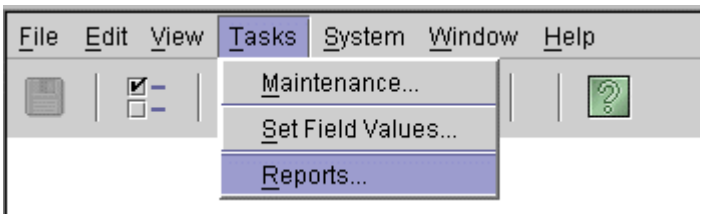
Note: Ignore the following system-defined sets: ALLPATCHES, AUTOAPPLY, NOSPAPP, ALLDEVICES, OAMDEVICES, AUTORESTARTDEVICES, MG9KDEVICES, and GWCDEVICES.

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 Select one of the user-defined reports, then click **Edit** to display the details.

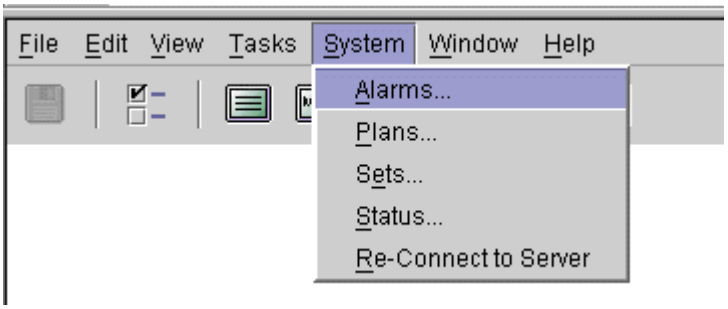
Note: Ignore the following system defined reports: ACTLIST, CALCLIST, DEVICE, DEVICELIST, DISABLEDAPPLIED, DISABLEDREMOVED, ENABLEDAPPLIED, ENABLEDREMOVED, FULLDEVICELIST, LOADLIST, PATCH, PATCHES_SINCE, PATCHINFO, PATCHLIST, DEVICE_ACTIVITY, DEVICE_ACTLEVEL, DEVICE_APPLEVEL, and INVALID_LOADNAME.

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 Select one of the user-defined alarms, then click **Edit** to display its details.

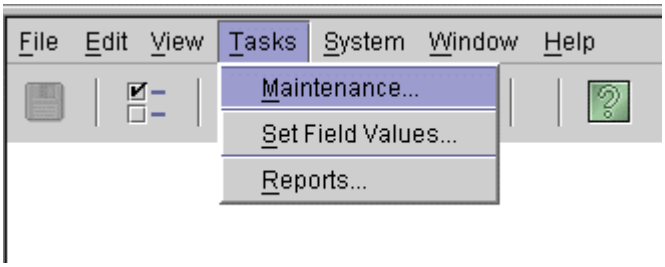
Note: Ignore the following system-defined alarms: ACT_NOT_APP, ACT_NOT_ACT, DEBUG_APP, DNR_NOT_APP, EMG_NOT_APP, GEN_NOT_APP, LTD_NOT_APP, OBS_NOT_REMOVED, OBE_NOT_REMOVED, REMOVED_PATCHES, PATCH_ONHOLD, DEVICE_ONHOLD, DEVICE_AUDITFAIL, DISABLED_APPLIED, ENABLED_REMOVED, REL-GEN_NOT_APP, PFRSGETPATCH, and PFRSGENREPORT.

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 Select one of the user-defined tasks, then click **Edit** to display its details.

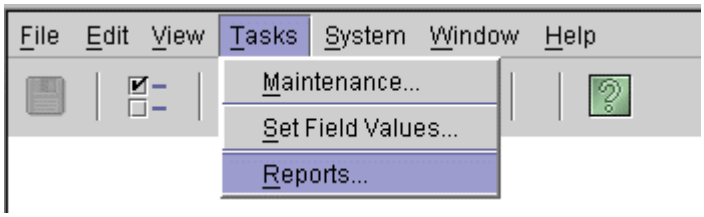
Note: Ignore the following system-defined tasks: AUTOAPPLY, AUTORESTART, AUDIT, PFRSGETPATCH, PFRSGENREPORT, and DELETEREPORTS.

23 Record the details of the task.

24 Repeat steps 21 through 23 for each user-defined task.

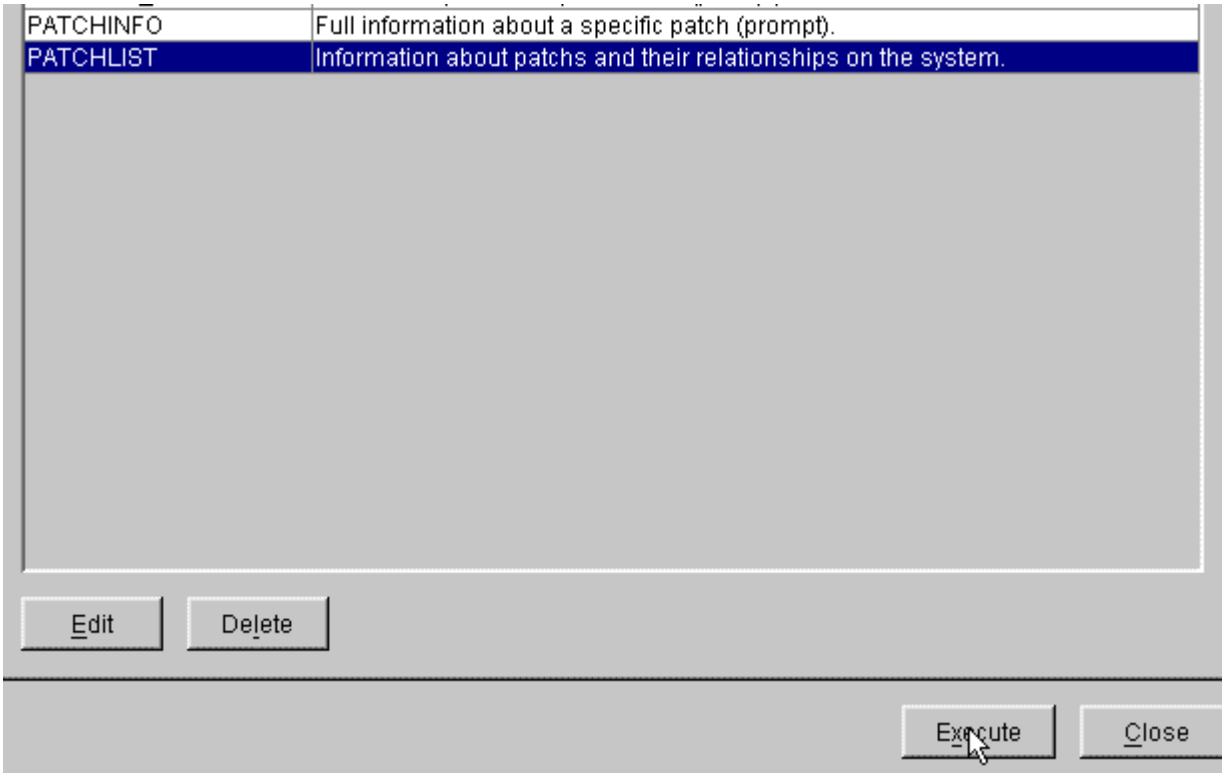
25 Click **Close** to close the Tasks window.

26 On the Tasks menu, click **Reports...**.

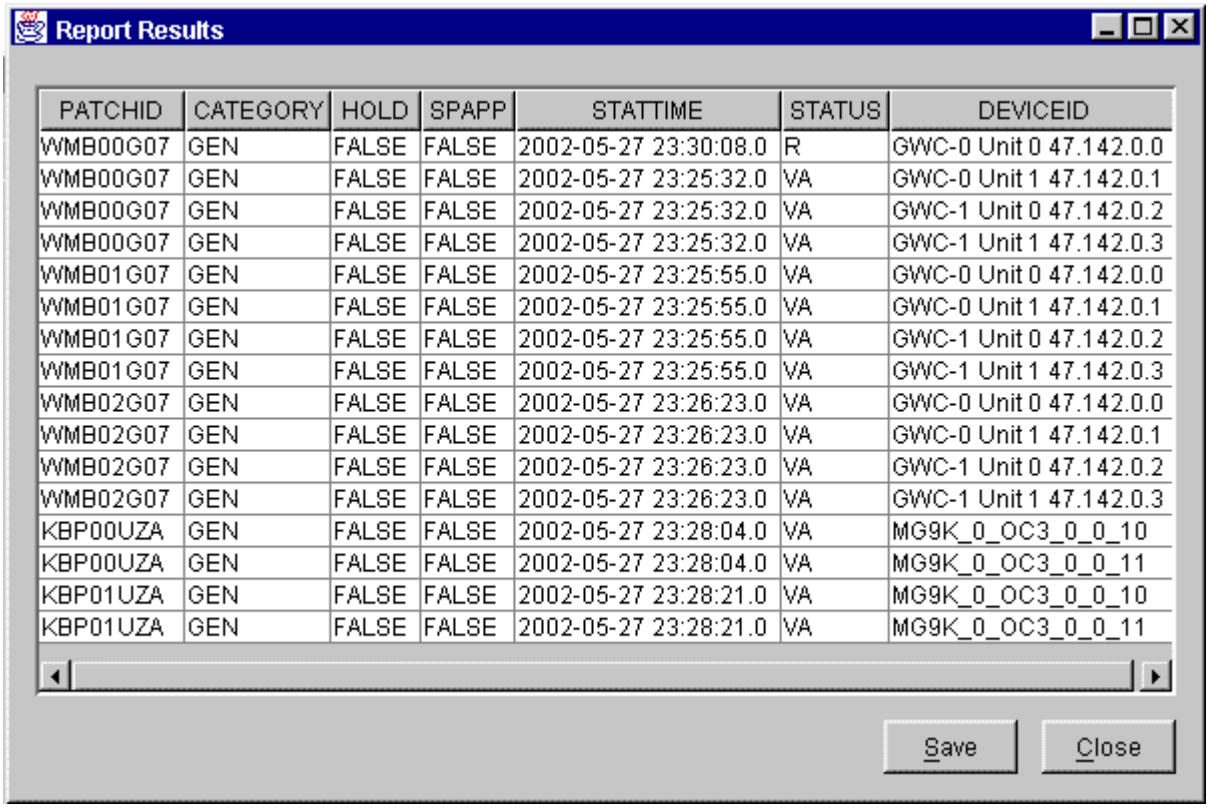


27 Click the **Reports List** tab to display the list of all reports.

28 Select PATCHLIST, then click **Execute** to run the PATCHLIST report.

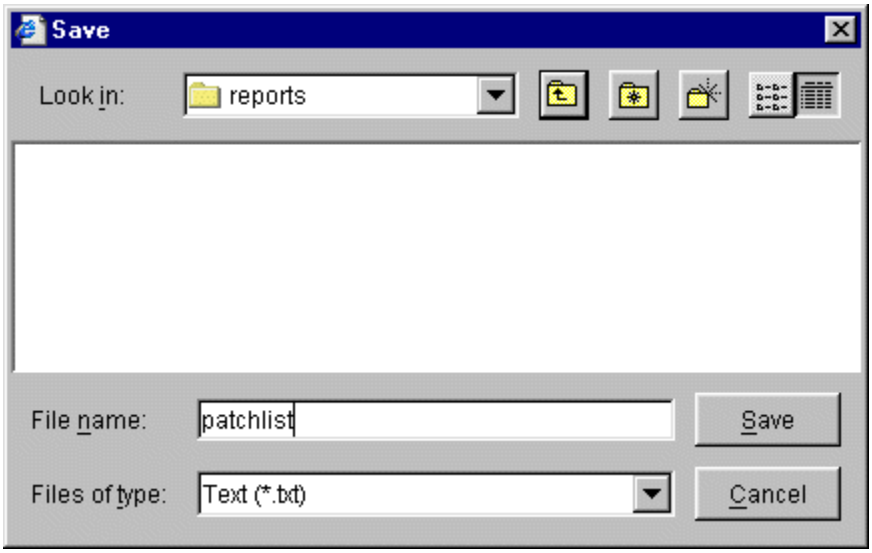


The Reports Results window is displayed.



29 Click **Save** to save the results of the PATCHLIST report.

30 In the Filename box enter a name for the saved report, then click **Save**.



31 Click **Close** to close the Report Results window.

32 Click **Close** to close the Reports window.

33 On the File menu, click **Exit** to exit the NPM GUI if required.

34 Click **Yes** to confirm you want to exit the NPM GUI.

35 You have completed this procedure if upgrading from (I)SN07. If applicable, return to the high-level task or procedure that directed you to this procedure.

If you are upgrading from (I)SN08, continue on to step 36 and archive the NPM backup data.

36 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the SSPFS-based server where NPM resides

37 When prompted, enter your user ID and password.

38 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

39 When prompted, enter the root password.

40 Change directory to the data directory by typing

```
# cd /data
```

and pressing the Enter key.

41 Make a directory to store the old NPM files by typing

```
# mkdir <npm_old>
```

where

npm_old
is a valid Unix directory name

42 Change directory to the directory you just created by typing

```
# cd <npm_old>
```

where

npm_old
is a valid Unix directory name

43 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_db
```

44 Archive the NPM database into the a file by typing

```
# tar -cvf old_npm_db.tar /data/npm/database/*
```

45 Return to the home directory by typing

```
# cd
```

and pressing the Enter key.

46 Continue this procedure by performing either Saving NPM patch files to tape (Sun Netra t1400 only) or Saving NPM patch files to CD (Sun Netra 240 only) procedure in Saving the NPM patch files on page 589.

Note: There are slightly different parameters used when saving NPM patch files to the selected media as opposed to when these actions are performed as part of this procedure.

When performing	Be aware that
Saving NPM patch files to tape (Sun Netra t1400 only)	the information about the two-server configuration does not apply.
	when copying the patch files to tape use the following command: **# tar cv /datanpm_old/old_NPM_db.tar**
Saving NPM patch files to CD (Sun Netra 240 only)	when making an ISO image of the patch files and writing this image to the CD or DVD use the following command: **# /opt/nortel/sspfs/bks/cdwrite /data/npm_old/ NPM_DB**

47 You have completed this procedure if upgrading from (I)SN08. If applicable, return to the high-level task or procedure that directed you to 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 590
- Saving NPM patch files to tape (Sun Netra t1400 only) on page 593
- Saving NPM patch files to CD (Sun Netra 240 only) on page 594

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 or DVD (Sun Netra 240), you can restore them using procedure “Restoring NPM patch files” in the ATM/IP Fault Management document, NN10408-900.

Prerequisites

This procedure has the following prerequisites if you are saving the NPM patch files to tape, CD or DVD:

- for a Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- for a Netra 240, you need one or more blank CD-R, CD-RW, DVD-R or DVD-RW to store the data

Note 1: The backup utility limits the storage to 2 GB on a DVD-R and DVD-RW.

Note 2: If you are using a new 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, if required.

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)

ATTENTION
In a two-sever configuration, execute this procedure on the active server.

Saving NPM patch files to disk

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the SSPFS-based server where NPM resides

In a two-server configuration, enter the physical IP address of the active server.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing **`ubmstat`**. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

5 Verify 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, then skip this step.

Save a copy of the needed patch files as follows:

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
```

Watch for any errors during the copy.

c Ensure the backup directory contains the patches by typing

```
# ls <directory_path>
```

and pressing the Enter key.

where

directory_path
is the path to the directory where you copied the patch files

Example

```
# ls /data/npm_old/patch_data
```

11 Return to the home directory of the UNIX host by typing

```
# cd
```

and pressing the Enter key.

You have completed this procedure.

Saving NPM patch files to tape (Sun Netra t1400 only)

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the SSPFS-based server where NPM resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 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.

You have completed this procedure.

Saving NPM patch files to CD (Sun Netra 240 only)

At the server

1 Insert a blank CD or DVD into the drive.

Note: In a two-server configuration, insert the blank CD or DVD into the Active server.

At your workstation

2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the SSPFS-based server where NPM resides

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

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

6 Create a temporary directory by typing

```
# mkdir /tmp/.iso
```

and pressing the Enter key.

Note: The directory may already exist.

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 1: Ensure there is a space between the directory /data/npm/Au and PATCHES.

Note 2: 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.

You have completed this procedure.

Performing an audit

Application

Use this procedure to manually perform a line, trunk, V5.2 interface, or CS 2000 (CS2K) data audit.

Note: The V5.2 audit is only available in the international version of the software and not in the North American.

You can set the audit to run automatically at a specific time on a daily or a weekly basis. Refer to procedure “Configuring an audit schedule” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

CS 2000 data audit

For a CS2K data audit, the system compares the GWC element manager database (part of the CS 2000 GWC Manager database) with the CS 2000 XA-Core database and flags any mismatches between the two databases. The XA-Core is considered to hold the ‘master’ database.

Remedial actions offered are likely to involve deletion of inconsistent data. However, where possible, the option to repair data inconsistencies will be given.

Line audit

For a line audit, the system compares the ENDPOINTENTRY area in the CS 2000 GWC Manager database with the following tables in the CS 2000 XA-Core database:

- DNINV
- LGRPINV
- LNINV
- LNENDPT (if DQOS gateway has been provisioned)
- HUNTMEM (if hunt groups have been provisioned)
- MDNMEM (if MADN groups have been provisioned)

The system writes the results of the audit into two files, one containing a list of valid data and the other containing a list of problem data. The files are stored on the CS 2000 Management Tools server.

Trunk audit

For a trunk audit, the system compares the ENDPOINTENTRY area in the CS 2000 GWC Manager database with the following tables in the CS 2000 XA-Core database:

- SERVRINV
- TRKMEM
- LTMAP
- TRKSGRP

The system writes the results of the audit into two files, one containing a list of valid data and the other containing a list of problem data. The files are stored on the CS 2000 Management Tools server.

V5.2 audit

For a V5.2 data integrity audit, the system compares data in the following databases and flags any mismatches:

- V5.2 interface data stored in the Network View database
- V5.2 endpoint data stored in the CS 2000 GWC Manger database
- V5.2 interface data stored in the table GPPTRNSL in the CS 2000 XA-Core database

Remedial actions offered are likely to involve deletion of inconsistent data. However, where possible, the option to repair data inconsistencies will be offered.

Prerequisites

It is recommended to run only one audit at a time, therefore, ensure your manual audit does not conflict with another scheduled audit. Running multiple audits at the same time may cause some unexpected errors.

You must be assigned to user group “mgcadm” to run an audit. If required, refer to procedure “Setting up users on a Sun server” in the ATM/IP Administration and Security document, NN10281-600.

Action

Perform the following steps to complete this procedure.

At your workstation

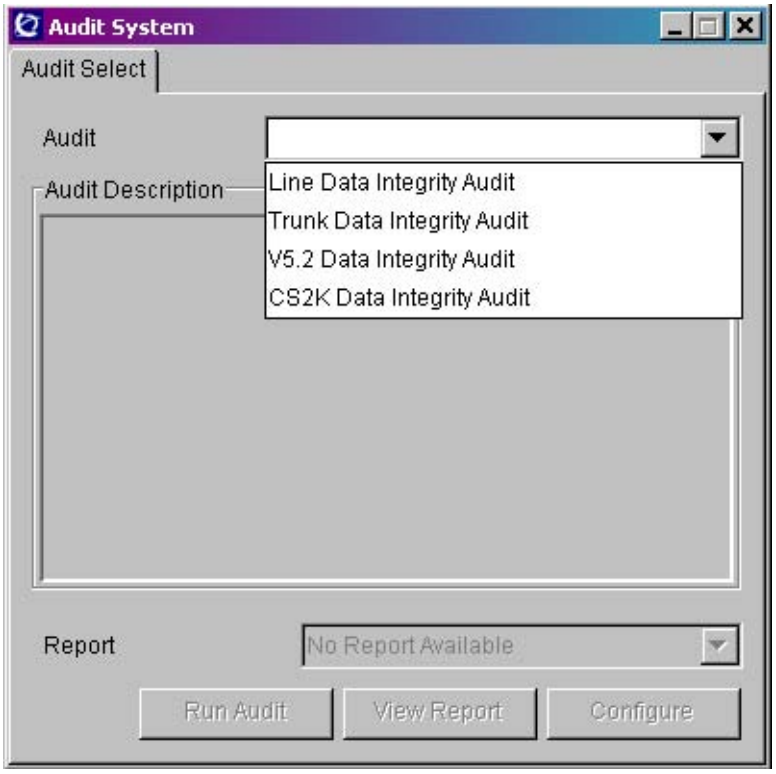
1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866 in this document if required.

At the CS2000 Management Tools GUI

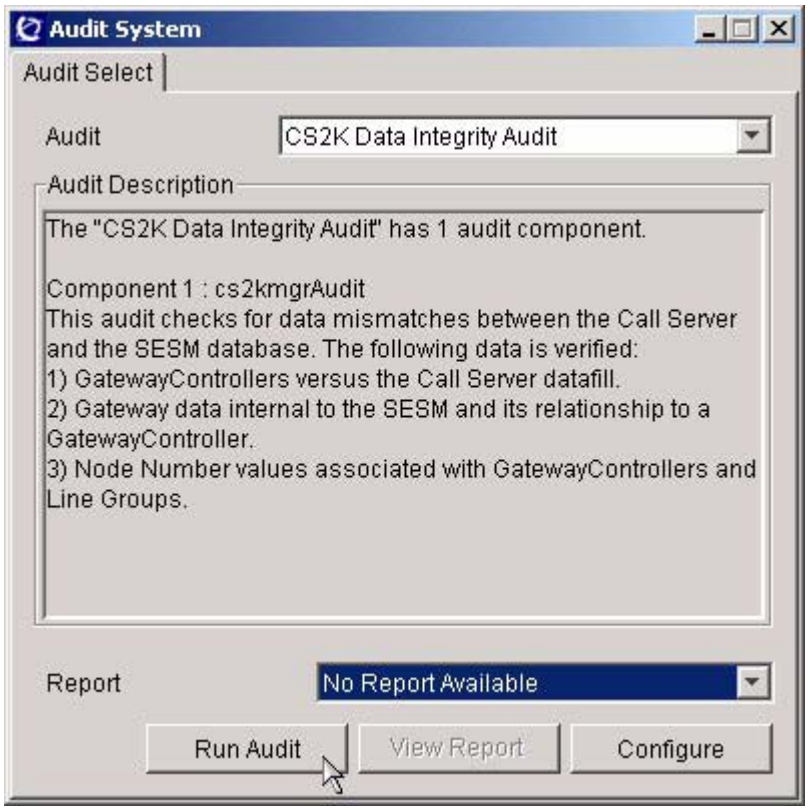
2 On the **Maintenance** menu, click **Audit System**.

The Audit System window opens.

3 In the **Audit** list, click the type of audit you want to perform.



4 Click **Run Audit**.



During the audit, an Audit Status window is displayed to indicate the audit is in progress. The Audit Status window indicates when the audit is complete.

Note: If the audit does not execute successfully, the Audit Status window indicates that the audit failed and provides the reason. Contact your next level of support to resolve the problem if required.

5 Once the audit completes, click **Close** to close the Audit Status window.

6 Use the following table to determine your next step.

If additional audits	Do
need to be run	step 3
do not need to be run	step 7

7 Use the following table to determine your next step.

If you performed a	Do
CS2K Data Integrity Audit	step 8
Line Data Integrity Audit	step 12
Trunk Data Integrity Audit	step 15
V5.2 Data Integrity Audit	step 18

8 Proceed as follows for a CS2K Data Integrity Audit:

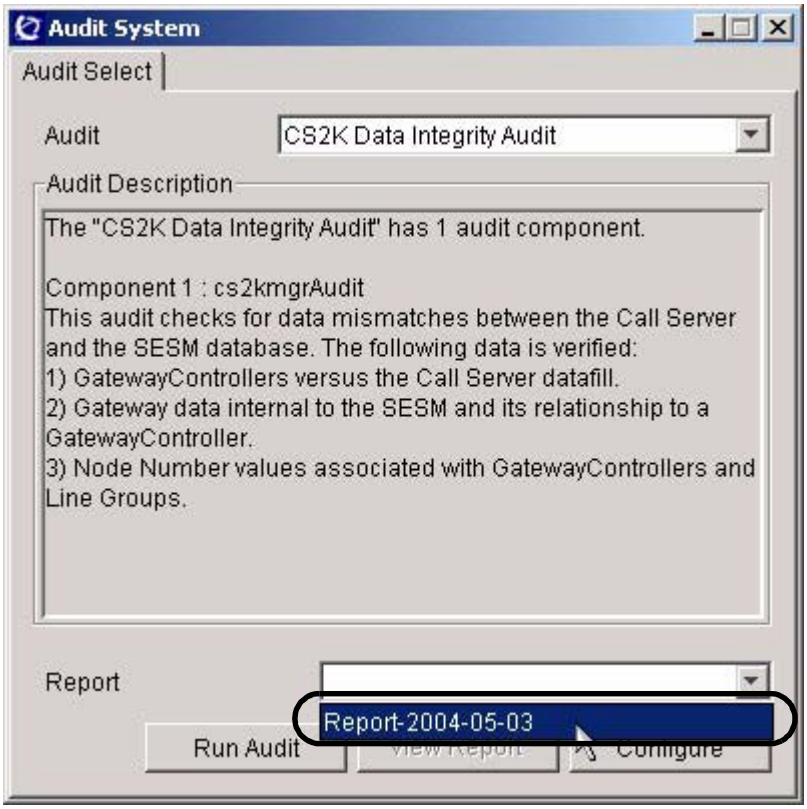
a Ensure that you have selected **CS2K Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

b Select **Report** <date> from the pull-down menu in the Report field at the bottom of the dialog box.

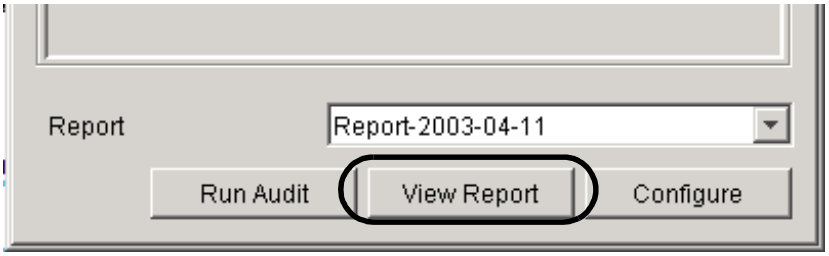
The file name has the following format:

Report-<date>

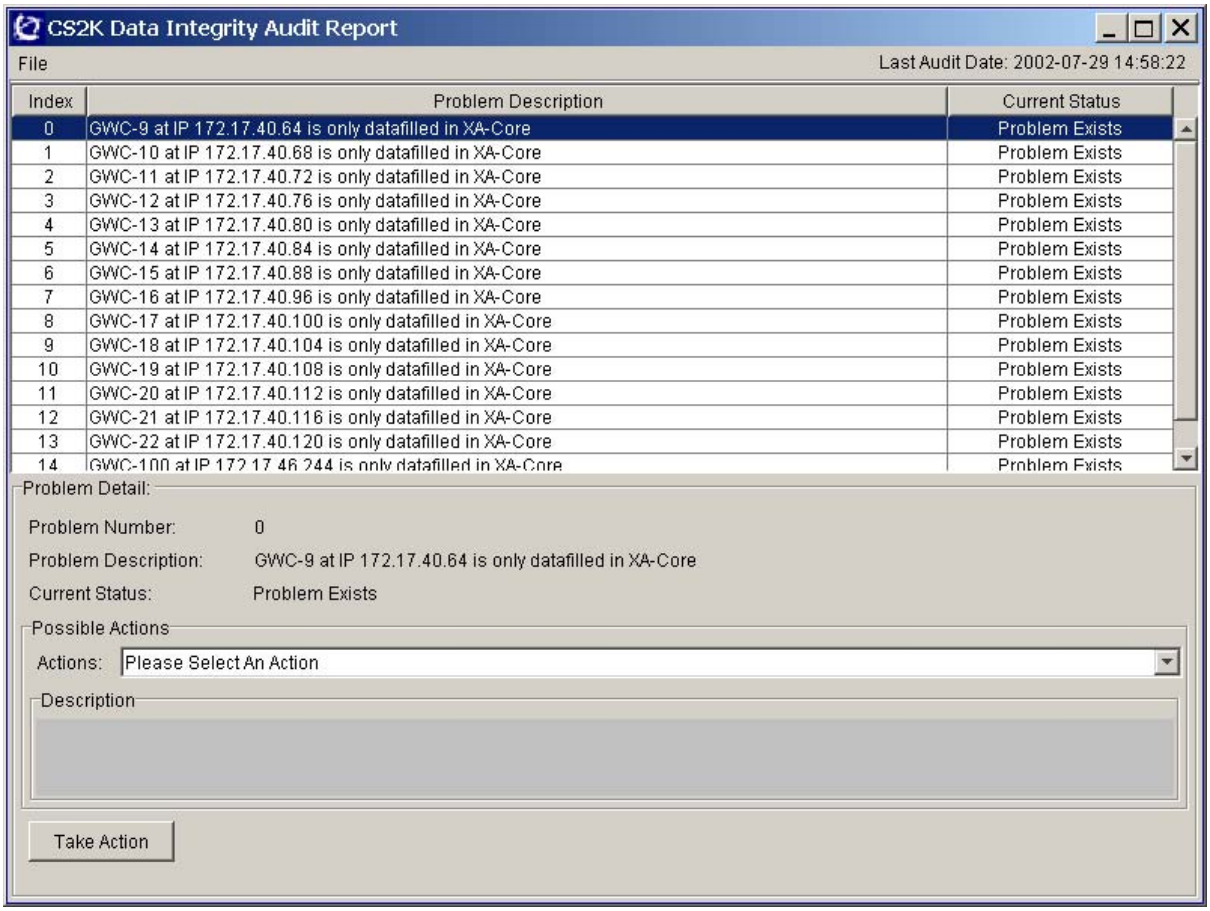
where
<date> is the date in yyyy-mm-dd format, for example, 2003-02-15.



c Click the **View Report** button.



The system displays the selected report. If no problems were discovered, the report will be empty. Here is an example of a report containing problems:



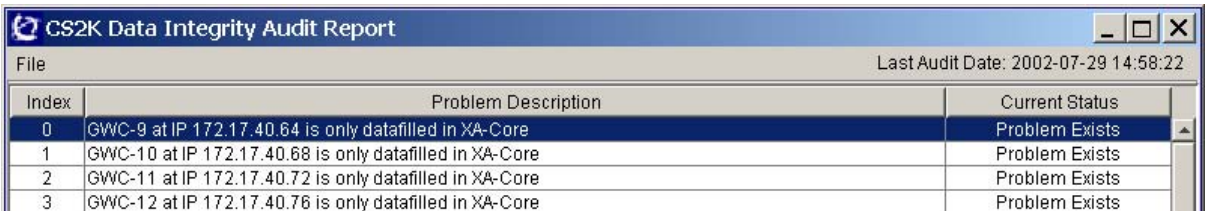
Note 1: The CS 2000 Management Tools server retains the most recent CS 2000 audit report. When a new audit occurs, the server deletes the previous report.

Note 2: The system places the audit report in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/MI2/apps/Audit.

Note 3: The CS 2000 GWC Manager does not provide an option to save a CS 2000 data audit report to local disk.

9 Review the results of the audit and click on a problem to resolve.

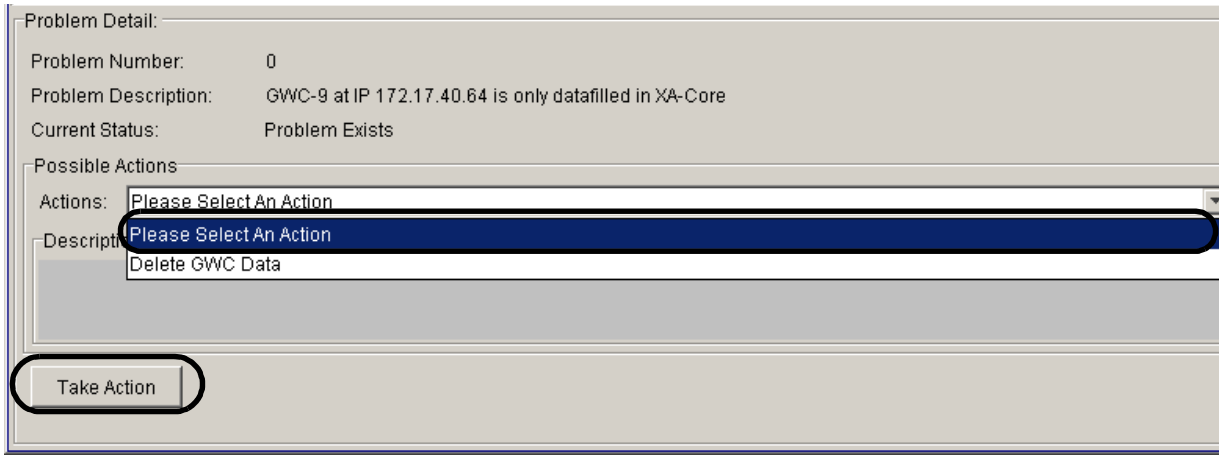
Note: If necessary, resize the entire window to completely view the Problem Description field.



10 Evaluate actions to resolve a problem and take action.

a Click and hold on the Action pull-down menu near the bottom of the screen to assess any possible actions.

b If appropriate, select an action. Read the description of the action and ensure that you observe any recommended steps or cautions.



c Click the **Take Action** button.

Note: If you see the message “Correction Failed”, please contact your next level of support.

11 Return to step 9 to review another problem.

12 Proceed as follows for a Line Data Integrity Audit:

If you want to view	Do
the line valid-data report	step 13
the line problem-data report	step 14

13 View the line valid-data report as follows:

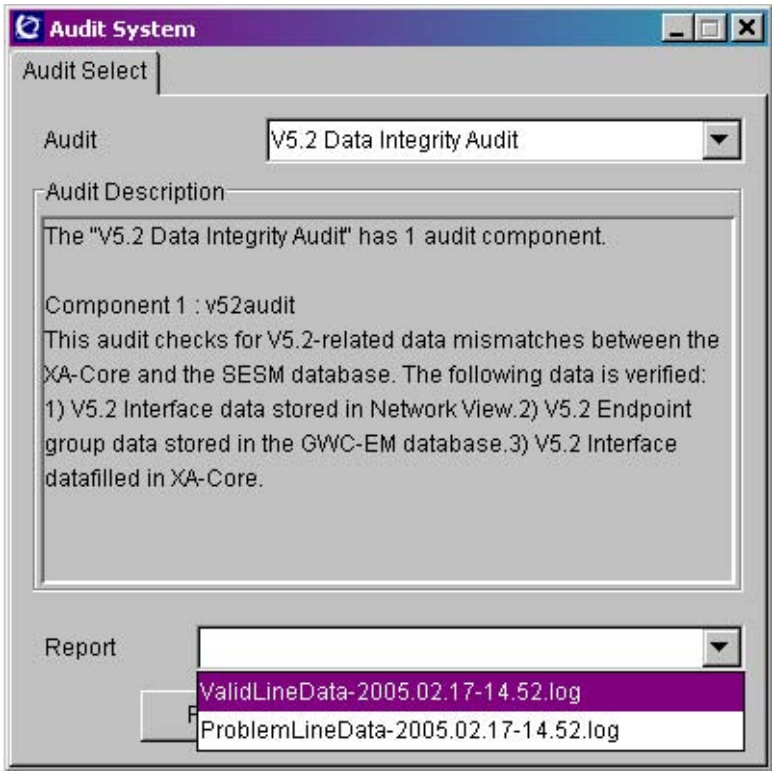
a Ensure that you have selected **Line Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

b Select **ValidLineData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ValidLineData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

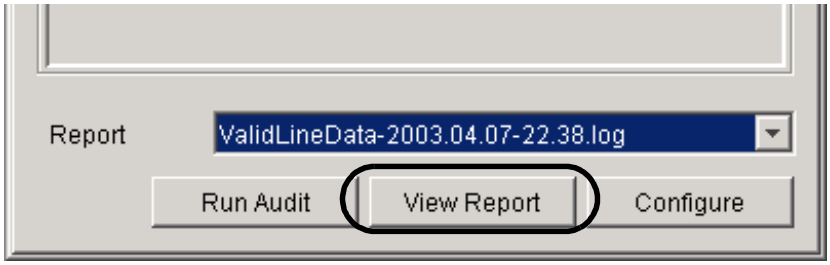
The file name has the following format:

ValidLineData-<date>-<time>.log

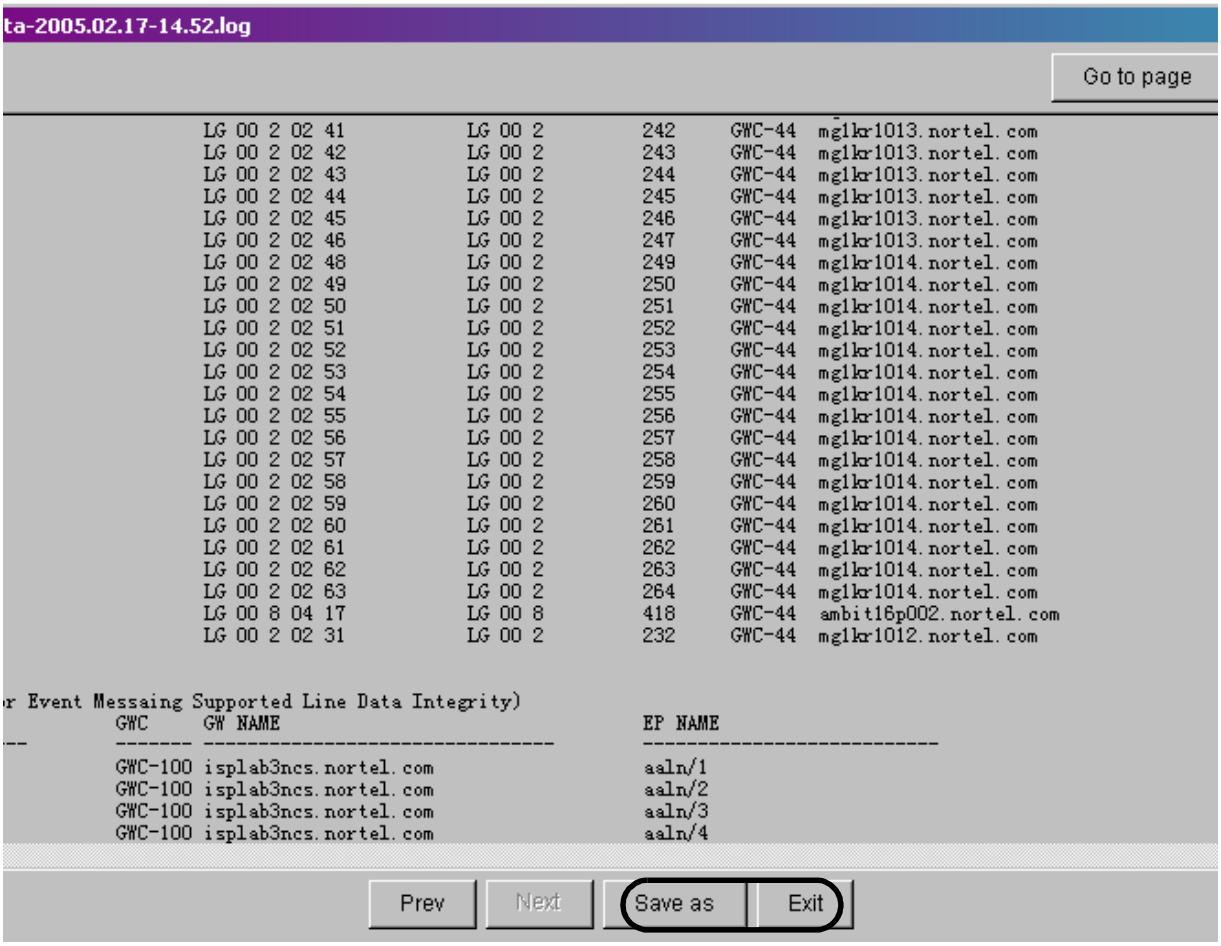
where
<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.
<time> is the time in hh.mm format, for example 17.30.



c Click **View Report**.



The system displays the selected report. Here is an example of a “ValidLineData” report.



Note 1: The CS 2000 Management Tools server retains the six most recent “ValidLineData” reports. When a new line audit occurs, the server deletes the oldest report.

Note 2: The system places valid data audit reports in the following directory on the CS 2000 Management Tools

server:
/opt/nortel/ptm/current/www/Audit/LineDataIntegrityAudit/.

d If you want to retain one of these reports for a longer time, or if you want to print a report, click the **Save as** button at the bottom of the screen. Then, save the report under a file name of your choice.

e To print a report you have saved, open the file using a text editor and print the file.

f After viewing the valid-data report, click the **Exit** button at the bottom of the screen.

14 View the line problem-data report as follows:

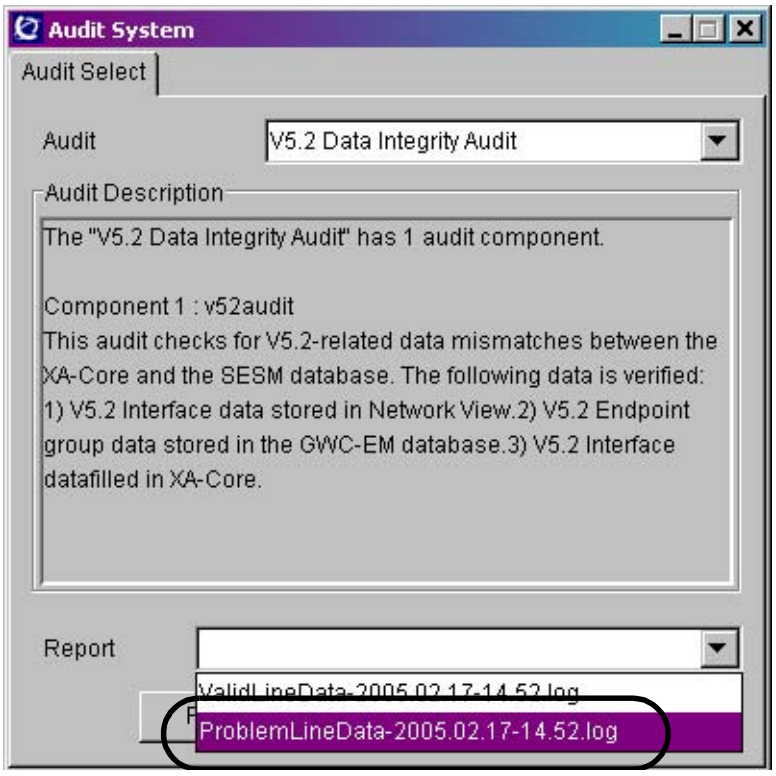
a Ensure that you have selected **Line Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

b Select **ProblemLineData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ProblemLineData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

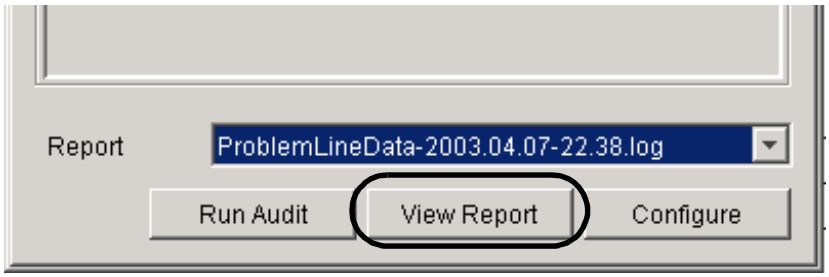
The file name has the following format:

ProblemLineData-<date>-<time>.log

where
<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.
<time> is the time in hh.mm format, for example 17.30.



c Click the **View Report** button.



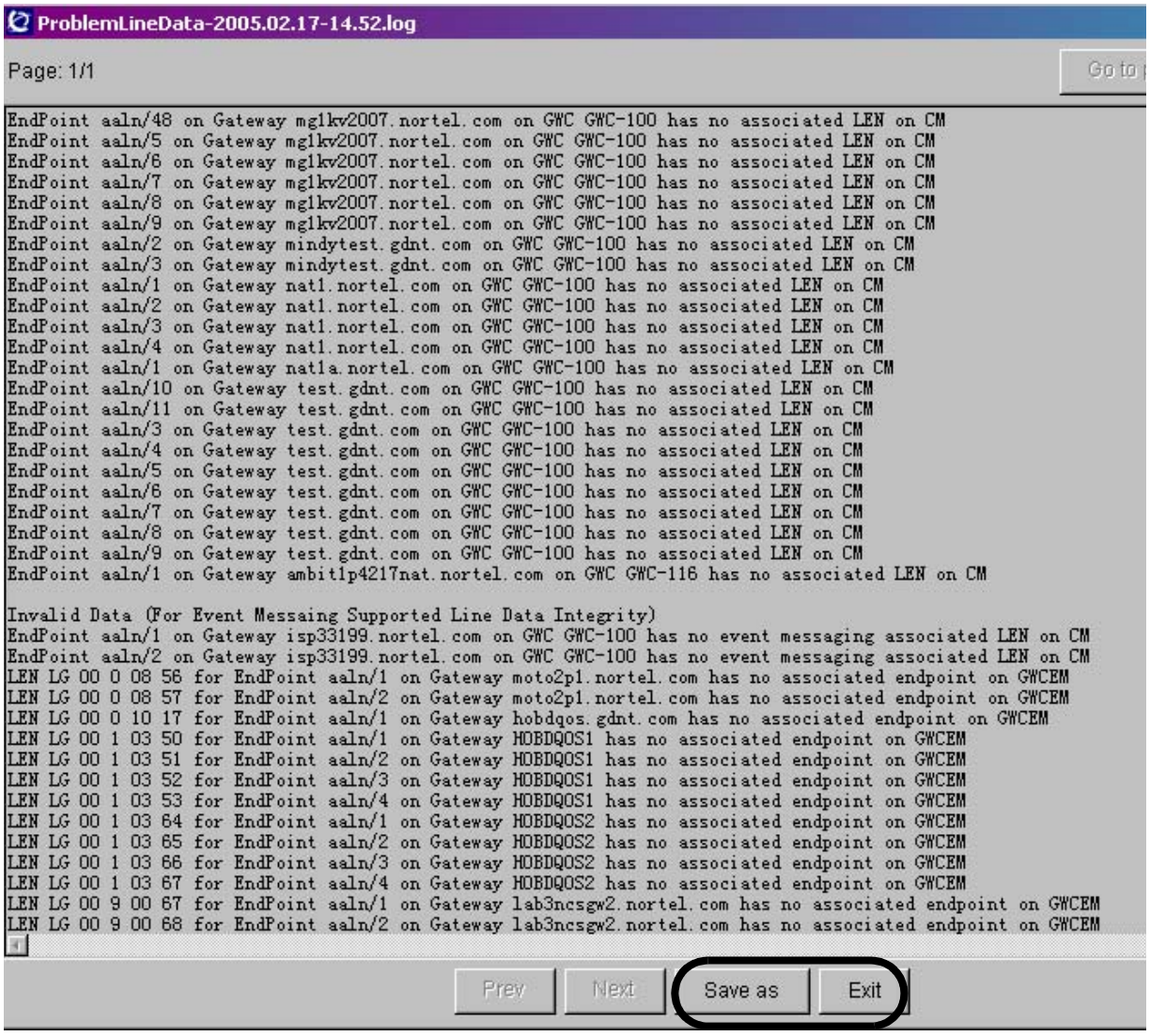
The system displays the selected report.

If the audit found no problems, the “Problem” report contains a message stating that no problems were found.

The “Problem” report produced by a line audit can contain messages in the following formats:

- DN <DN> for LEN <len> has no associated Endpoint on <GWC ID>.
- Endpoint <endpointname> on gateway <gatewayname> on GWC <GWCname> has no associated DN/LEN on CM.

Here is an example of a “ProblemLineData” report:



Note 1: The CS 2000 Management Tools server retains the six most recent “ProblemLineData” reports. When a new audit occurs, the server deletes the oldest report.

Note 2: The system places problem data audit reports in the following directory on the CS 2000 Management Tools server:
/opt/nortel/ptm/current/www/Audit/LineDataIntegrityAudit/.

d If you want to retain one of these reports for a longer time, or print a report, click the **Save as** button at the bottom of the screen. Then, save the report under a new file name.

e To print a report you have saved, open the file using a text editor and print the file.

f To correct the problems, refer to the printed copy of the report. You will need to delete and then reprovision the listed lines.

g After viewing the problem-data report, click the **Exit** button at the bottom of the viewer screen.

15 Proceed as follows for a Trunk Data Integrity Audit:

If you want to view	Do
the trunk valid-data report	step 16
the trunk problem-data report	step 17

16 View the trunk valid-data report as follows:

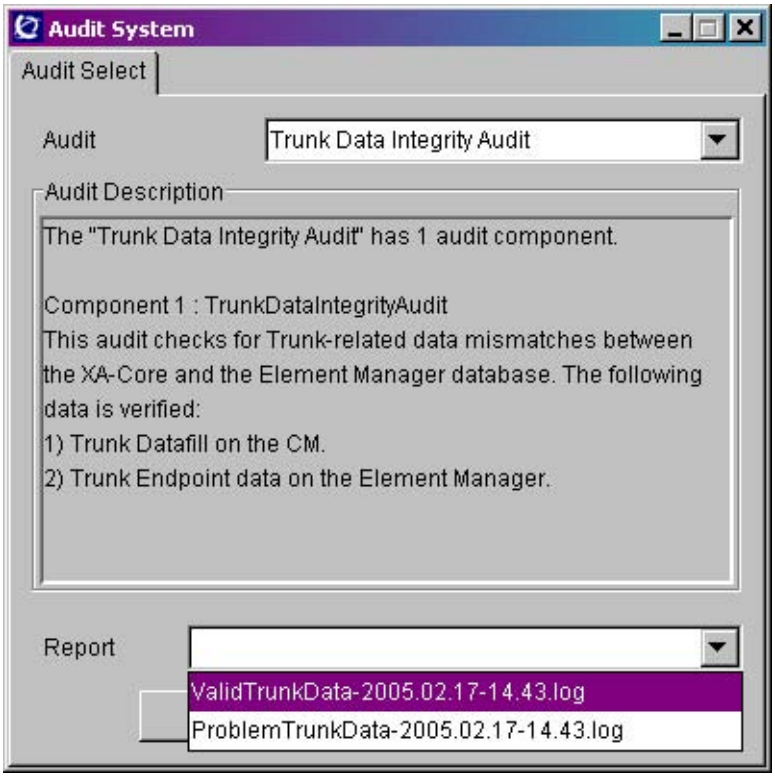
a Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

b Select **ValidTrunkData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ValidTrunkData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

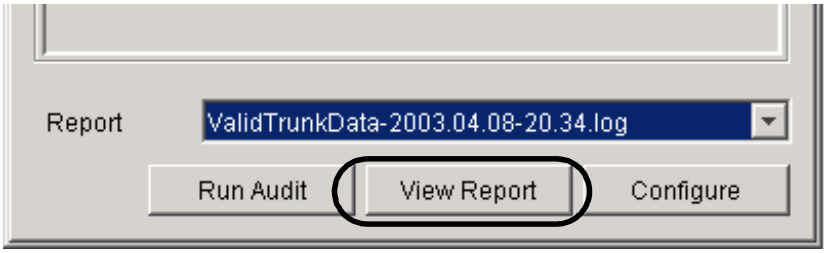
The file name has the following format:

ValidTrunkData-<date>-<time>.log

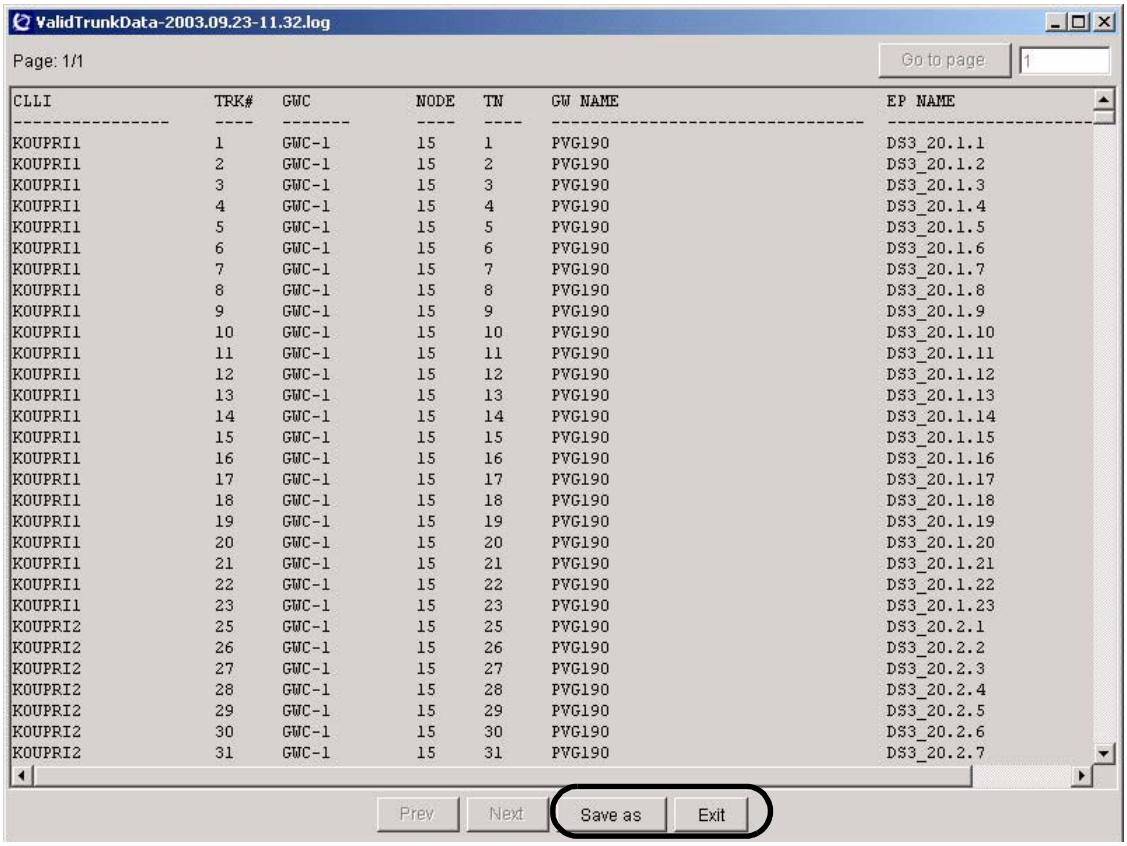
where
<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.
<time> is the time in hh.mm format, for example 17.30.



c Click **View Report**.



The system displays the selected report. Here is an example of a “ValidTrunkData” report.



CLLI	TRK#	GWC	NODE	TN	GW NAME	EP NAME
KOUPRI1	1	GWC-1	15	1	PVG190	DS3_20.1.1
KOUPRI1	2	GWC-1	15	2	PVG190	DS3_20.1.2
KOUPRI1	3	GWC-1	15	3	PVG190	DS3_20.1.3
KOUPRI1	4	GWC-1	15	4	PVG190	DS3_20.1.4
KOUPRI1	5	GWC-1	15	5	PVG190	DS3_20.1.5
KOUPRI1	6	GWC-1	15	6	PVG190	DS3_20.1.6
KOUPRI1	7	GWC-1	15	7	PVG190	DS3_20.1.7
KOUPRI1	8	GWC-1	15	8	PVG190	DS3_20.1.8
KOUPRI1	9	GWC-1	15	9	PVG190	DS3_20.1.9
KOUPRI1	10	GWC-1	15	10	PVG190	DS3_20.1.10
KOUPRI1	11	GWC-1	15	11	PVG190	DS3_20.1.11
KOUPRI1	12	GWC-1	15	12	PVG190	DS3_20.1.12
KOUPRI1	13	GWC-1	15	13	PVG190	DS3_20.1.13
KOUPRI1	14	GWC-1	15	14	PVG190	DS3_20.1.14
KOUPRI1	15	GWC-1	15	15	PVG190	DS3_20.1.15
KOUPRI1	16	GWC-1	15	16	PVG190	DS3_20.1.16
KOUPRI1	17	GWC-1	15	17	PVG190	DS3_20.1.17
KOUPRI1	18	GWC-1	15	18	PVG190	DS3_20.1.18
KOUPRI1	19	GWC-1	15	19	PVG190	DS3_20.1.19
KOUPRI1	20	GWC-1	15	20	PVG190	DS3_20.1.20
KOUPRI1	21	GWC-1	15	21	PVG190	DS3_20.1.21
KOUPRI1	22	GWC-1	15	22	PVG190	DS3_20.1.22
KOUPRI1	23	GWC-1	15	23	PVG190	DS3_20.1.23
KOUPRI2	25	GWC-1	15	25	PVG190	DS3_20.2.1
KOUPRI2	26	GWC-1	15	26	PVG190	DS3_20.2.2
KOUPRI2	27	GWC-1	15	27	PVG190	DS3_20.2.3
KOUPRI2	28	GWC-1	15	28	PVG190	DS3_20.2.4
KOUPRI2	29	GWC-1	15	29	PVG190	DS3_20.2.5
KOUPRI2	30	GWC-1	15	30	PVG190	DS3_20.2.6
KOUPRI2	31	GWC-1	15	31	PVG190	DS3_20.2.7

Note 1: The CS 2000 Management Tools server retains the six most recent “ValidTrunkData” reports. When a new trunk audit occurs, the server deletes the oldest report.

Note 2: The system places trunk audit reports in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/www/Audit/TrunkDataIntegrityAudit/.

d If you want to retain one of these reports for a longer time, or if you want to print a report, click **Save as** at the bottom of the screen. Then, save the report under a file name of your choice.

e To print a report you have saved, open the file using a text editor and print the file.

f After viewing the valid-data report, click **Exit** at the bottom of the screen.

17 View the trunk problem-data report as follows:

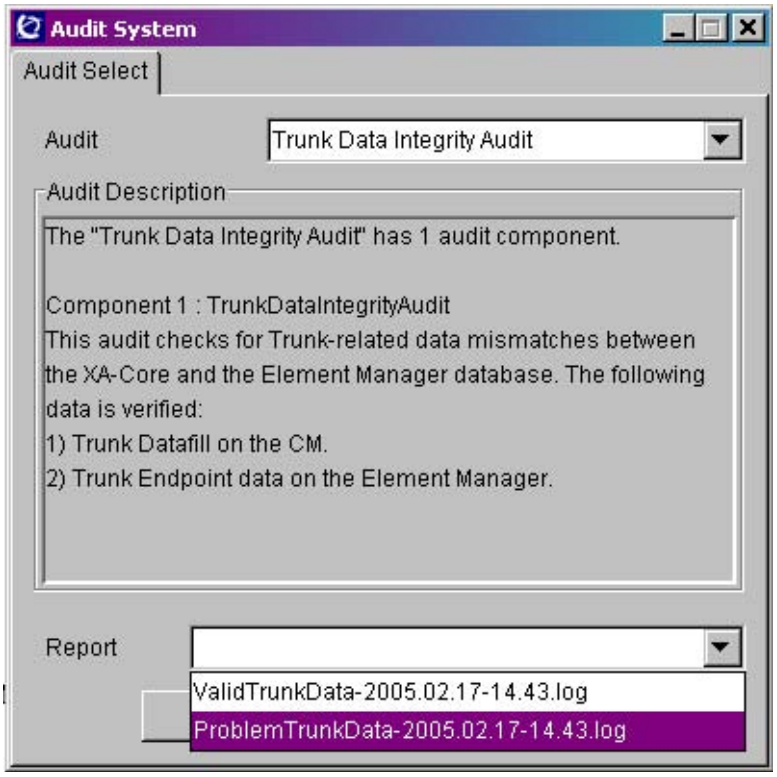
a Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit system dialog box.

b Select **ProblemTrunkData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ProblemTrunkData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

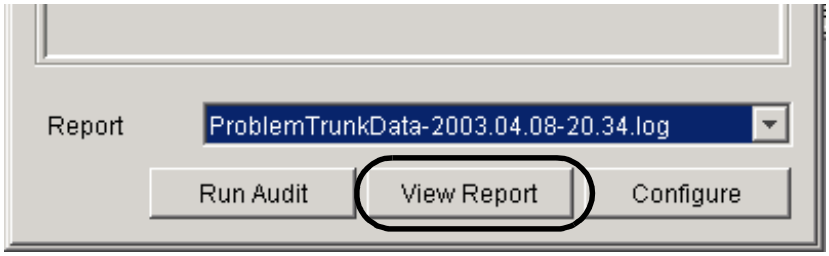
The file name has the following format:

ProblemTrunkData-<date>-<time>.log

where
<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.
<time> is the time in hh.mm format, for example 17.30.



c Click the **View Report** button.



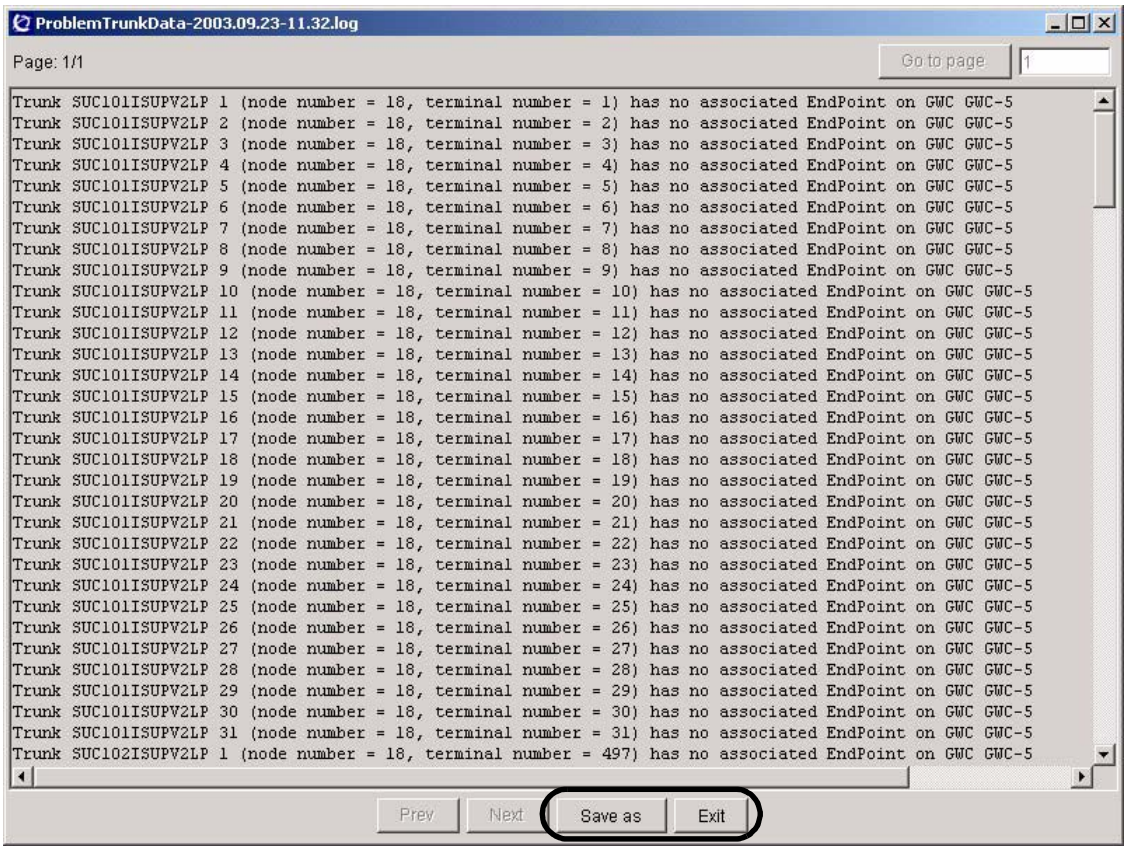
The system displays the selected report.

If the audit found no problems, the “Problem” report contains a message stating that no problems were found.

The “Problem” report produced by a trunk audit can contain messages in the following formats:

- Trunk <trunk name> (node number = <NODE>, terminal number = <TID>) has no associated Endpoint on GWC <GWC ID>.
- Endpoint <EP NAME> on gateway <GW NAME> (terminal number = <TID>) on GWC <GWC ID> has no associated trunk member datafilled on the CM.

Here is an example of a “ProblemTrunkData” report:



Note 1: The CS 2000 Management Tools server retains the six most recent “ProblemTrunkData” reports. When a new audit occurs, the server deletes the oldest report.

Note 2: The system places trunk audit reports in the following directory on the CS 2000 Management Tools server:
/opt/nortel/ptm/current/www/Audit/TrunkDataIntegrityAudit/.

d If you want to retain one of these reports for a longer time, or print a report, click **Save as** at the bottom of the screen. Then, save the report under a file name of your choice.

e To print a report you have saved, open the file using a text editor and print the file.

f To correct the problems, refer to the printed copy of the report. You will need to delete and then reprovision the listed trunks.

g After viewing the problem-data report, click **Exit** at the bottom of the viewer screen.

18 View a V5.2 audit report as follows:

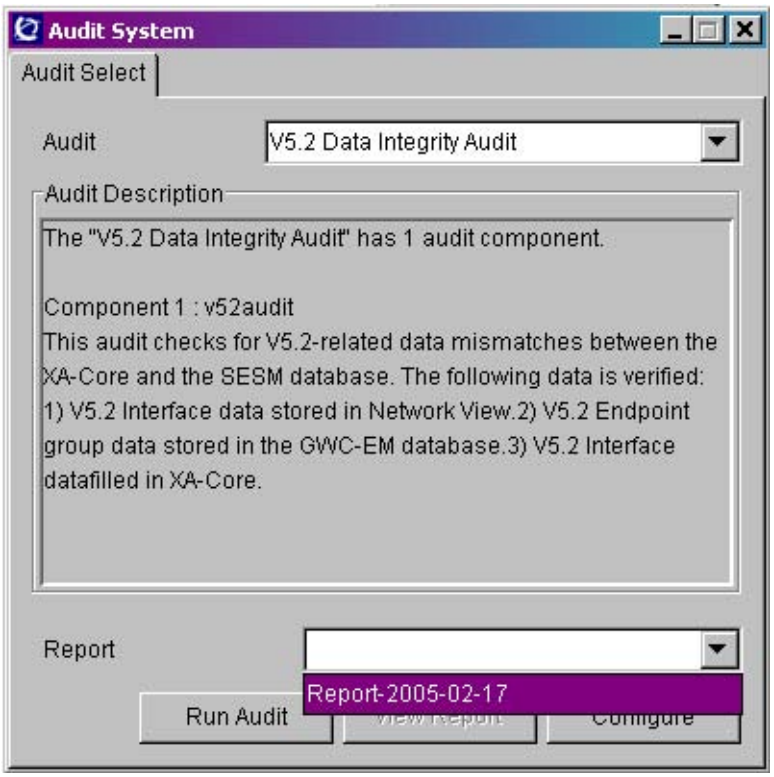
a Ensure that you have selected **V5.2 Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

b Select **Report** <date> from the pull-down menu in the Report field at the bottom of the dialog box.

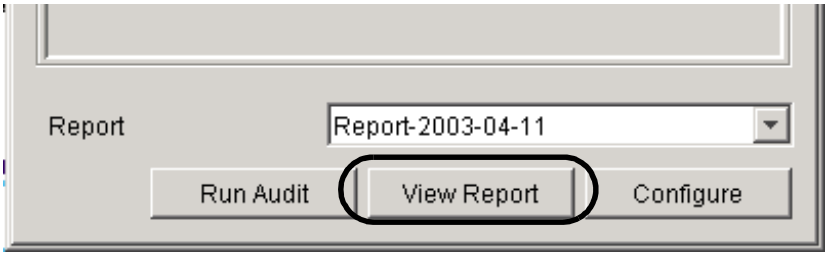
The file name has the following format:

Report-<date>

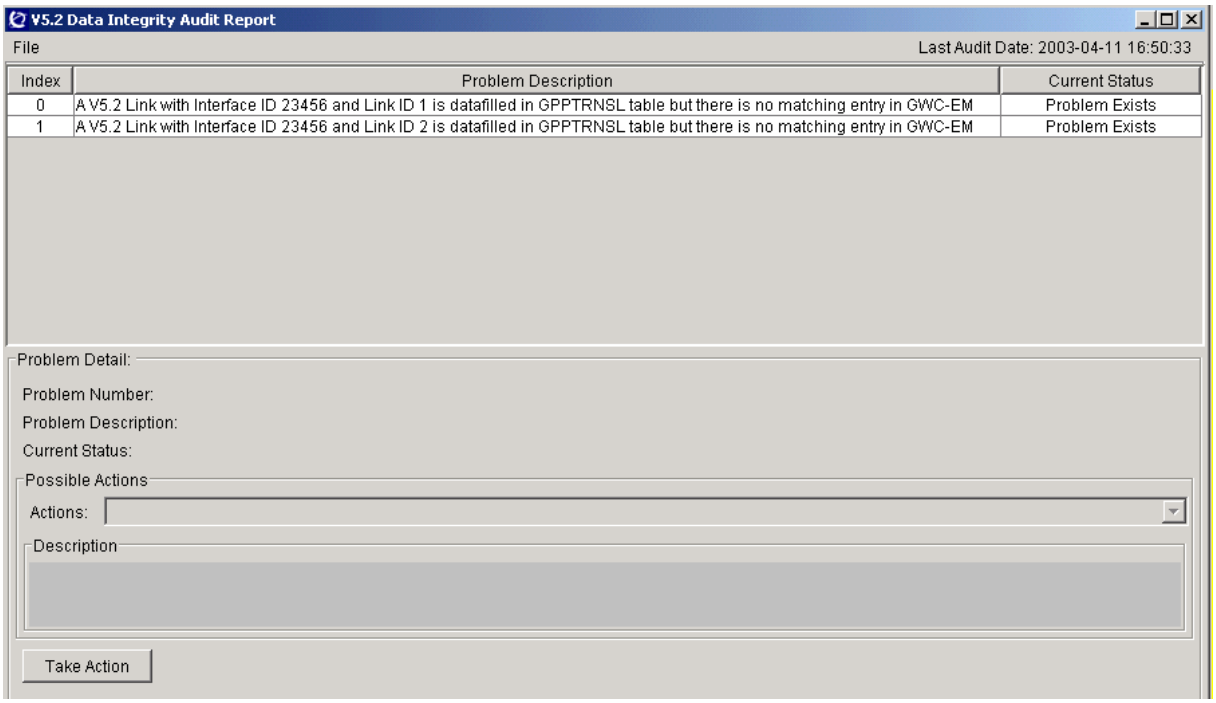
where
<date> is the date in yyyy-mm-dd format, for example, 2003-02-15.



c Click **View Report**.



The system displays the selected report. If no problems were discovered, the report will be empty. Here is an example of a report in which two problems were discovered:



Note 1: The CS 2000 Management Tools server retains the most recent V5.2 audit report. When a new audit occurs, the server deletes the previous report.

Note 2: The system places the audit report in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/MI2/apps/Audit.

Note 3: The CS 2000 GWC Manager does not provide an option to save a V5.2 audit report to local disk.

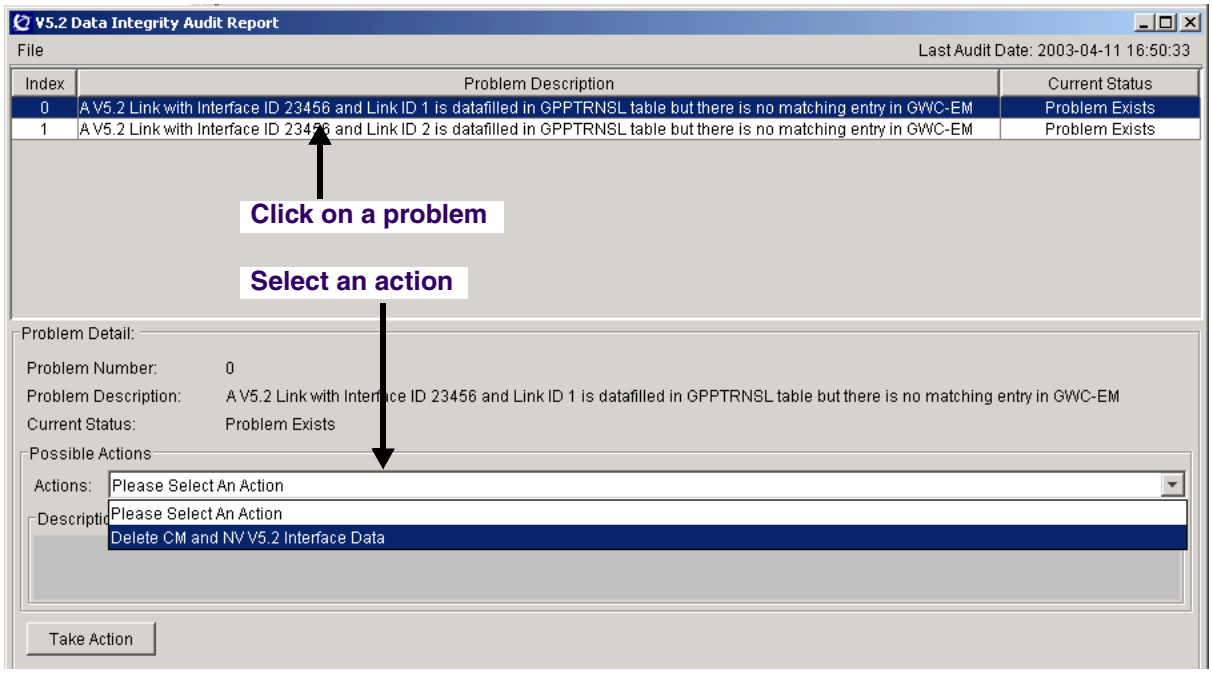
19 Review the results of the audit and click on a problem to resolve.

Note: If necessary, resize the entire window to completely view the Problem Description field.

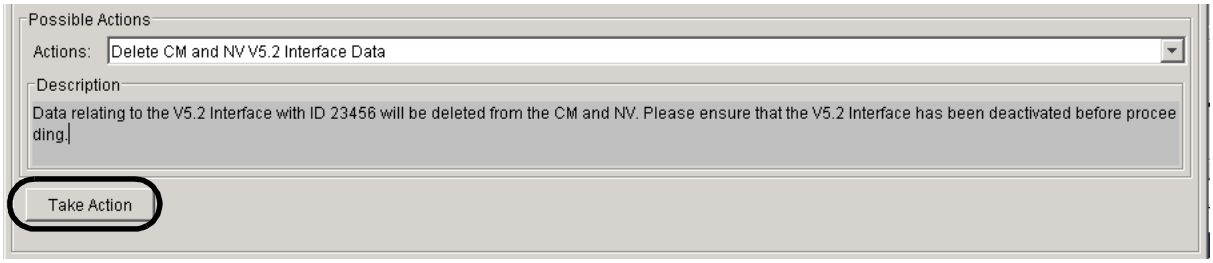
20 Evaluate actions to resolve a problem and take action.

a Click and hold on the Action pull-down menu near the bottom of the screen to assess any possible actions.

b If appropriate, select an action. Read the description of the action and ensure that you observe any recommended steps or cautions.



c Click **Take Action**.



Note: If you see the message “Correction Failed”, please contact your next level of support.

21 Return to step 19 to review another problem.

22 You have completed this procedure.

Performing a backup of APS audio files to tape

Application

Use this procedure to back up APS audio files to a 4mm Digital Audio Tape (DAT).

ATTENTION
This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure Performing a backup of APS audio files to CD or DVD on page 621.

Prerequisites

You need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the audio files.

Action

Perform the following steps to complete this procedure.

At the server

1 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides.

At the server console

2 Log in to the server through the console (port A) using the root user ID and password.

3 Rewind the tape by typing

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

and pressing the Enter key.

4 Change directories to the root filesystem by typing

```
# cd /
```

and pressing the Enter key.

5 Back up the APS audio files by typing

```
# /usr/ntdb/uas/scripts/backup_appl_data.sh
```

and pressing the Enter key.

Note: This command backs up file systems /PROV_data, /audio_files, and /user_audio_files.

6 Rewind the backup tape by typing

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

and pressing the Enter key.

7 To ensure that the backup was successful, list the content of the tape by typing

```
# tar tvf /dev/rmt/0c | more
```

and pressing the Enter key.

8 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen) to prevent the data on the tape from being accidentally over-written. Store the tape for later use.

9 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Performing a backup of APS audio files to CD or DVD

Application

Use this procedure to back up APS audio files to a CD or DVD, or move the backup of audio files to another server if the backup is more than 2 GB.

ATTENTION
This procedure only applies to a Sun Netra 240 server with a CD/DVD drive. Use procedure Performing a backup of APS audio files to tape on page 619 for a Sun t1400 server with a DAT drive.

Prerequisites

You need one blank CD-R, DVD-R, CD-RW or DVD-RW to store the data if the data is less than 2 GB. Otherwise you need a server accessible through FTP with adequate space to hold the data.

Note 1: The backup utility limits the storage to 2 GB on a DVD-R, or DVD-RW.

Note 2: If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

Action

ATTENTION
In a two-sever configuration, execute this procedure on the active server.

At the server

1 Insert a blank CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the active server.

At your workstation

2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server on which you are performing the backup

In a two-server configuration, enter the physical IP address of the active server.

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

5 When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing **ubmstat**. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

6 Change directories to the root file system by typing

```
# cd /
```

and pressing the Enter key.

7 Create a “tar” file of the APS audio files by typing

```
# tar cvf AudioFiles.tar /audio_files
/user_audio_files /opt/uas/uas_conf_backup
```

and pressing the Enter key.

Note: The above command is entered on one line, and includes a space between each directory.

8 Verify the size of the “AudioFiles.tar” file by typing

```
# ls -l AudioFiles.tar
```

and pressing the Enter key.

If the “AudioFiles.tar” file is	Do
under 2 GB	step 10
over 2 GB	step 9

9 Move the “AudioFiles.tar” file onto another server using File Transfer Protocol (FTP).

Proceed to step 13

10 Create a temporary directory by typing

```
# mkdir /tmp/.iso
```

and pressing the Enter key.

Note: The directory may already exist.

11 Backup the tar file of the APS audio files onto the CD or DVD by typing

```
# /opt/nortel/sspfs/bks/cdwrite AudioFiles.tar
```

and pressing the Enter key.

12 Remove the CD or DVD from the drive, label it, and store it in a safe place.

13 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Performing a backup of APS oracle data to tape

Application

Use this procedure to back up APS oracle data to a 4mm Digital Audio Tape (DAT).

ATTENTION
This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure Performing a backup of APS oracle data to CD or DVD on page 626.

Prerequisites

You need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the oracle data.

Action

Perform the following steps to complete this procedure.

At the server

1 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides.

At the server console

2 Log in to the server through the console (port A) using the root user ID and password.

3 Rewind the tape by typing

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

and pressing the Enter key.

4 Change directories to the root filesystem by typing

```
# cd /
```

and pressing the Enter key.

5 Back up the APS oracle files by typing

```
# ips_export_db.sh -t /dev/rmt/0 | tee
./export_log
```

and pressing the Enter key.

6 Rewind the backup tape by typing

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

and pressing the Enter key.

7 To ensure the backup was successful, list the content of the tape by typing

```
# tar tvf /dev/rmt/0c | more
```

and pressing the Enter key.

8 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen) to prevent the data on the tape from being accidentally over-written. Store the tape for later use.

9 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Performing a backup of APS oracle data to CD or DVD

Application

Use this procedure to back up APS oracle onto a CD or DVD.

ATTENTION
This procedure only applies to a Sun Netra 240 server with a CD/DVD drive. Use procedure Performing a backup of APS oracle data to tape on page 624 for a Sun t1400 server with a DAT drive.

Prerequisites

You need one blank CD-R, DVD-R, CD-RW or DVD-RW to store the data

Note 1: The backup utility limits the storage to 4 GB on a DVD-R, or DVD-RW.

Note 2: If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

Action

ATTENTION
In a two-sever configuration, execute this procedure on the active server.

At the server

1 Insert a blank CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the active server.

At your workstation

2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server on which you are performing the backup

Enter the physical IP address of the active server in a two-server configuration.

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 Back up the APS oracle data to hard disk by typing

```
# ips_export_db.sh -diskonly
```

and pressing the Enter key.

7 Change directories to where the backup is by typing

```
# cd /audio_files/aps_db_backup
```

and pressing the Enter key.

8 Create a tar file of the APS oracle files by typing

```
# tar cvf aps_oracle_bkup.tar *
```

and pressing the Enter key.

9 Verify the size of the “aps_oracle_bkup.tar ” file by typing

```
# ls -l aps_oracle_bkup.tar
```

and pressing the Enter key.

If the “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 Create a temporary directory by typing

```
# mkdir /tmp/.iso
```

and pressing the Enter key.

Note: The directory may already exist.

12 Backup the tar file of the APS oracle data onto the CD or DVD by typing

```
# /opt/nortel/sspfs/bks/cdwrite
aps_oracle_bkup.tar
```

and pressing the Enter key.

13 Remove the CD or DVD from the drive, label it, and store it in a safe place.

You have completed this procedure.

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. You can view log SPFS310 through the IEMS GUI or in file /var/log/customerlog on the server.

Note: For more information on logs, refer to the *Carrier Voice over IP 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 Log in 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.

Note: Ensure you are on the Inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

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.

You have completed this 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 or as an ISO image through Electronic Software Delivery (ESD).

The supported upgrade paths to the (I)SN08 release are listed below. Follow the link associated with the release you are upgrading from.

- Upgrading from (I)SN06.2 to (I)SN08 on page 633
- Upgrading from (I)SN07 to (I)SN08 on page 647
- Upgrading from (I)SN08 to (I)SN08 (maintenance release) on page 661

Upgrading from (I)SN06.2 to (I)SN08

The configurations that support an upgrade from (I)SN06.2 to (I)SN08 are listed below. Follow the link associated with your configuration.

- Sun Netra t1400 on page 634
- Sun Netra 240 one-server configuration on page 638
- Sun Netra 240 two-server configuration on page 642

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)SN08.

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)SN08.

ATTENTION

The SSPFS and all applications on the server 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

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

CAUTION
Potential for operational problems
Once you have upgraded the SSPFS, continue until you have upgraded all applications on that server. Failing to upgrade an application to the same release as the SSPFS will result in operational problems.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

(I)SN06.2 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
1	Upgrade the Succession Server Platform Foundation Software (SSPFS).		Perform procedure Upgrading SSPFS software on page 666.
2	Install any SSPFS MNCLs. ***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	Obtain any patches applicable to components on the CS 2000 Management Tools server (PSE, SAM21EM, NPM, SESM, QCA, SSPFS, IEMS, IEMSCSS, COREM).		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
4	Apply all SSPFS patches.		Perform procedure Applying patches using the NPM on page 1895.

(I)SN06.2 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
5	Apply all NPM patches and restart NPM. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Applying patches using the NPM on page 1895.
6	If you have a large office, abort any NPM tasks that are queued ahead of the NPM restart task. In a large office, the list of NPM tasks queued ahead of the NPM restart task, can be long and can take many hours to complete. Therefore, aborting NPM tasks is recommended in large offices to shorten the upgrade time. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Prioritizing a patching maintenance request using the NPM on page 2000.
7	Upgrade the CS 2000 Management (CS2M) components software.		If upgrading through Electronic Software Delivery (ESD), transfer the CS2M software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
8	If you upgraded through Electronic Software Delivery (ESD), unmount and remove the CS2M software load from the CS 2000 Management Tools server.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.

(I)SN06.2 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
9	As the root user, test the system configuration.		Type the following command: **> ptmctl diag** If the system prompts you to upgrade the SESM database, enter "1" to confirm you want to upgrade the SESM database.
10	Apply all patches that correspond to the following components on this server: PSE, SESM, SAM21 Manager, QCA, and NPM devices.		Perform procedure Applying patches using the NPM on page 1895.
11	Start the SESM and SAM21EM server applications.		Perform procedure Starting the SESM server application on page 751. Perform procedure Upgrading the CS2M software on page 713.
			Perform procedure Starting the SAM21 Manager server application on page 754.
12	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. ***Note:*** Only perform this activity if you have MG 9000 network elements in your network.		Perform procedure Stopping the PSE server application on an SSPFS-based server on page 778.
			Perform procedure Starting the PSE server application on an SSPFS-based server on page 780.

(I)SN06.2 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
13	If the APS is present on this server, upgrade the APS software.		If you are upgrading through Electronic Software Delivery (ESD), transfer the APS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading APS software on page 756.
14	If you upgraded through Electronic Software Delivery (ESD), unmount and remove the APS software load from the CS 2000 Management Tools server.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
15	If the IEMS is not in the network, neither on this server nor on a separate SSPFS-based server, and you want IEMS to co-reside with the CS 2000 Management Tools on this server, install the IEMS software. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Perform procedure Installing the Integrated EMS application on a SSPFS-based server on page 719.
16	Accept the upgraded environment on this server, or fallback.		Perform procedure Confirming the upgrade on an SSPFS-based server on page 764.
17	Complete the CS 2000 Management Tools upgrade.		Refer to Completing the CS 2000 Management Tools upgrade on page 782.

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.

CAUTION
Potential for operational problems
Once you have upgraded the SSPFS, continue until you have upgraded all applications on that server. Failing to upgrade an application to the same release as the SSPFS will result in operational problems.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

(I)SN06.2 to (I)SN08 (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 666.
2	Install any SSPFS MNCLs. ***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	Obtain any patches applicable to components on the CS 2000 Management Tools server (PSE, SAM21EM, NPM, SESM, QCA, SSPFS, IEMS, IEMSCSS, COREM).		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
4	Apply all SSPFS patches.		Perform procedure Applying patches using the NPM on page 1895.

(I)SN06.2 to (I)SN08 (Sun Netra 240 one-server) Upgrade checklist

	Activities	√	Procedures
5	Apply all NPM patches and restart NPM. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Applying patches using the NPM on page 1895.
6	If you have a large office, abort any NPM tasks that are queued ahead of the NPM restart task. In a large office, the list of NPM tasks queued ahead of the NPM restart task, can be long and can take many hours to complete. Therefore, aborting NPM tasks is recommended in large offices to shorten the upgrade time. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Prioritizing a patching maintenance request using the NPM on page 2000.
7	Upgrade the CS 2000 Management (CS2M) components software.		If upgrading through Electronic Software Delivery (ESD), transfer the CS2M software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
8	If you upgraded through Electronic Software Delivery (ESD), unmount and remove the CS2M software load from the CS 2000 Management Tools server.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.

(I)SN06.2 to (I)SN08 (Sun Netra 240 one-server) Upgrade checklist

	Activities	√	Procedures
9	As the root user, test the system configuration.		Type the following command: **> ptmctl diag** If the system prompts you to upgrade the SESM database, enter "1" to confirm you want to upgrade the SESM database.
10	Apply all patches that correspond to the following components on this server: PSE, SESM, SAM21 Manager, QCA, and NPM.		Perform procedure Applying patches using the NPM on page 1895.
11	Start the SESM and SAM21EM server applications.		Perform procedure Starting the SESM server application on page 751. Perform procedure Upgrading the CS2M software on page 713.
			Perform procedure Starting the SAM21 Manager server application on page 754.
12	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. ***Note:*** Only perform this activity if you have MG 9000 network elements in your network.		Perform procedure Stopping the PSE server application on an SSPFS-based server on page 778.
			Perform procedure Starting the PSE server application on an SSPFS-based server on page 780.

(I)SN06.2 to (I)SN08 (Sun Netra 240 one-server) Upgrade checklist

	Activities	√	Procedures
13	If the APS is present on this server, upgrade the APS software.		If you are upgrading through Electronic Software Delivery (ESD), transfer the APS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading APS software on page 756.
14	If you upgraded through Electronic Software Delivery (ESD), unmount and remove the APS software load from the CS 2000 Management Tools server.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
15	If the IEMS is not in the network, neither on this server nor on a separate SSPFS-based server, and you want IEMS to co-reside with the CS 2000 Management Tools on this server, install the IEMS software. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Perform procedure Installing the Integrated EMS application on a SSPFS-based server on page 719.
16	Accept the upgraded environment on this server, or fallback.		Perform procedure Confirming the upgrade on an SSPFS-based server on page 764.
17	Complete the CS 2000 Management Tools upgrade.		Refer to Completing the CS 2000 Management Tools upgrade on page 782.

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)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
On the ACTIVE server			
1	Remove the active server from the cluster.		Perform procedure Removing a server from a cluster on page 684.
On the INACTIVE server			
2	Upgrade the Succession Server Platform Foundation Software (SSPFS).		Perform procedure Upgrading SSPFS software on page 666.
3	Install any SSPFS MNCLs. ***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 all SSPFS patches. ***Note:*** Ensure that patches JFJ47OZ8, JFJ49OZ8, and LEX32OZ8 are applied on the unit which is being upgraded.		If the NPM is installed on a separate SSPFS-based server with the IEMS, perform procedure Applying patches using the NPM on page 1895. If the NPM is installed on this server, perform procedure Patching the inactive node of a cluster during an upgrade on page 737.
5	Apply all NPM patches. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Patching the inactive node of a cluster during an upgrade on page 737.

(I)SN06.2 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
6	Apply all PSE patches.		If the NPM is installed on a separate SSPFS-based server with the IEMS, perform procedure Applying patches using the NPM on page 1895. If the NPM is installed on this server, perform procedure Patching the inactive node of a cluster during an upgrade on page 737.
7	Upgrade the CS 2000 Management (CS2M) components software.		If upgrading through Electronic Software Delivery (ESD), transfer the CS2M software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the CS2M software on page 713.
8	If you upgraded through Electronic Software Delivery (ESD), unmount and remove the CS2M software load from the CS 2000 Management Tools server.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
9	Apply all patches that correspond to the following components on this server: SESM, SAM21EM, and QCA.		If the NPM is installed on a separate SSPFS-based server with the IEMS, perform procedure Applying patches using the NPM on page 1895. If the NPM is installed on this server, perform procedure Patching the inactive node of a cluster during an upgrade on page 737.

(I)SN06.2 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
10	If the IEMS is not in the network, neither on this server nor on a separate SSPFS-based server, and you want IEMS to co-reside with the CS 2000 Management Tools on this server, install the IEMS software. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Perform procedure Installing the Integrated EMS application on a SSPFS-based server on page 719.
On the ACTIVE server			
11	Return the active server to the cluster		Perform procedure Returning a server to a cluster on page 744.
On the INACTIVE server			
12	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. ***Note:*** Only perform this activity if you have MG 9000 network elements in your network.		Perform procedure Stopping the PSE server application on an SSPFS-based server on page 778.
			Perform procedure Starting the PSE server application on an SSPFS-based server on page 780.

(I)SN06.2 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
On the ACTIVE server			
13	Determine if the upgraded SN08 unit is missing the added alias entries required for the Central Security Server.		Type the following command: # grep unit.-priv0.sspfs.net /etc/hosts The entries have been removed if the command does not display the two example entries below. EXAMPLE: # grep unit.-priv0.sspfs.net /etc/hosts 192.168.47.1 unit0-priv0 unit0-priv0.sspfs.net 192.168.47.2 unit1-priv0 unit1-priv0.sspfs.net # **Note:** To restore the entries if they are missing in SN08, remove SSPFS patch LEX32OZ8 if applied and simply apply/reapply LEX32OZ8 to the system.
14	Stop the cluster.		Perform procedure Stopping a cluster on page 749.
On the newly ACTIVE server with (I)SN08 software			
15	If the APS is present on this server, upgrade the APS software.		If you are upgrading through Electronic Software Delivery (ESD), transfer the APS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading APS software on page 756.
16	If you upgraded through Electronic Software Delivery (ESD), unmount and remove the APS software load from the CS 2000 Management Tools server.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.

(I)SN06.2 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
17	Accept the upgraded environment on this server, or fallback.		Perform procedure Confirming the upgrade on an SSPFS-based server on page 764.
18	Clone the image of the upgraded server onto the other server. ***Note:*** Only perform this procedure at this point if you accepted the upgraded environment.		Perform procedure Cloning the image of one node in a cluster to the other node on page 766.
19	Complete the CS 2000 Management Tools upgrade.		Refer to Completing the CS 2000 Management Tools upgrade on page 782.

Upgrading from (I)SN07 to (I)SN08

The configurations that support an upgrade from (I)SN07 to (I)SN08 are listed below. Follow the link associated with your configuration.

- Sun Netra t1400 on page 648
- Sun Netra 240 one-server configuration on page 652
- Sun Netra 240 two-server configuration on page 656

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)SN08.

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)SN08.

ATTENTION

The SSPFS and all applications on the server 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

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

CAUTION
Potential for operational problems
Once you have upgraded the SSPFS, continue until you have upgraded all applications on that server. Failing to upgrade an application to the same release as the SSPFS will result in operational problems.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

(I)SN07 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
1	Upgrade the Succession Server Platform Foundation Software (SSPFS).		Perform procedure Upgrading SSPFS software on page 666.
2	Install any SSPFS MNCLs. ***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	Obtain any patches applicable to components on the CS 2000 Management Tools server (PSE, SAM21EM, NPM, SESM, QCA, SSPFS, IEMS, IEMSCSS, COREM).		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
4	Apply all SSPFS patches.		Perform procedure Applying patches using the NPM on page 1895.

(I)SN07 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
5	Apply all NPM patches and restart the NPM. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Applying patches using the NPM on page 1895.
6	If you have a large office, abort any NPM tasks that are queued ahead of the NPM restart task. In a large office, the list of NPM tasks queued ahead of the NPM restart task, can be long and can take many hours to complete. Therefore, aborting NPM tasks is recommended in large offices to shorten the upgrade time. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Prioritizing a patching maintenance request using the NPM on page 2000.
7	Apply all PSE patches and restart PSE.		Perform procedure Applying patches using the NPM on page 1895.
8	If prior to starting the upgrade, PAM Radius was configured on this server, reconfigure it. PAM Radius uses the IEMS central security server for authentication. ***Note:*** Only perform this activity on the CS 2000 Management Tools server if the IEMS is installed on a separate SSPFS-based server. This configures this server as a radius client of the IEMS centralized security server.		Perform procedure Configuring an SSPFS-based client server to use PAM Radius on page 693.

(I)SN07 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
9	If the IEMS is present on this server, upgrade the IEMS software. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		If you are upgrading through Electronic Software Delivery (ESD), transfer the IEMS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the Integrated EMS software on page 700.
			Perform procedure Completing the Integrated EMS software upgrade on page 706.
10	Upgrade the CS 2000 Management (CS2M) components software.		If upgrading through Electronic Software Delivery (ESD), transfer the CS2M software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the CS2M software on page 713.
11	If you upgraded CS2M through Electronic Software Delivery (ESD), unmount and remove the CS2M iso image file.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
12	Apply all patches that correspond to the following components on this server: SESM, SAM21EM, and QCA.		Perform procedure Applying patches using the NPM on page 1895.
13	Start the SESM and SAM21EM server applications.		Perform procedure Starting the SESM server application on page 751.
			Perform procedure Starting the SAM21 Manager server application on page 754.

(I)SN07 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
14	If the APS is present on this server, upgrade the APS software.		If you are upgrading through Electronic Software Delivery (ESD), transfer the APS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading APS software on page 756.
15	If you upgraded APS, and you upgraded through Electronic Software Delivery (ESD), unmount and remove the APS iso image file.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
16	If the IEMS is not in the network, neither on this server nor on a separate SSPFS-based server, and you want IEMS to co-reside with the CS 2000 Management Tools on this server, install the IEMS software. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Perform procedure Installing the Integrated EMS application on a SSPFS-based server on page 719.
17	Accept the upgraded environment on this server, or fallback.		Perform procedure Confirming the upgrade on an SSPFS-based server on page 764.
18	Complete the CS 2000 Management Tools upgrade.		Refer to Completing the CS 2000 Management Tools upgrade on page 782.

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.

CAUTION
Potential for operational problems
Once you have upgraded the SSPFS, continue until you have upgraded all applications on that server. Failing to upgrade an application to the same release as the SSPFS will result in operational problems.

Use this table as a checklist, and place a check (√) in the √column as you complete each procedure.

(I)SN07 to (I)SN08 (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 666.
2	Install any SSPFS MNCLs. ***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	Obtain any patches applicable to components on the CS 2000 Management Tools server (PSE, SAM21EM, NPM, SESM, QCA, SSPFS, IEMS, IEMSCSS, COREM).		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
4	Apply all SSPFS patches.		Perform procedure Applying patches using the NPM on page 1895.

(I)SN07 to (I)SN08 (Sun Netra 240 one-server) Upgrade checklist

	Activities	√	Procedures
5	Apply all NPM patches and restart the NPM. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Applying patches using the NPM on page 1895.
6	If you have a large office, abort any NPM tasks that are queued ahead of the NPM restart task. In a large office, the list of NPM tasks queued ahead of the NPM restart task, can be long and can take many hours to complete. Therefore, aborting NPM tasks is recommended in large offices to shorten the upgrade time. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Prioritizing a patching maintenance request using the NPM on page 2000.
7	Apply all PSE patches and restart PSE.		Perform procedure Applying patches using the NPM on page 1895.
8	If prior to starting the upgrade, PAM Radius was configured on this server, reconfigure it. PAM Radius uses the IEMS central security server for authentication. ***Note:*** Only perform this activity on the CS 2000 Management Tools server if the IEMS is installed on a separate SSPFS-based server. This configures this server as a radius client of the IEMS centralized security server.		Perform procedure Configuring an SSPFS-based client server to use PAM Radius on page 693.

(I)SN07 to (I)SN08 (Sun Netra 240 one-server) Upgrade checklist

	Activities	√	Procedures
9	If the IEMS is present on this server, upgrade the IEMS software. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		If you are upgrading through Electronic Software Delivery (ESD), transfer the IEMS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the Integrated EMS software on page 700.
			Perform procedure Completing the Integrated EMS software upgrade on page 706.
10	Upgrade the CS 2000 Management (CS2M) components software.		If upgrading through Electronic Software Delivery (ESD), transfer the CS2M software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the CS2M software on page 713.
11	If you upgraded CS2M through Electronic Software Delivery (ESD), unmount and remove the CS2M iso image file.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
12	Apply all patches that correspond to the following components on this server: SESM, SAM21EM, and QCA.		Perform procedure Applying patches using the NPM on page 1895 .
13	Start the SESM and SAM21EM server applications.		Perform procedure Starting the SESM server application on page 751.
			Perform procedure Starting the SAM21 Manager server application on page 754.

(I)SN07 to (I)SN08 (Sun Netra 240 one-server) Upgrade checklist

	Activities	√	Procedures
14	If the APS is present on this server, upgrade the APS software.		If you are upgrading through Electronic Software Delivery (ESD), transfer the APS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading APS software on page 756.
15	If you upgraded APS, and you upgraded through Electronic Software Delivery (ESD), unmount and remove the APS iso image file.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
16	If the IEMS is not in the network, neither on this server nor on a separate SSPFS-based server, and you want IEMS to co-reside with the CS 2000 Management Tools on this server, install the IEMS software. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Perform procedure Installing the Integrated EMS application on a SSPFS-based server on page 719.
17	Accept the upgraded environment on this server, or fallback.		Perform procedure Confirming the upgrade on an SSPFS-based server on page 764.
18	Complete the CS 2000 Management Tools upgrade.		Refer to Completing the CS 2000 Management Tools upgrade on page 782.

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)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
On the INACTIVE server			
1	Remove the inactive server from the cluster.		Perform procedure Removing a server from a cluster on page 684.
2	Upgrade the Succession Server Platform Foundation Software (SSPFS).		Perform procedure Upgrading SSPFS software on page 666.
3	Install any SSPFS MNCLs. ***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 all SSPFS patches. ***Note:*** Ensure that patches JFJ47OZ8, JFJ49OZ8, and LEX32OZ8 are applied on the unit which is being upgraded.		If the NPM is installed on a separate SSPFS-based server with the IEMS, perform procedure Applying patches using the NPM on page 1895. If the NPM is installed on this server, perform procedure Patching the inactive node of a cluster during an upgrade on page 737.
5	Apply all NPM patches. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Patching the inactive node of a cluster during an upgrade on page 737.

(I)SN07 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
6	Apply all PSE patches.		If the NPM is installed on a separate SSPFS-based server with the IEMS, perform procedure Applying patches using the NPM on page 1895. If the NPM is installed on this server, perform procedure Patching the inactive node of a cluster during an upgrade on page 737.
7	If prior to starting the upgrade, PAM Radius was configured on this server, reconfigure it. PAM Radius uses the IEMS central security server for authentication. ***Note:*** Only perform this activity on the CS 2000 Management Tools server if the IEMS is installed on a separate SSPFS-based server. This configures this server as a radius client of the IEMS centralized security server.		Perform procedure Configuring an SSPFS-based client server to use PAM Radius on page 693.
8	If the IEMS is present on this server, upgrade the IEMS software. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		If you are upgrading through Electronic Software Delivery (ESD), transfer the IEMS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the Integrated EMS software on page 700.

(I)SN07 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
9	Upgrade the CS 2000 Management (CS2M) components software.		If upgrading through Electronic Software Delivery (ESD), transfer the CS2M software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the CS2M software on page 713.
10	If you upgraded CS2M through Electronic Software Delivery (ESD), unmount and remove the CS2M iso image file.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
11	Apply all patches that correspond to the following components on this server: SESM, SAM21EM, QCA.		Perform procedure Patching the inactive node of a cluster during an upgrade on page 737.
12	Return the inactive server to the cluster.		Perform procedure Returning a server to a cluster on page 744.
13	If the IEMS is not in the network, neither on this server nor on a separate SSPFS-based server, and you want IEMS to co-reside with the CS 2000 Management Tools on this server, install the IEMS software. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Perform procedure Installing the Integrated EMS application on a SSPFS-based server on page 719.

(I)SN07 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
On the ACTIVE server			
14	Stop the cluster. ***Note:*** Skip this activity if you just installed IEMS, since during the IEMS install, the server with the (I)SN08 software became the newly active server.		Perform procedure Stopping a cluster on page 749.
On the newly ACTIVE server with (I)SN08 software			
15	If you upgraded the IEMS on this server, complete the IEMS software upgrade. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Perform procedure Completing the Integrated EMS software upgrade on page 706.
16	Determine if the upgraded SN08 unit is missing the added alias entries required for the Central Security Server.		Type the following command: # grep unit.-priv0.sspfs.net /etc/hosts The entries have been removed if the command does not display the two example entries below. EXAMPLE: # grep unit.-priv0.sspfs.net /etc/hosts 192.168.47.1 unit0-priv0 unit0-priv0.sspfs.net 192.168.47.2 unit1-priv0 unit1-priv0.sspfs.net # **Note:** To restore the entries if they are missing in SN08, remove SSPFS patch LEX32OZ8 if applied and simply apply/reapply LEX32OZ8 to the system.

(I)SN07 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
17	If the APS is present on this server, upgrade the APS software.		If you are upgrading through Electronic Software Delivery (ESD), transfer the APS software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading APS software on page 756.
18	If you upgraded APS, and you upgraded through Electronic Software Delivery (ESD), unmount and remove the APS iso image file.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
19	Accept the upgraded environment on this server, or fallback.		Perform procedure Confirming the upgrade on an SSPFS-based server on page 764.
20	Clone the image of the upgraded server onto the other server. ***Note:*** Only perform this procedure at this point if you accepted the upgraded environment.		Perform procedure Cloning the image of one node in a cluster to the other node on page 766.
21	Complete the CS 2000 Management Tools upgrade.		Refer to Completing the CS 2000 Management Tools upgrade on page 782.

Upgrading from (I)SN08 to (I)SN08 (maintenance release)

The configurations that support an upgrade from (I)SN08 to (I)SN08 are listed below. Follow the link associated with your configuration.

- Sun Netra t1400 on page 661
- Sun Netra 240 one-server configuration on page 663
- Sun Netra 240 two-server configuration on page 664

ATTENTION

The SSPFS and all applications on the server 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

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)SN08 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
1	Stop the SESM and SAM21EM server applications.		Perform procedure Stopping the SESM server application on page 689.
			Perform procedure Stopping the SAM21 Manager server application on page 691.
2	Upgrade the CS 2000 Management (CS2M) components software.		If upgrading through Electronic Software Delivery (ESD), transfer the CS2M software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the CS2M software on page 713.

(I)SN08 to (I)SN08 (Sun Netra t1400) Upgrade checklist

	Activities	√	Procedures
3	If you upgraded through Electronic Software Delivery (ESD), unmount and remove the CS2M software load from the CS 2000 Management Tools server.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
4	Apply all patches that correspond to the following components on this server: SESM, SAM21EM, and QCA.		Perform procedure Applying patches using the NPM on page 1895.
5	Start the SESM and SAM21EM server applications.		Perform procedure Starting the SESM server application on page 751.
			Perform procedure Starting the SAM21 Manager server application on page 754.

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)SN08 to (I)SN08 (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 689.
			Perform procedure Stopping the SAM21 Manager server application on page 691.
2	Upgrade the CS 2000 Management (CS2M) components software.		If upgrading through Electronic Software Delivery (ESD), transfer the CS2M software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the CS2M software on page 713.
3	If you upgraded through Electronic Software Delivery (ESD), unmount and remove the CS2M software load from the CS 2000 Management Tools server.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
4	Apply all patches that correspond to the following components on this server: SESM, SAM21EM, and QCA.		Perform procedure Applying patches using the NPM on page 1895.
5	Start the SESM and SAM21EM server applications.		Perform procedure Starting the SESM server application on page 751.
			Perform procedure Starting the SAM21 Manager server application on page 754.

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)SN08 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
On the INACTIVE server			
1	Remove the Inactive server from the cluster		Perform procedure Removing a server from a cluster on page 684.
2	Upgrade the CS 2000 Management (CS2M) components software.		If upgrading through Electronic Software Delivery (ESD), transfer the CS2M software load from the drop box on the repository server to this server, and mount it using procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.
			Perform procedure Upgrading the CS2M software on page 713.
3	If you upgraded through Electronic Software Delivery (ESD), unmount and remove the CS2M software load from the CS 2000 Management Tools server.		Perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.
4	Apply all patches that correspond to the following components on this server: SESM, SAM21EM, and QCA.		Perform procedure Applying patches using the NPM on page 1895.
5	Return the Inactive server to the cluster		Perform procedure Returning a server to a cluster on page 744.
On the ACTIVE server			
6	Stop the cluster.		Perform procedure Stopping a cluster on page 749.

(I)SN08 to (I)SN08 (Sun Netra 240 two-server) Upgrade checklist

	Activities	√	Procedures
On the newly ACTIVE server with (I)SN08 maintenance release software			
7	Determine if the upgraded SN08 unit is missing the added alias entries required for the Central Security Server.		Type the following command: # grep unit.-priv0.sspfs.net /etc/hosts The entries have been removed if the command does not display the two example entries below. EXAMPLE: # grep unit.-priv0.sspfs.net /etc/hosts 192.168.47.1 unit0-priv0 unit0-priv0.sspfs.net 192.168.47.2 unit1-priv0 unit1-priv0.sspfs.net # **Note:** To restore the entries if they are missing in SN08, remove SSPFS patch LEX32OZ8 if applied and simply apply/reapply LEX32OZ8 to the system.
Note: At this point, you can easily revert this upgraded server back to the previous release. Continuing with this procedure, clones the image of the upgraded server onto the server running the previous release, and once both servers are upgraded, reverting back to the previous release will require a full system restore.			
8	Clone the image of the upgraded server onto the other server.		Perform procedure Cloning the image of one node in a cluster to the other node on page 766.

Upgrading SSPFS software

Application

Use this procedure to upgrade the SSPFS software on a Sun Netra t1400 or Sun Netra 240 from (I)SN06.2 or (I)SN07 to the (I)SN08 release.

Prerequisites

This procedure has the following prerequisites:

- Ensure you have SSPFS Disk 1, SSPFS Disk 2, and SSPFS Disk 3 for the (I)SN08 release.
- Ensure you have backed up your Oracle data and file systems before proceeding with this procedure. If required, refer to the following procedures:
  - — Performing a backup of oracle data on an SSPFS-based server on page 566
  - — Performing a backup of file systems on an SSPFS-based server on page 572

  Note: Backing up the Oracle data is not applicable on an SSPFS-based server that is hosting the Core Billing Manager (CBM).

- 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 563.

  Note: It is not necessary to verify the group IDs or user IDs on an SSPFS-based server that is hosting the Core and Billing Manager (CBM).

- Ensure the site spec book is available with IP addresses, hostnames, and non-system logins.

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.

> ***Note:*** In a two-server configuration, ensure you are on the Inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

At the server

2 Insert “SSPFS Disk 1” into the drive.

At the server console

3 Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

4 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.

The execution of this step takes approximately 5 minutes to complete on a Netra t1400, and 3 minutes on a Netra 240. These completion times for the execution of the pre-upgrade script are averages and can vary based on such factors as machine load.

> ***Note:*** Once the pre_upgrade process is complete, the disks will no longer be in redundant mode, and log SPFS310 will be generated indicating disk or disk mirroring errors. This is an expected condition during an upgrade, and no action is required.

5 Start the upgrade process by typing

```
# /liveupgrade.ksh
```

and pressing the Enter key.

If prompted, accept the specified device as the boot device by typing

```
yes
```

and pressing the Enter key.

Note: The execution of this step takes approximately 120 minutes to complete on a Netra t1400, and 60 minutes on a Netra 240 depending on the system configuration. However, during this time, the server is fully functional and applications can be used.

Once this step completes, the system will eject SSPFS Disk 1 and prompt you to insert SSPFS Disk 2.

At the server

6 Remove “SSPFS Disk 1” from the CD ROM drive, and insert “SSPFS Disk 2”.

At the server console

7 When ready, indicate you want to proceed by typing

```
# ok
```

and pressing the Enter key

Note: The execution of this step takes approximately 35 minutes to complete on a Netra t1400, and 25 minutes on a Netra 240 depending on the system configuration.

Once this step completes, the system will eject SSPFS Disk 2 and prompt you to insert SSPFS Disk 3.

At the server

8 Remove “SSPFS Disk 2” from the CD ROM drive, and insert “SSPFS Disk 3”.

At the server console

9 When ready, indicate you want to proceed by typing

```
# ok
```

and pressing the Enter key

Note: The execution of this step takes approximately 165 minutes to complete on a Netra t1400, and 75 minutes on a Netra 240 depending on the system configuration.

10 Use the following table to determine your next step.

If you	Do
are prompted with "Please select the software delivery method that is being used for the CBM load?	continue with Procedure for upgrading a CBM 850 on page 462 to upgrade the Core Billing Manager (CBM)
are not prompted with "Please select the software delivery method that is being used for the CBM load?	step 11

11 Wait until the upgraded server fully comes up from the boot before you proceed.

12 Log back in to the server using the root user ID and password.

13 Verify that your system is running the SN08 version of the SSPFS as follows:

Note: You must be the root user to execute the steps that follow.

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 - exist

select -
```

b Enter the number next to the “View” option in the menu.

Example response

```
View
 1 - sspfs_soft (Display Software
     Installation Level Of SSPFS)
 2 - chk_sspfs (Check SSPFS Processes)
 3 - sw_conf (The software configuration of
     the wrtypyxp)
 4 - cpu_util (Overall CPU utilization)
 5 - cpu_util_proc (CPU utilization by
     process)
 6 - port_util (I/O port utilization)
 7 - disk_util (Filesystem utilization)

 X - exist

select -
```

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

Example response

```
=== Executing “sspfs_soft”

SSPFS version: 08.0 Build: 200508421 Server
Profile: cbm850

===”sspfs_soft” completed successfully
```

d Note the SSPFS version.

If the SSPFS version is	Do
08.0	step 14
anything else	contact your next level of support

At the server

14 Remove “SSPFS Disk 3” from the CD ROM drive.

You have completed this procedure.

Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server

Application

Use this procedure to perform the following tasks:

- uncompress the load on your ESD load repository server
- transfer an uncompressed iso image file from your ESD load repository server to the SPFS-based server
- mount the image on the SPFS-based server

Nortel delivers compressed software loads through Electronic Software Delivery (ESD) to a local ESD load repository server. Once the loads are uncompressed, they are then available as International Standard of Organization (ISO) 9660-compliant images for transfer to an SSPFS-based server.

Prerequisites

This procedure has the following prerequisites:

- The ESD load must be available on your ESD load repository server.
- You must know the name or IP address of the load repository server and the location of the dropbox directory on the server.
- You must know the name or IP address of the SSPFS-based server.
- You must know the root password to the SSPFS-based server.

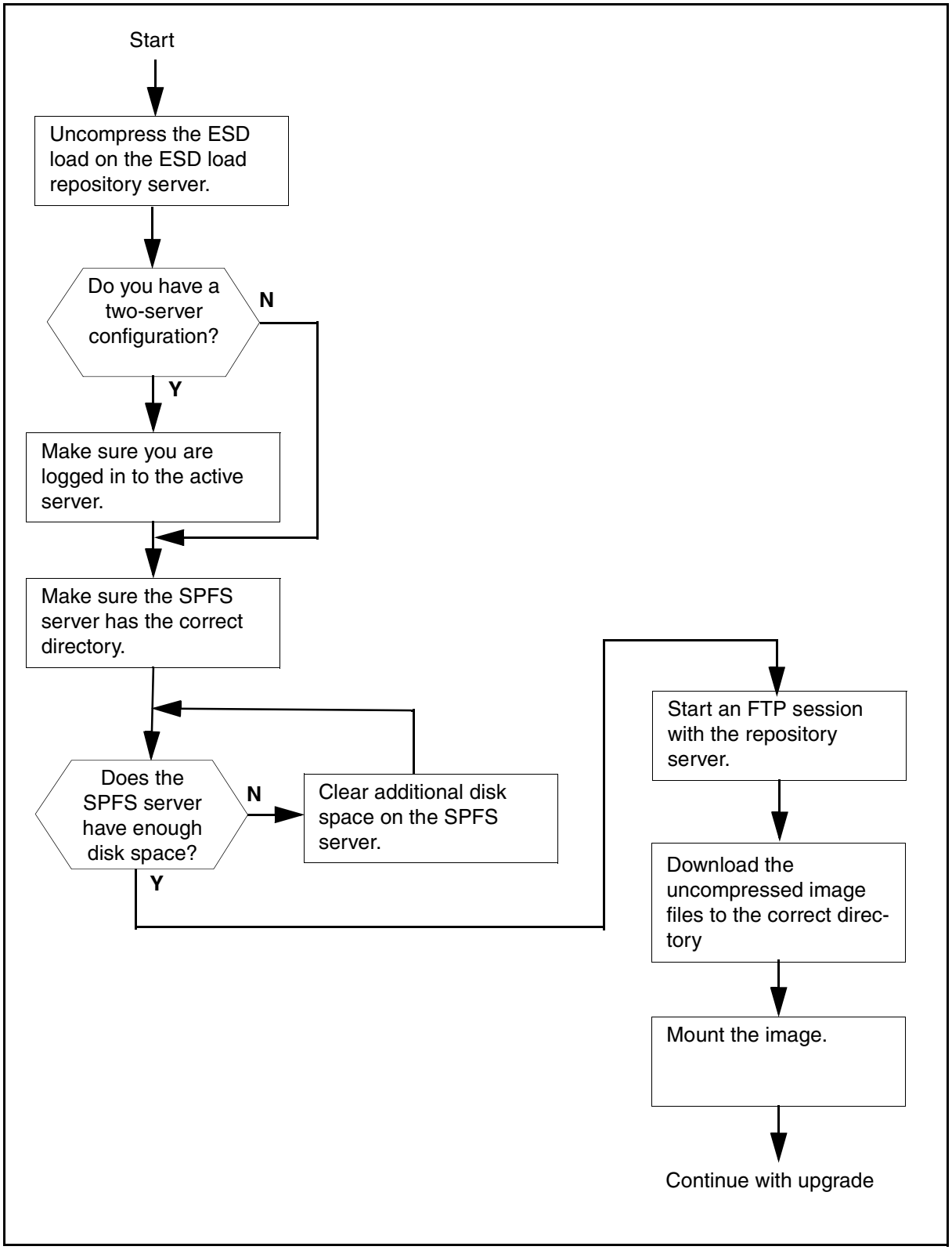
This procedure requires you to confirm the availability of disk space on the SSPFS-based server. If the server does not have the required amount of available disk space, follow your local office policy to clear space. If you do not know your policy or cannot clear the required amount of available disk space, contact your next level of support.

Note: Recommended minimum disk space is 2.3 GBytes.

Action

Use the flowchart as an overview of the tasks required to complete this procedure. Use the step-by-step instructions to complete the procedure.

Overview of steps to transfer and mount an ISO image to an SPFS-based server



Uncompressing the load on the ESD load repository server

At the ESD load repository server

1 Log in to the ESD load repository server, and change directory to the drop box location.

Note: Ensure you log in with a user ID that has permission to uncompress files.

2 List the contents of the drop box by typing

```
ls *.gz
```

and pressing the Enter key.

3 Locate the file you want to uncompress.

4 Uncompress the file by typing

```
gzip -d <esd_filename>.tar.gz
```

and pressing the Enter key.

where

esd_filename
is the name of the ESD software load, for example SPFS009F.9F.R.NCL.NAP.VAULT.1.D, which is the esd_filename for SPFS

5 List the uncompressed file by typing

```
ls *.tar
```

and pressing the Enter key.

Example response

```
SPFS0091.91.R.NCL.NAP.VAULT.1.D.tar
```

6 Unpack the file by typing

```
tar -xvf <esd_filename>.tar
```

and pressing the Enter key.

where

esd_filename
is the name of the ESD software load, for example SPFS009F.9F.R.NCL.NAP.VAULT.1.D, which is the esd_filename for SPFS

The unpacked file is a directory, for example, SPFS009F.9F.R.NCL.NAP.VAULT.1.D, that contains the iso image files.

7 Access this directory by typing

cd <esd_filename_directory>

where

esd_filename_directory
is the directory with the iso image files, for example, SPFS009F.9F.R.NCL.NAP.VAULT.1.D

8 List the contents of the directory by typing

ls

Example response

```
platform_disk_1.iso.tape
platform_disk_2.iso.tape
platform_disk_3.iso.tape
```

9 Rename each file without the .tape extension by typing

mv <filename.tape> <filename>

and pressing the Enter key.

where

filename.tape
is the name of the file with the .tape extension

filename
is the name of the file without the .tape extension

Example

```
mv platform_disk_1.iso.tape platform_disk_1.iso
```

10 Log out of the ESD load repository server.

11 Perform the steps under Transferring an ISO image to an SSPFS-based server on page 675 to continue with this procedure.

Transferring an ISO image to an SSPFS-based server

ATTENTION
In a two-server configuration, you will transfer the ISO image to the active server.

At your workstation

1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 7

2 Log in to the server using telnet by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 Go to step 9.

7 Log in to the server using ssh by typing

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

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

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

8 When prompted, enter the root password and press the Enter key.

9 Use the following table to determine your next step.

If	Do
you have a two-server configuration	step 10
otherwise	step 13

10 Make sure you are on the active server by typing

```
# ubmstat
```

and pressing the Enter key.

11 Use the following table to determine your next step.

If the response is	Do
ClusterIndicatorSTBY	step 12
ClusterIndicatorACT	step 13

12 You are logged on to the inactive server. Log out of this server and return to step 1 to log in to the active server.

13 Make sure the server has the correct directories. Use the following table as reference.

Component	Directory path
ERS 8600	/swd
GWC	/gwc
All other components	/data/esd_iso

List the directory for your component by typing

```
# ls <directory>
```

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data/esd_iso

14 Use the following table to determine your next step.

If the response	Do
indicates no such directory exists	step 15
displays the name of the directory	step 16

15 Create the directory by typing

```
# mkdir <directory>
```

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data/esd_iso

16 Display the available disk space in the directory by typing

```
# df -k <directory>
```

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data

Example response

```
# df -k /data
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2         3082223  144125 2876454     5%    /data
```

17 Record the amount of available disk space, which is provided in kilobytes. You will need the information later in this procedure.

Note: Recommended minimum disk space is 2.3 GBytes.

18 Transfer the ESD software load from the drop box on the repository server to the server as follows:

a Access the repository server through FTP by typing

```
# ftp <repository_server>
```

where

<repository_server>
is the machine owned by the operating company that was selected to be the destination for ESD software.

b Log in and change directory to the drop box location on the repository server.

c Change the transfer mode to binary by typing

```
ftp> bin
```

d List the contents of the drop box by typing

```
ftp> ls
```

e Transfer the ESD software load onto the SSPFS-based server by typing

```
ftp> get <iso_image>
```

where

<iso_image>
is the CS2M ISO image filename for the software load.

f End the FTP session by typing

```
ftp> bye
```

g Uncompress the software load file.

```
# gunzip -d
CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar.gz
```

h Untar the software load file.

```
# tar -xvf
CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar
```

i Remove the .tar file by typing

```
# rm CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar
```

j Access the directory that contains the software load file by typing

```
# cd CS2M0080.80.P.NCL.NAP.VAULT.1.D
```

and list the file in the directory.

k Change the name of the file in the directory by typing

```
# mv CS2M0080_load.iso.tape
CS2M0080_load.iso
```

19 List the contents of the directory to ensure the files successfully transferred to the server by typing

```
# ls -l
```

and pressing the Enter key.

You are now ready to mount the iso image on the server.

20 Perform the steps under Mounting an ISO image on an SSPFS-based server on page 679 to complete this procedure.

Mounting an ISO image on an SSPFS-based server

ATTENTION

In a two-server configuration, you will mount the ISO image on the inactive server with the exception of the APS and Media Server 2000 ISO images, which you will mount on the active server.

At your workstation

1 Use the following table to determine your first step.

If	Do
you have a two-server configuration	step 2
otherwise	step 14

2 Use the following table to determine your next step.

If	Do
you are mounting the APS or Media Server 2000 iso image	step 14
otherwise	step 3

3 Establish a login session to the inactive server using one of the following methods:

If using	Do
telnet (unsecure)	step 4
ssh (secure)	step 9

4 Log in to the inactive server using telnet by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the inactive server

5 When prompted, enter your user ID and password.

6 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

7 When prompted, enter the root password.

8 Go to step 11.

9 Log in to the inactive server using ssh by typing

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

and pressing the Enter key.

where

server
is the physical IP address of the inactive server

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

10 When prompted, enter the root password.

11 Make sure you are on the inactive server by typing

```
# ubmstat
```

and pressing the Enter key.

12 Use the following table to determine your next step.

If the response is	Do
ClusterIndicatorSTBY	step 14
ClusterIndicatorACT	step 13

13 You are logged on to the active server. Log out of this server and return to step 3 to log in to the inactive server.

14 Start the command line interface by typing

```
# cli
```

and pressing the Enter key.

15 Enter the number next to the Other option in the menu.

16 Enter the number next to the mount_image option in the menu.

17 Use the following table to determine your next step.

If the system response is	Do
`Enter full path to ISO image`	step 19
`ISO image Already Mounted`	step 18

18 Enter the number next to the umount_image option in the menu and retry step 16.

Note: If either command is unsuccessful a second time, contact your next level of support.

19 When prompted, enter the full path name of the iso image on the server by typing

```
# <directory_path>/<iso_image>
```

and pressing the Enter key.

where

directory_path
is /swd, /gwc, or /data/esd_iso

iso_image
is the full name of the ISO image file

Note: Do not attempt to change directories to the /tmpmnt directory until the mount command is complete.

20 Use the following table to determine your next step.

If the response	Do
is a warning to unmount the image before removing the image file	step 21
indicates the path you provided does not exist	Verify the location and name of the image and retry step 18.
indicates an error creating the image device location	Retry step 18. An operating system error with the loopback file driver occurred. If the command fails a second time, contact your next level of support.
indicates an error mounting the file	Repeat the steps under Transferring an ISO image to an SSPFS-based server on page 675. The ISO image is corrupt or the /tmpmnt directory has been deleted. If the procedure fails a second time, contact your next level of support.

21 Exit each menu level of the command line interface by typing

```
select - x
```

and pressing the Enter key.

22 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Removing a server from a cluster

Application

Use this procedure to remove a server from a cluster. A cluster refers to a Sun Netra 240 server pair.

ATTENTION
Only perform this procedure when directed to do so.

Prerequisites

You need the root user ID and password.

Action

ATTENTION
Execute this procedure on the Active server of the cluster if the software release is SN06.2. For SN07 or later, you can execute this procedure on the Inactive server of the cluster.

At your workstation

1 Establish a login session to the Active server if the software release is SN06.2 or to the Inactive server if the software release is SN07 or later, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the Active server if the software release is SN06.2, or the Inactive server if the software release is SN07 or later

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: Ensure you are on the right server by typing ubmstat. If the software release is SN06.2, you must be on the Active server and the response must be *ClusterIndicatorACT*. If the software release is SN07 or later, you must be on the Inactive server and the response must be *ClusterIndicatorSTBY*.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server
is the physical IP address of the Active server if the software release is SN06.2, or the Inactive server if the software release is SN07 or later

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

b When prompted, enter the root password.

Note: Ensure you are on the right server by typing ubmstat. If the software release is SN06.2, you must be on the Active server and the response must be *ClusterIndicatorACT*. If the software release is SN07 or later, you must be on the Inactive server and the response must be *ClusterIndicatorSTBY*.

4 Use the following table to determine your next step:

If the software release is	Do
SN06.2	step 5
SN07 or later	step 6

5 For SN06.2, remove the Active server from the cluster by typing

```
# Cluster evict
```

and pressing the Enter key.

You have completed this procedure.

6 For SN07 or later, remove the Inactive server from the cluster as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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


 X - exit

select -
```

b Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

c Enter the number next to the “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 -
```

d Enter the number next to the “evict_cluster” option in the menu.

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

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

Stopping the SESM server application

Application

Use this procedure to stop the Succession Element and Subelement Manager (SESM) server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

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

5 Verify the status of the SESM server application by typing

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

If SESMService is	Do
running	step 6
not running	you have completed this procedure

6 Stop the SESM server application by typing

```
# servstop SESMService
```

and pressing the Enter key.

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

8 Verify the SESM server application stopped by typing

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

and pressing the Enter key.

Example response:

```
Succession CS2K Management Tools is not running
```

You have completed this procedure.

Stopping the SAM21 Manager server application

Application

Use this procedure to stop the SAM21 Manager server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

> **ATTENTION**
> In a two-server configuration, perform the steps that follow on the Active server.

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

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

5 Verify the status of the SAM21 Manager server application by typing

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

If SAM21EM is	Do
running	step 6
not running	you have completed this procedure

6 Stop the SAM21EM server application by typing

```
# servstop SAM21EM
```

and pressing the Enter key.

7 Verify the SAM21EM server application stopped by typing

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

and pressing the Enter key.

Example response:

```
Executing: /opt/servman/bin/servquery -status -
group SAM21EM

Succession SAM21 Element Manager version:
SAM21EM_8_017_0

Current status of the Succession SAM21 Element
Manager:
     SNMP Access Gateway is not running.
    SAM21 Element Manager Server is not running.
```

You have completed this procedure.

Configuring an SSPFS-based client server to use PAM Radius

Application

Use this procedure to configure an SSPFS-based client server to use PAM Radius, which uses the Integrated Element Management System (IEMS) central security server.

Following is a list of SSPFS-based client servers on which you can execute this procedure:

- CS 2000 Management Tools (without the IEMS)
- base and midtier servers of the Media Gateway 9000 manager
- Core and Billing Manager (CBM)

ATTENTION
You must perform this procedure on SSPFS-based client servers after an upgrade from the SN07 release to a newer release if you were using the IEMS central security server for authentiction prior to the upgrade and want to continue using the IEMS central security server for authentication.

CAUTION
System corruption
Do not execute this procedure on an SSPFS-based server that is hosting the IEMS whether the IEMS is standalone or co-resident with the CS 2000 Management Tools. Executing this procedure on an SSPFS-based server that is hosting the IEMS will have negative consequences.

Prerequisites

The following prerequisites apply to this procedure.

- all the current patches are applied
- you have root user privileges

Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based client server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

select -
```

6 Configure the IEMS Security Server Location as follows:

a 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 -
```

b Enter the number next to the “Security Services Configuration” option in the menu.

Example response

```
Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 x - exit

select -
```

c Enter the number next to the “IEMS Server Location Configuration” option in the menu.

Example response

```
IEMS Server Location Configuration
 1 - iems_ip (Configure IEMS Server IP)

 x - exit

select -
```

d Enter the number next to the “iems_ip” option in the menu.

Example response

```
===Executing “iems_ip”

Enter the IEMS Server IP Address (default
45.12.23.56):
```

e When prompted, enter the virtual IP address of the Integrated EMS server, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter IEMS Fully Qualified Domain Name
(default :test3iems.us.nortel.com):
```

f When prompted, enter the Fully Qualified Domain Name (FQDN) of the Integrated EMS server, or press the Enter key to accept the default value if one is specified.

Example response

```
: 45.12.23.56
IEMS Fully Qualified Domain
Name:test3iems.us.nortel.com

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

g Accept the IP address and FQDN you just entered by typing

ok

and pressing the Enter key.

Example response

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

h Return to the Security Services Configuration level of the CLI by typing

select - x

and pressing the Enter key.

Example response

```
Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 x - exit

select -
```

7 Configure PAM as follows:

a Enter the number next to the “PAM Configuration” option in the menu.

Example response

```
PAM Configuration
 1 - Central Security Client Configuration

 x - exit

select -
```

b Enter the number next to the “Central Security Client Configuration” option in the menu.

Example response

```
Central Security Client Configuration
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)
 3 - saml_passwd_conf (Configure saml
     password)

 x - exit

select -
```

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

Example response

```
===Executing "pam_radius"

Activating pam radius components

IEMS Security Server IP: 45.12.23.56
IEMS Fully Qualified Domain Name:
test3iems.us.nortel.com
Enter the Shared Secret (default:
nortelnetworks):
```

d When prompted, enter the shared secret, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter Radius Client Timeout (default: 12):
```

e When prompted, enter the Radius Client timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response

```
Enter SAML Connection Timeout (default: 20):
```

f When prompted, enter the SAML connection timeout, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter SAML Request Timeout (default: 10):
```

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

Example response

```
** Confirm Settings **

IEMS Security Server IP: 45.12.23.56
IEMS Server Domain Name:
test3iems.us.nortel.com
Shared Secret: nortelnetworks
Radius Client Timeout: 12
SAML server Protocol: https
SAML server Port: 58081
SAML Connection Timeout: 20
SAML Request Timeout: 10
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

h Accept the settings by typing

ok

and pressing the Enter key.

Example response

```
Configuring pam_radius

configuring nsssaml

Updating PAM Configuration to use IEMS
Security Server

Restarting name service daemon

===”pam_radius” completed successfully
```

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

select - x

and pressing the Enter key.

You have completed this procedure.

Upgrading the Integrated EMS software

Application

Use this procedure to upgrade the Integrated Element Management System (EMS) software on the SSPFS-based server that is also hosting the CS 2000 Management Tools software.

Prerequisites

This procedure has the following prerequisites:

- Ensure all console and telnet sessions used during the upgrade, are recorded to a file.
- Ensure all users are logged out of the server prior to the upgrade.
- If upgrading from CD, ensure you have the CD that contains the Integrated EMS software for the release you are upgrading to. If upgrading through Electronic Software Delivery (ESD), ensure the software has been transferred and mounted onto the server. If required, refer to procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.

Action

Perform the following steps to complete this procedure.

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

At the server console

1 Obtain the password for user nortel prior to the upgrade, as the password will be changed during the upgrade, and you will need to reset it following the upgrade.

2 Log in to the SSPFS-based server through the console (port A) using the root user ID and password. In a two-server configuration, log in to the inactive server.

3 Use the following table to determine your next step.

If you are upgrading from a	Do
CD	step 4
directory	step 6

At the server

4 Insert the CD that contains the Integrated EMS software into the drive. In a two-server configuration, insert the disk into the inactive server.

At the server console

5 Upgrade the Integrated EMS software using a CD as follows:

a Access the upgrade script by typing

```
# cd /cdrom/cdrom0/bin/
```

and pressing the Enter key.

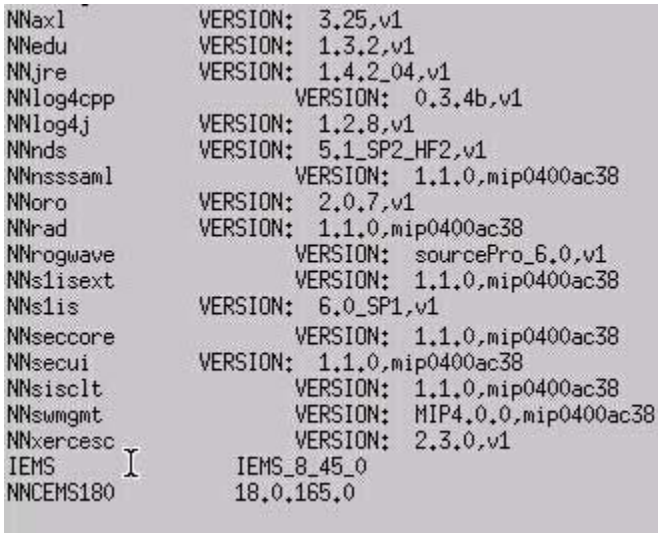
b Run the upgrade script by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

The screen output lists the currently installed packages and confirms the upgrade.

The screen output then lists the contents of the Integrated EMS software package to be installed, similar to the following screen shot:



c Proceed to step 7.

At the server console

6 Upgrade the Integrated EMS software using ESD as follows:

a Access the upgrade script by typing

```
# cd /tmpmnt/bin/
```

and pressing the Enter key.

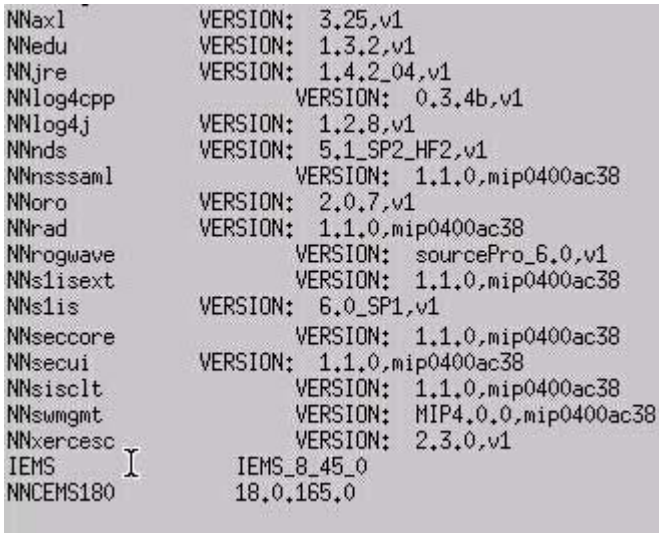
b Run the upgrade script by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

The screen output lists the currently installed packages and confirms the upgrade.

The screen output then lists the contents of the Integrated EMS software package to be installed, similar to the following screen shot:



7 When prompted, confirm you want to upgrade by typing

y

and pressing the Enter key.

A message appears, similar to the following screen shot:

Note: The upgrade can take 30 minutes or more depending on the user data. If one or more error or failure messages are generated during the software upgrade, contact your next level of support.

```
Installing the new security server components...
Done installing the new security server components.

==================================
Checking version of IEMS package...

Installing IEMS Package...
Done Installing IEMS Package.

Installing the CEM ...

==================================
Upgrade of the IEMS software package completed successfully

Exporting data for migration
Configuring ... this will take 30 minutes or more depending on user data
```

8 Ensure you are at the root directory level by typing

cd /

and pressing the Enter key.

9 Reset the password for user nortel by typing

passwd -r files nortel

and pressing the Enter key.

10 When prompted, enter the password for user nortel that you obtained prior to the upgrade.

11 When prompted, enter the password again to confirm it.

12 Use the following table to determine your next step.

If you upgraded from a	Do
CD	step 13
directory	step 16

13 Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

 # /etc/init.d/volmgt stop

 # /etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

14 Remove the CD or DVD from the drive.

15 Proceed to step 17.

16 Unmount the IEMS iso image file as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

b Enter the number next to the “Other” option in the menu.

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

d Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

```
select - x
```

and pressing the Enter key.

17 To make the IEMS patch current, choose your next step as follows.

If the IEMS is in a	Do
two-server configuration	step 18
one-server configuration	step 20

18 In a two-server configuration, apply all IEMS, IEMSCSS, COREM patches using procedure Patching the inactive node of a cluster during an upgrade on page 737.

19 Proceed to step 22.

20 In a one-server configuration, apply all IEMS, IEMSCSS, COREM patches using Patching procedures checklist for the IEMS, COREM, and IEMS security components on page 1856.

21 Ensure the IEMS is running by typing

```
# servquery -status -group IEMS
```

and pressing the Enter key.

22 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Completing the Integrated EMS software upgrade

Application

Use this procedure to complete the upgrade of the IEMS sofware.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

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

At server

1 Use the following table to determine your next step.

If you upgraded from a	Do
CD	step 2
directory	step 3

2 If you upgraded from a CD, run the Config File Swap script as follows:

a Insert the CD that contains the IEMS software into the drive.

b Run the script by typing

/cdrom/cdrom0/bin/switch08conf.ksh

and pressing the Enter key.

c When prompted, confirm you want to continue by typing

y

and pressing the Enter key.

d Proceed to step 4.

3 If you upgraded from a directory, run the Config File Swap script as follows:

a Access the command line interface to mount the IEMS iso image file by typing

```
# cli
```

and pressing the Enter key.

b Enter the number next to the “Other” option in the menu.

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

If the response is	Do
`Enter the full path of the ISO image`	substep e
`ISO Image Already Mounted`	substep d

d Enter the number next to the “umount_image” option in the menu and retry substep c.

Note: If the umount_image or mount-image command is unsuccessful a second time, contact your next level of support.

e When prompted, enter the full path name of the ISO image on the server from the root.

The contents of the ESD software file are placed in directory /tmpmnt.

Note: Do not attempt to access the /tmpmnt directory until the mount command is complete.

If the response is	Do
`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`	step f
`Provided full path to ISO image does not exist`	Verify the location and name of the ISO 9660 image.
`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 your next level of support.
`ERROR MOUNTING <ESD_filename>`	This response indicates that either the ISO 9660 file is corrupt, or the `/tmpmnt` directory has been deleted. Repeat this procedure, and if it fails a second time, contact your next level of support.

f Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

`select - x`

and pressing the Enter key.

g Run the script by typing

`# /tmpmnt/bin/switch08conf.ksh`

and pressing the Enter key.

h When prompted, confirm you want to continue by typing

`y`

and pressing the Enter key.

4 Use the following table to determine your next step.

If	Do
the Media Server 2000 is in the network	step 5
otherwise	step 8

5 Determine if the bootptab file is present on the server by typing

`# ls -l /data/sspfs/etc/bootp/bootptab`

and pressing the Enter key.

6 Use the following table to determine your next step.

If the bootptab file is	Do
not present	step 7
present	step 8

7 Set up the BootP file using procedure Setting up the BootP file on SSPFS on page 516.

8 If you determined at the beginning of the upgrade that the server was using a third-party security application, the special edits that were in the NSCD, PAM and NSSwitch configuration files (nscd.conf, pam.conf and nsswitch.conf), need to be put back since during the IEMS software upgrade, the configuration files were replaced with new configuration files that use the IEMS security application.

Contact your system administrator.

9 Use the following table to determine your next step.

If you upgraded from	Do
SN07	step 10
SN08	step 11

10 Run the IEMS cleanup script.

a Change directory by typing:

cd /opt/nortel/iems/current/bin

and pressing the Enter key.

b Run the script by typing

./CleanUpSN07Data.sh

and pressing the Enter key.

11 Use the following table to determine your next step.

If you upgraded from a	Do
CD	step 12
directory	step 13

12 Eject the CD from the drive as follows:

a Ensure you are at the root directory level by typing

cd /

and pressing the Enter key.

b Eject the CD by typing

eject cdrom

and pressing the Enter key.

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

/etc/init.d/volmgt stop

/etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

d Proceed to step 14.

13 If you upgraded from a directory, unmount and remove the ISO image file from the server using procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716.

14 Update the CEM documentation.

If you are using	Do
a CD	step 15
electronic software delivery (ESD)	step 18

15 Insert the CD that contains the CEM documentation into the drive.

16 Upgrade the CEM documentation by typing

```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.

17 Eject the CD from the drive as follows:

a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

 # /etc/init.d/volmgt stop

 # /etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

d Proceed to step 20.

18 Mount the CEM help file. See Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server.

19 Upgrade the CEM documentation by typing

```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.

Note: To configure CEM, see Integration of Core Element Manager with Integrated EMS in *Integrated EMS Basics*, NN10329-111.

20 Use the following table to determine your next step.

If the IEMS is in a	Do
one-server configuration	step 21
two-server configuration (HA)	step 23

21 Start the IEMS server application if not already started by typing

```
# servstart IEMS
```

and pressing the Enter key.

22 Verify the IEMS server application started by typing

```
# servman query -status -group IEMS
```

and pressing the Enter key.

Example response:

```
IEMS Instance is UP
```

23 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Upgrading the CS2M software

Application

Use this procedure to upgrade the CS 2000 Management (CS2M) software on the CS 2000 Management Tools server.

Prerequisites

If upgrading from CD, ensure you have the CD that contains the CS2M software for the release you are upgrading to. If upgrading through Electronic Software Delivery (ESD), ensure the software has been transferred and mounted onto the server. If required, refer to procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.

Action

Perform the following steps to complete this procedure.

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

At the CS 2000 Management Tools server console

1 Log in to the CS 2000 Management Tools server through the console (port A) using the root user ID and password. In a two-server configuration, log in to the inactive server.

Note: In a two-server configuration, ensure you are on the inactive server by typing ubmstat. If ClusterIndicatorACT is displayed in the response, which indicates you are on the active server, log out of that server and log in to the other server. The response must display ClusterIndicatorSTBY, which indicates you are on the inactive server.

2 Use the following table to determine your next step.

If upgrading from a	Do
CD	step 3
directory	step 4

At the CS 2000 Management Tools server

3 Insert the CD that contains the CS2M software into the drive. In a two-server configuration, insert the CD into the inactive server.

At the CS 2000 Management Tools server console

4 Upgrade the CS2M software using substep a or b.

a If you are upgrading from a CD, upgrade the CS2M software by typing

```
# /cdrom/cdrom0/bin/appl_mgr.ksh
```

and pressing the Enter key.

Proceed to step 5.

b If you are upgrading from a directory, upgrade the CS2M software by typing

```
# /tmpmnt/bin/appl_mgr.ksh
```

and pressing the Enter key.

5 When prompted, confirm you want to upgrade by typing

```
# y
```

The upgrade takes approximately 10 minutes to complete.

If you upgraded from a	Do
CD	step 6
directory	proceed to procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716

6 Eject the CD from the drive as follows:

a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the CD by typing

eject cdrom

and pressing the Enter key.

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

/etc/init.d/volmgt stop

/etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Unmounting and removing an ISO image from an SSPFS-based server

Application

Use this procedure to unmount and remove an ISO image delivered through Electronic Software Delivery (ESD) from a Succession Server Platform Foundation Software (SSPFS)-based server.

This procedure is applicable to software loads for the following components:

- Gateway Controller (GWC)
- CS 2000 Management Tools (CS2M)
- Audio Provisioning Server (APS)
- Integrated Element Management System (EMS)

Prerequisites

The component has been upgraded.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server on which the software you want to unmount and remove 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 Unmount the ISO image 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)


 X - exit

select -
```

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

d Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

```
select - x
```

and pressing the Enter key.

6 Remove the ISO image from the server by typing

```
# rm /<directory>/<loadname>
```

and pressing the Enter key.

You have completed this procedure.

Installing the Integrated EMS application on a SSPFS-based server

Application

Use the following procedures to perform a fresh install of the Integrated Element Management System (IEMS) application on the same server as the Communication Server 2000 Management Tools (CS2KMT):

Only perform this procedure when the IEMS is not already present in the network, neither on the SPFS-based server that host the CS 2000 Management Tools nor on a separate SPFS-based server.

Performing a fresh install of the IEMS consists of the following tasks:

- increasing the size of the /data/oradata file system
- configuring a virtual IP address for the IEMS application
- installing the IEMS on the server
- verifying the IEMS application is installed and started

Prerequisites

This procedure has the following prerequisites:

- Before you install the IEMS on the server, verify you have met the security certificate and DNS requirements by performing Installing or replacing an HTTPS certificate on an SSPFS-based server.
- If you are installing the IEMS using a CD, obtain the CD labelled for the release you are installing.
- If you are installing the IEMS through Electronic Software Delivery (ESD), transfer and mount the IEMS ISO image on the server using Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.

Action

Perform the steps under each of the following headings in the order they are listed, to complete this procedure:

- Increasing the size of a file system on a simplex configuration (one server) on page 720 or Increasing the size of a file system on a high-availability (HA) cluster configuration (two servers) on page 722
- Configuring a virtual IP address on an SSPFS-based server on page 725
- Installing Integrated EMS on a SSPFS-based server on page 731
- Verifying installation and startup of the Integrated EMS application on page 736

Perform the following steps to complete this procedure.

Increasing the size of a file system on a simplex configuration (one server)

At your workstation (on the Inactive node)

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Determine the current size of the file system by typing

```
# df -k
```

and pressing the Enter key.

Note the size of the file system mounted on “/data/oradata” by reading the number in the Kbytes column.

If the system response	Do
displays that the file system space is less than 16GB	step 6
displays that there is 16GB or more in file system space	proceed to Configuring a virtual IP address on an SSPFS-based server on page 725

6 Determine the size by which to increase the file system, by subtracting its current size (noted in step 5) from the desired size for the file system based on your specific needs (16 GB).

For example, if you determined that the current size of the file system is 12GB then the size by which to increase the “/data/oradata” file system, arrived at by subtracting its current size of 12GB from the desired size of 16GB, is 4GB.

7

ATTENTION
Once you increase the size of a file system, you cannot decrease it.

Increase the size of the file system by typing

```
# filesys grow -m /data/oradata -s <size>
```

Where

size
is the size in bytes by which you want to increase the file system (determined in step 6)

Example

```
# filesys grow -m /data/oradata -s 4g
```

Note: The example above increases the "/data/oradata" file system by 4 gigabytes (GB).

Wait for the # prompt to display signaling that this process is complete.

You have completed this procedure. Proceed to Configuring a virtual IP address on an SSPFS-based server on page 725.

Increasing the size of a file system on a high-availability (HA) cluster configuration (two servers)

At your workstation (on the Inactive node)

1 Log in to the server by typing

```
> telnet <Cluster IP Address>
```

and pressing the Enter key.

where

<Cluster IP Address>
is the IP address or host name of the SSPFS-based server to which you want to transfer the software load

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
# su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

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

```
# udstat
```

and pressing the Enter key.

If the file systems are	Do
STANDBY normal UP clean	step 6
not STANDBY normal UP clean	contact your next level of support

6 Determine the current size of your file system by typing

```
# df -k
```

and pressing the Enter key.

Note the size of the file system mounted on "/data/oradata" by reading the number in the Kbytes column.

If the system response	Do
displays that the file system space is less than 16GB	step 8
displays that there is 16GB or more in file system space	proceed to Configuring a virtual IP address on an SSPFS-based server on page 725

7 Determine the size by which to increase the file system, by subtracting its current size (noted in step 6) from the desired size for the file system based on your specific needs (16 GB).

For example, if you determined that the current size of the file system is 10GB then the size by which to increase the “//data/oradata” file system, arrived at by subtracting its current size of 10MB from the desired size of 16GB, is 6GB.

8 Increase the size of the file system by typing

#/opt/nortel/sspfs/ha/GrowClusteredFileSystem.ksh /data/oradata <size>

and pressing the Enter key.

Where

size
is the size in bytes by which you want to increase the file system (determined in step 6)

Example
 # filesys grow -m /data/oradata -s 6g

Note: The example above increases the "/data/oradata" file system by 6 gigabytes (GB).

Wait for the # prompt to display signaling that this process is complete.

9 Restart the server by typing

 # init 6

and pressing the Enter key.

You remain on the inactive unit following the restart of the server.

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

 # udstat

and pressing the Enter key.

If	Do
the system response is `STANDBY normal UP clean`	step 11
otherwise	contact your next level of support

11 Perform the steps under Configuring a virtual IP address on an SSPFS-based server on page 725 to continue with this procedure.

Configuring a virtual IP address on an SSPFS-based server

At your workstation (on the Inactive node)

1 Log in to 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 configuring the virtual IP address

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

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

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

 X - exit

select -
```

6 Enter the number that corresponds to the “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 that corresponds to the “IP Configuration” option in the menu.

Example response

```
IP Configuration
 1 - config_router (Configure Default Router and
     Netmask)
 2 - config_data (Configure System Data IP
     Addresses)

 X - exit

select -
```

8 Enter the number that corresponds to the “config_data” option in the menu.

Example response

```
===Executing “config_data”

WARNING: Changing the network settings will
effect all applications! Improper network
configuration will result in loss of service!
Applications may require restart or
reconfiguration after network changes

CAUTION: You are not accessing this tool via the
system console. Changing network configuration
may disrupt this session.

CAUTION: HTTPS Certificate is installed for web
services. Changing the hostname or ip may
require an updated certificate.

hostname:           <hostname>
ip address:           <ip address>

Enter the hostname for this system [hostname]
```

9 When prompted, enter the hostname for this SSPFS-based server, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter ip address for <hostname> [00.00.00.00]
```

10 When prompted, enter the IP address for this SSPFS-based server, or press the Enter key to accept the default value if one is specified.

Example response

```
Configure additional ip address? [yes]
```

11 When prompted, indicate whether you want to configure an additional IP address.

If you enter	Do
yes	step 12
no	step 15

12 When prompted, enter the virtual IP address you want to configure on this server, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter application for ip address <ip address>
```

13 When prompted, enter the application name for the additional IP address you just specified, or press the Enter key to accept the default value if one is specified.

Note 1: When configuring a virtual IP address for APS, the application name is APS. When configuring a virtual IP address for IEMS, the application name is IEMS.

Note 2: The system allocates a hostname for each virtual IP address that is configured. The hostname is in the form of <sspfs_primary_hostname-application>, for example, “wxe0s00j-iems” when the virtual IP address is set up for IEMS. Hostnames are stored in file” /etc/hosts” on the system.

Example response

```
Configure additional ip address? [no]
```

14 Enter no at the prompt.

15 When prompted, confirm the settings by typing

ok

and pressing the Enter key.

*Example response on an **HA system***

```
The network changes have been made, however the
cluster requires a restart of both units. The
units must be restarted in the below order.

1) Login as root on the console of the standby
   unit and shut it down with the command:
   “shutdown -i 0 -y”.
2) After the standby unit has shutdown, restart
   the active unit with the command: “shutdown
   -i 6 -y”.
3)After the restart is complete, the new network
  settings are in effect.
4) Boot the standby unit with the command
   “boot”.

===”config_data” completed successfully
```

*Example response on a **simplex system***

```
The network changes have been made, however a
restart is required to use the new network
settings. Reboot to ensure all applications are
restarted. Exit this "cli" tool and reboot using
the Solaris command "shutdown -i 6 -y".

===" config_data" completed successfully
```

16 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.

If you have	Do
a simplex system	step 17
an HA system	step 18

17 Reboot the server by typing

`# shutdown -i 6 -y`

and pressing the Enter key.

Proceed to step 27.

At the console of the Inactive node

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

> ***Note:*** Ensure you are on the Inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

19 Shutdown the inactive node by typing

`# shutdown -i 0 -y`

and pressing the Enter key.

At the console of the active node

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

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

21 Restart the active node by typing

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

and pressing the Enter key.

At the console of the Inactive node

22 Boot the inactive node by typing

```
# boot
```

and pressing the Enter key.

At the console of the active server

23 Log in to the active server through the console (port A) using the root user ID and password.

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

24 Shutdown the active server by typing

```
# init 0
```

and pressing the Enter key.

The active server is taken down to the OK prompt and the standby (inactive) server takes over and starts providing OAM&P services as the new active server.

Note: The high-availability (HA) cluster can take up to approximately 3 hours to failover and bring up the standby server to active state depending on the size of the configuration.

At the console of the newly active server

25 Log in to the newly active server through the console (port A) using the root user ID and password.

26 Verify the failover status by typing

```
# ubmstat -m
```

and pressing the Enter key.

The failover is complete once the response to this command is as follows:

```
Group      State
------------------
ClusterIndicatorACT

Monitor    State
-----------------
ClusterIndicatorMonitorOnUnit0UNREG
ClusterIndicatorMonitorOnUnit1ACT
```

27 Perform the steps under Installing Integrated EMS on a SSPFS-based server on page 731 to continue with this procedure.

Installing Integrated EMS on a SSPFS-based server

At your workstation (on the newly active node)

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
# su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the software is available	Do
on CD	step 6
as an ISO image (ESD)	step 7

6 Insert the IEMS software CD in the DVD drive and change directories by typing

```
# cd cdrom/cdrom0/bin
```

and pressing the Enter key.

```
# ls
```

and pressing the Enter key.

The appl_mgr.ksh file needs to be present in the bin directory.

Proceed to step 8.

7 If you are using a mounted ISO image to install the IEMS software, change directories by typing

```
# cd /tmpmnt/bin
```

and pressing the Enter key.

```
# ls
```

and pressing the Enter key.

The appl_mgr.ksh file needs to be present in the bin directory.

8 Start the installation by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

When prompted, confirm the installation by typing

```
yes
```

and pressing the Enter key.

Note: The execution of this installation takes approximately 45 minutes to complete.

9 Change directories again by typing

```
# cd /opt/nortel/iems/current/bin
```

and pressing the Enter key.

```
# ls
```

and pressing the Enter key.

The iems_config.sh file needs to be present in the bin directory.

10 Start the IEMS script by typing

```
# ./iems_config.sh
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - Configure OfficeName

 X - exit

select -
```

11 Enter the number next to the “Configure OfficeName” option in the menu.

Example response

```
Please enter the office name:
```

12 Enter the Primary Server HostName at the prompt.

The Primary Server HostName is the primary IP address for the CS 2000 Management Tools server.

Example response

```
Command Line Interface
 1 - Configure OfficeName

X - exit

select -
```

13 Exit the command line interface by typing

```
select - x
```

and pressing the Enter key.

14 If required, update the CEM documentation. Select your next step.

If you are using	Do
a CD	step 15
an iso image file	step 18

15 Insert the CD that contains the CEM documentation into the drive.

16 Upgrade the CEM documentation by typing

```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.

17 Go to step 22.

18 Mount the CEM help file. See Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server.

19 Upgrade the CEM documentation by typing

```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.

Note: To configure CEM, see Integration of Core Element Manager with Integrated EMS in *Integrated EMS Basics*, NN10329-111.

20 Apply all IEMS, IEMSCSS, COREM patches using procedure Patching procedures checklist for the IEMS, COREM, and IEMS security components on page 1856.

21 Use the following table to determine your next step.

If you have	Do
a simplex system	step 22
an HA system	step 23

22 Start the IEMS application by typing

```
# servstart IEMS
```

and pressing the Enter key.

Note: The first time the IEMS application is started will take longer to run than subsequent times because the database tables are being created.

23 Verify that the IEMS application is running by typing

```
# servquery -status -group IEMS
```

and pressing the Enter key.

Example response

```
IEMS Instance is UP
```

24 Use the following table to determine your next step.

If you installed the software using	Do
a CD	step 26
an ISO image (ESD)	step 25

25 Unmount and remove the IEMS ISO image from the the server and proceed to step step 28.

For detailed steps, refer to Unmounting and removing an ISO image from an SSPFS-based server on page 716

26 Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

 # /etc/init.d/volmgt stop

 # /etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

27 Remove the CD from the drive.

28 Perform the steps on Verifying installation and startup of the Integrated EMS application on page 736 to complete this procedure.

Verifying installation and startup of the Integrated EMS application

At your workstation

1 Verify that IEMS has started by typing

```
# servquery -status -group IEMS
```

Note: The workstation must be on the same subnet as the IEMS server.

2 Open a web browser and then access the IEMS homepage by typing

`https://<IEMS IP Address>:9091`

and pressing the Enter key.

The Nortel Network Integrated EMS window displays on the screen.

3 Click Web Start Client in the bottom right-hand corner of the Nortel Network Integrated EMS window.

The Integrated Element Management System window displays on the screen.

4 Enter the following information by typing

`iemsadm`

in the User ID field and

`public`

in the Password field

The IEMS Security Notice Message window displays on the screen.

5 Click OK.

The Integrated EMS Client window displays on the screen.

6 Leave the web browser open and proceed to the next procedure in the upgrade.

Note: If you were not able login, ensure the IEMS server is running and contact your next level of support.

7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to 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 one of the following procedures to transfer the patches to the NPM database:
  - — Transferring patches delivered on CD to the NPM database on page 1884
  - — Transferring patches delivered through ESD to the NPM database on page 1889
- Ensure you have the root password for the NPM host.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in 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 -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If	Do
you are currently upgrading the MG 9000 Manager	step 6
otherwise	step 7

6 Configure the MG9000 PSEs as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

select -
```

b Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)
```

```
X - exit

Select -
```

c Enter the number next to the “Succession Element Configuration” option in the menu.

Example response

```
Succession Element Configuration
 1 - RESMON Application Configuration
 2 - NPM Application Configuration
 3 - PSE Application Configuration
 4 - OMPUSH Application Configuration

 x - exit

select -
```

d Enter the number next to the “PSE Application Configuration” option in the menu.

Example response

```
PSE Application Configuration
 1 - View_NPM_host_or_ip (View NPM
hostname/ip address location)
 2 - Update_NPM_host_or_ip (Update NPM
hostname/ip address location)
 3 - Create_PSE_Database (Initialize or
re-initialize the PSE database)
 4 - Update_Patch_Corba_Mirroring (Mirror the
NPM patch CORBA name reference)
 5 - Remove_Patch_Corba_Mirroring (Remove the
NPM patch CORBA name mirror reference)
 6 - Unconfigure_PSE (Remove PSE as a system
process)

 x - exit

select -
```

e Enter the number next to the “View_NPM_host” option in the menu.

Example response

```
===Executing “View_NPM_host_or_ip”

The PSE on this machine is looking at the NPM
on: 47.xxx.xxx.xx

===“View_NPM_host_or_ip” completed
successfully
```

Verify that the PSE application is pointing to the CS2000 Management Tool machine where NPM is running. If the PSE application is not configured correctly, reconfigure the PSE to point to the CS 20000 Management Tool machine that is running NPM. Refer to Upgrading SSPFS software on page 666 in *ATM Solution Upgrades*, NN10261-450 or *IP Solution Upgrades*, NN10344-450.

f Enter the number next to the “PSE Application Configuration” option in the menu.

Example response

```
PSE Application Configuration
 1 - View_NPM_host_or_ip (View NPM
hostname/ip address location)
 2 - Update_NPM_host_or_ip (Update NPM
hostname/ip address location)
 3 - Create_PSE_Database (Initialize or
re-initialize the PSE database)
 4 - Update_Patch_Corba_Mirroring (Mirror the
NPM patch CORBA name reference)
 5 - Remove_Patch_Corba_Mirroring (Remove the
NPM patch CORBA name mirror reference)
 6 - Unconfigure_PSE (Remove PSE as a system
process)

 x - exit

select -
```

g When prompted, enter x to exit each level until you exit the command line interface.

7

ATTENTION

If the NPM resides on the server, use the patchUpToDate command. If the NPM does not reside on the server, use the procedure Applying patches using the NPM on page 1895.

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]
```

8 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.
```

9 When prompted, enter “root” (without the quotation marks) as the user on the NPM host <hostname>.

Example response:

```
Obtaining the list of devices that can be
patched.
```

10 Press the Enter key to confirm that you want the patches applied.

Note: Entering “no” causes the processing to stop.

Example response:

```
PSE [1 of 1]: There are 3 patches to be applied.
   Applying KAA00007 [1 of 3] to PSE.
   Applying KAA01007 [2 of 3] to PSE.
   Applying KAA02007 [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 as well as any errors. The summary includes patches applied, any patches that were already applied when the patchUpToDate utility started, any patches that have been applied and removed when the patchUpToDate utility started, and any patches that were not applied because their prerequisite patches were not available.

11 If prompted, confirm that you want a restart to occur on each of the listed devices by entering **`yes`**.

Note: A restart enables the patches on the device.

12 If prompted, confirm that you want a system reboot to occur by entering **`yes`**.

A report is generated which contains all the console output from the patchUpToDate session.

The report that is produced contains a summary of the patching actions that occurred as well as any errors. The summary includes patches applied, any patches that were already applied when the patchUpToDate utility started, any patches that have been applied and removed when the patchUpToDate utility started, and any patches that were not applied because their prerequisite patches were not available.

13 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Returning a server to a cluster

Application

Use this procedure to return a server to a cluster. A cluster refers to a Sun Netra 240 server pair

ATTENTION
Only perform this procedure when directed to do so.

Prerequisites

None

Action

ATTENTION
Execute this procedure on the Active server of the cluster if the software release is SN06.2. For SN07 or later, you can execute this procedure on the Inactive server of the cluster.

At your workstation

1 Establish a login session to the Active server if the software release is SN06.2 or to the Inactive server if the software release is SN07 or later, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the Active server if the software release is SN06.2, or the Inactive server if the software release is SN07 or later

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: Ensure you are on the right server by typing ubmstat. If the software release is SN06.2, you must be on the Active server and the response must be *ClusterIndicatorACT*. If the software release is SN07 or later, you must be on the Inactive server and the response must be *ClusterIndicatorSTBY*

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server
is the physical IP address of the Active server if the software release is SN06.2, or the Inactive server if the software release is SN07 or later

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

b When prompted, enter the root password.

Note: Ensure you are on the right server by typing ubmstat. If the software release is SN06.2, you must be on the Active server and the response must be *ClusterIndicatorACT*. If the software release is SN07 or later, you must be on the Inactive server and the response must be *ClusterIndicatorSTBY*.

4 Use the following table to determine your next step:

If the software release is	Do
SN06.2	step 5
SN07 or later	step 6

5 For SN06.2, join the Active server to the cluster by typing

```
# Cluster join
```

and pressing the Enter key.

You have completed this procedure.

6 For SN07 or later, join the Inactive server to the cluster as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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


 X - exit

select -
```

b Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

c Enter the number next to the “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 -
```

d Enter the number next to the “join_cluster” option in the menu.

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

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

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.

Prerequisites

You must perform this procedure on the active node.

Action

Perform the following steps to complete this procedure.

At the active server console

1 Log in to the active server through the console (port A) using the root user ID and password.

2 Stop the cluster by typing

```
# /opt/servman/bin/stopAll
```

and pressing the Enter key.

```
# init 0
```

and pressing the Enter key.

The active server is taken down to the OK prompt and the standby (inactive) server takes over and starts 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 server to Active state.

3 Log in to the newly active server through the console (port A) using the root user ID and password.

4 Verify the failover status by typing

```
# ubmstat -m
```

and pressing the Enter key.

The failover is complete once the response to this command is as follows:

```
Group      State
------------------
ClusterIndicatorACT

Monitor    State
-----------------
ClusterIndicatorMonitorOnUnit0UNREG
ClusterIndicatorMonitorOnUnit1ACT
```

5 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Starting the SESM server application

Application

Use this procedure to start the Succession Element and Subelement Manager (SESM) server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

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

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

Note: In a two-server configuration, enter the physical IP address of the active server (unit 0 or unit 1).

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

5 Verify the status of the SESM server application by typing

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

If SESMService is	Do
not running	step 6
running	you have completed this procedure

6 Start the SESM server application by typing

```
# servstart SESMService
```

and pressing the Enter key.

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

Note: Starting SESM for the first time after an upgrade from a pre-SN07 release, can take up to 90 minutes depending on the number of GWs provisioned in the office. This is a one-time event that occurs during an upgrade to facilitate better topological management of data.

8 Verify the SESM server application started as follows:

a Verify the SESM services started by typing

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

and pressing the Enter key.

Example response prior to SN08:

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

Succession CS2K Management Tools VERSION:
SESM_8_019_0

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

Example response for SN08 and up:

```
Succession CS2K Management Tools is running
```

b Verify the SESM applications started by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

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

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

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

SESM APPLICATION STATUS: All Applications Ready
```

You have completed this procedure.

Starting the SAM21 Manager server application

Application

Use this procedure to start the SAM21 Manager server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

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

5 Verify the status of the SAM21 Manager server application by typing

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

If SAM21EM is	Do
not running	step 6
running	you have completed this procedure

6 Start the SAM21EM server application by typing

```
# servstart SAM21EM
```

and pressing the Enter key.

7 Verify the SAM21EM server application started by typing

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

and pressing the Enter key.

Example response:

```
Executing: /opt/servman/bin/servquery -status -
group SAM21EM

Succession SAM21 Element Manager version:
SAM21EM_8_017_0

Current status of the Succession SAM21 Element
Manager:
     SNMP Access Gateway is running.
     SAM21 Element Manager Server is running.
```

You have completed this procedure.

Upgrading APS software

Application

Use this procedure to upgrade the APS software from release APS08_2 ((I)SN06.2) or APS09 ((I)SN07), to release APS10 ((I)SN08) on the CS 2000 Management Tools server.

ATTENTION
This procedure assumes the 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 on page 619, which applies to a Sun t1400 server with a DAT drive.
  - — Performing a backup of APS audio files to CD or DVD on page 621, which applies to a Sun Netra 240 server with a CD/DVD drive
  - — Performing a backup of APS oracle data to tape on page 624, which applies to a Sun t1400 server with a DAT drive.
  - — Performing a backup of APS oracle data to CD or DVD on page 626, which applies to a Sun Netra 240 server with a CD/DVD drive
- If upgrading from CD, ensure you have the CD that contains the APS and IPS database software required for an upgrade to release APS10 ((I)SN08). If upgrading through Electronic Software Delivery (ESD), ensure the software has been transferred and mounted onto the server. If required, refer to procedure Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.

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, log in to the active server as you must upgrade APS software on the active server.

2 List the APS software package and any patches that have been applied by typing

pkginfo | grep aps

and pressing the Enter key.

Example command and system response:

pkginfo | grep aps

application ACaps10 APS10-22.0 Package - /opt/uas/aps.April 19, 2005
application ACips IPS10-22.0 DB Package which goes into /usr/ntdb/aps10

3 Remove each package one at a time by typing

pkgrm ACaps10

and pressing the Enter key.

Note: ACaps10 is the package identifier shown in the example system response in step 2

4 When prompted, indicate you want to remove the aps package by typing

y

and pressing the Enter key.

5 When prompted, indicate you want to continue with the removal of the package by typing

y

and pressing the Enter key.

6 Remove the ips package by typing

pkgrm ACips

and pressing the Enter key.

Note: ACips is the package identifier shown in the example system response in step 2

7 When prompted, indicate you want to remove the ips package by typing

y

and pressing the Enter key.

8 When prompted, indicate you want to continue with the removal of the package by typing

y

and pressing the Enter key.

9 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.

10 Use the following table to determine your next step.

If you are installing from a	Do
CD	step 11
directory	step 18

11 When installing from a CD, insert the APS10 CD into the CD-ROM drive.

12 Wait approximately 30 seconds for the server to auto mount the CD drive.

13 Verify you can see the CD-ROM drive listed in the mounted drive list by typing

```
# df
```

and pressing the Enter key.

Look for /cdrom/<APS CD (mount point)>

where

APS CD (mount point)
is the label of the APS CD and its mount point

14 Copy the contents on the CD to the root directory by typing

```
# cp /cdrom/cdrom0/* /
```

and pressing the Enter key.

15 Verify the loads got copied by typing

```
# ls -l /ACaps10* ACips*
```

and pressing the Enter key.

You will see two loads listed.

16 Change directory to where the software is, which is the root directory, by typing

```
# cd /
```

and pressing the Enter key.

17 Proceed to step 19.

18 When installing from ESD, change directory to where the software is by typing

```
# cd /tmpmnt
```

and pressing the Enter key.

You will see two loads listed.

19 Install the APS10 software package by typing

```
# pkgadd -d ACaps10-<xx>.pkg
```

and pressing the Enter key.

where

xx
is the APS loadbuild number

Example response:

```
The following packages are available:
1 ACaps10   APS10-20.0 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 <ACaps10> from
</ACaps10-20.0.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]
```

20 Use the following table to determine your next step.

If	Do
the system prompts you about installing conflicting files	step 21
otherwise	step 23

21 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
<ACaps10> [y, n,?, q]
```

22 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 <ACaps10>
```

23 Install the IPS software package by typing:

```
# pkgadd -d ACips10-<xx>.pkg
```

and pressing the Enter key.

where

xx
is the APS loadbuild number

24 When prompted, indicate you want to install all packages by typing

all

and pressing the Enter key.

If	Do
the system prompts you about installing conflicting files	step 25
otherwise	step 27

25 Indicate you do not want to install these conflicting files by typing

n

and pressing the Enter key.

26 When prompted, confirm you want to continue with the installation by typing

y

and pressing the Enter key.

27 When prompted, confirm you want to continue with the installation by typing

y

and pressing the Enter key.

28 Run the IPS 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.

29 Check the /apsinst.log for application install errors by typing

```
# cat /apsinst.log |more
```

and pressing the Enter key.

30 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.

31 Delete the previous NTaps and NORTips packages if they are still present under the root (/) directory.

32 Verify the database, webserver, webservices, 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
```

33 Configure the SNMP agent. If required, refer to procedure “Configuring the SNMP agent” in the Media Server 2000 Configuration Management document, NN10340-511.

Note: The APS SNMP is not running at the end of the APS upgrade.

34 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.

35 Use the following table to determine your next step.

If you upgraded from a	Do
CD	step 36
directory	perform procedure Unmounting and removing an ISO image from an SSPFS-based server on page 716

36 Eject the APS10 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.

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

 # /etc/init.d/volmgt stop

 # /etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

You have completed this procedure.

Confirming the upgrade on an SSPFS-based server

Application

Use this procedure to either accept the upgraded environment permanently, or rollback to the state prior to the upgrade.

ATTENTION
Only use this procedure when directed to do so.

Prerequisites

In a two-server configuration, you must perform this procedure on the newly upgraded node in the cluster, which is now the active node.

Action

Perform the following steps to complete this procedure.

At the sever console

1 Log in to the server through the console (port A) using the root user ID and password if not already logged in. In a two-server configuration, log in to the active node.

2 Use the following table to determine your next step:

If	Do
you choose to accept the upgraded environment	step 3 only
you choose to rollback to the state prior to the upgrade	step 4

3 Accept the upgraded environment by typing

```
# /SSPFS_Upgrade.accept
```

and pressing the Enter key.

In a two-server configuration, you are now ready to clone the image of this upgraded node onto the other node. Refer to procedure Cloning the image of one node in a cluster to the other node on page 766.

You have completed this procedure.

4 Rollback to the state prior to the upgrade by typing

```
# /SSPFS_Upgrade.fallback
```

and pressing the Enter key.

The upgraded server is taken down to the OK prompt.

If your server configuration is a	Do
one-server configuration	step 5
two-server configuration	step 6

5 Restore the oracle data on the server using procedure "Restoring the oracle data on an SSPFS-based server" in the ATM/IP Security and Administration document, NN10402-600

You have completed this procedure.

6 Connect to the console port of the other server that has the previous software on it.

7 Boot the server by typing

```
OK boot
```

and pressing the Enter key.

8 Verify the status of replicated disk volumes by typing

```
# udstat
```

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 9
not ACTIVE	contact your next level of support

9 Clone the image of the active server onto the other server. Cloning the image of one node in a cluster to the other node on page 766

Once the clone is complete, the cluster is restored as it was before the upgrade.

You have completed this procedure.

Cloning the image of one node in a cluster to the other node

Application

Use this procedure to clone the image of the active node in a cluster to the inactive node.

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need console access to the Inactive node if this is the first time you clone, or if you replaced the Inactive unit or executed a reverse restore (switched unit 0 and 1)

ATTENTION
Ensure no provisioning activities are in progress, or are scheduled to take place during this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Establish a login session to the Active node using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the Active node using telnet (unsecure) as follows:

a Log in to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the cluster IP address, which automatically defaults to the Active node in the cluster

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d When prompted, enter the root password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the Active node by typing

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

and pressing the Enter key.

where

server
is the cluster IP address, which automatically defaults to the Active node in the cluster

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

b When prompted, enter the root password.

4 Verify the status of replicated disk volumes by typing

```
# udstat
```

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 5
not ACTIVE	contact your next level of support

5 Determine the server profile as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

 X - exit

select -
```

b Enter the number next to the “View” option in the menu.

Example response

```
View
 1 - sspfs_soft (Display Software
     Installation Level Of SSPFS)
 2 - chk_sspfs (Check SSPFS Processes)
 3 - sw_conf (The software configuration of
     the wrtypyxp)
 4 - cpu_util (Overall CPU utilization)
 5 - cpu_util_proc (CPU utilization by
     process)
 6 - port_util (I/O port utilization)
 7 - disk_util (Filesystem utilization)

 X - exit

select -
```

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

Example response

```
=== Executing “sspfs_soft”

SSPFS version: 08.0 Build: 200508421 Server
Profile: cbm850

===”sspfs_soft” completed successfully
```

d Note the Server Profile.

If the Server Profile is	Do
cbm850	step 16
anything else	step 6

6 Verify that all applications on the server are running by typing

```
# servquery -status all
```

and pressing the Enter key.

Example response:

```
APP NAME                              STATUS
========                              ======
SNMP_POLLER                           RUNNING
DELEGATE                              RUNNING
PROP_SRV                              RUNNING
WEBSERVER                             RUNNING
DATABASE                              RUNNING
SAM21EM                               RUNNING
SESMService                           RUNNING
CORBA                                 RUNNING
ORA_ARCHIVE_ROTATOR                   RUNNING
OMPUSH                                RUNNING
BOOTP                                 RUNNING
WEBSERVICES                           RUNNING
ORA_AUTO_BACKUP                       RUNNING
APS                                   RUNNING
NPM                                   RUNNING
```

7 Use the following table to determine your next step.

If	Do
all applications are running	step 10
one or more applications are not running	step 8

8 Start each application that is not running by typing

```
# servstart <app_name>
```

and pressing the Enter key.

where

app_name
is the name of the application that is not in a “RUNNING” state, for example, SAM21EM

9 Use the following table to determine your next step.

If	Do
one or more applications do not start	contact your next level of support
all applications are running	step 10

10 Use the following table to determine your next step.

If this server is	Do
running the NPM software	step 11
not running the NPM software	step 13

Note: The Network Patch Manager (NPM) software is running on this server if NPM appeared in the response from step 6.

11 Verify the Patching Server Element (PSE) server application is running by typing

```
# pse status
```

and pressing the Enter key.

If PSE is	Do
running	step 13
not running	step 12

12 Start the PSE server application by typing

```
# pse start
```

and pressing the Enter key.

If PSE	Do
does not start	contact your next level of support
starts	step 13

13 Use the following table to determine your next step.

If this server is	Do
running the CS 2000 Management Tools software	step 14
not running the CS 2000 Management Tools software	step 16

14 Verify that the SESMservice application is fully functional by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS
-------------------------
COMPONENT                 STATUS
---------                 ------
Proxy Agent               RUNNING
RMI Registry              RUNNING
Snmpfactory               RUNNING
MI2 Server                RUNNING

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

  SESM APPLICATION STATUS: All Applications ready
```

15 Use the following table to determine your next step.

If the SESMService is	Do
not fully functional	contact your next level of support
fully functional	step 16

16 Use the following table to determine your next step.

If	Do
this is the first time you are cloning the unit, or you replaced the unit or executed a reverse restore (i.e. switched unit 0 and unit 1)	step 17
this is not the first time you are cloning the unit, and you did not replace the unit or execute a reverse restore (i.e. switched unit 0 and unit 1)	step 20

17 Use the following table to determine your next step.

If you	Do
know the Ethernet address of the Inactive unit	step 19
do not know the Ethernet address of the Inactive unit	step 18

At the console connected to the inactive node

18 Determine the Ethernet address of the Inactive node as follows:

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

Note: Ensure you are on the Inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

b Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

c At the OK prompt, display the Ethernet address of the inactive node by typing

```
OK banner
```

and pressing the Enter key.

Example response:

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

d Take note of the Ethernet address that is displayed.

At your workstation (login session to the Active node)

19 Start the cloning process by typing

```
# startb <Ethernet address>
```

and press the Enter key.

where

Ethernet address
is the Ethernet address of the Inactive unit

Proceed to step 21

20 Start the cloning process by typing

```
# startb
```

and press the Enter key.

21 Use the following table to determine your next step.

If the system	Do
prompts you to enter the command “boot net - image”	step 22
does not prompt you to enter the command “boot net - image”	step 26

22 Connect to the console port of the Inactive node.

If the console displays	Do
the OK prompt	step 25
the login prompt	step 23

At the console connected to the inactive node

23 Log in using the root user ID and password.

24 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

25 At the OK prompt, boot the inactive node from the image of the active node by typing

```
OK boot net - image
```

and press the Enter key.

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

Example response:

```
SC Alert: Host System has Reset


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

Rebooting with command: boot net - image
.
.
.
SC Alert: Host System has Reset
```

At your workstation (login session to the Active node)

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

Example response:

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

27 Once the cloning is complete, wait approximately 5 minutes before you proceed to the next step.

At your workstation (login session to the Active node)

28 Verify the status of replicated disk volumes by typing

```
# udstat
```

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 29
not ACTIVE	contact your next level of support

At your workstation

29 Establish a login session to the Inactive node using one of the following methods:

If using	Do
telnet (unsecure)	step 30
ssh (secure)	step 31

30 Log in to the Inactive node using telnet (unsecure) as follows:

a Log in to the Inactive node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

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

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d When prompted, enter the root password.

Proceed to step 32.

31 Log in using ssh (secure) as follows:

a Log in to the Inactive node by typing

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

and pressing the Enter key.

where

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

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

b When prompted, enter the root password.

32 Verify the status of replicated disk volumes by typing

```
# udstat
```

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 33
not ACTIVE	contact your next level of support

At your workstation (login session to the Active node)

33 Complete the cloning process by typing

```
# finishb
```

and pressing the Enter key.

You have completed this procedure.

Stopping the PSE server application on an SSPFS-based server

Application

Use this procedure to stop the Patching Server Element (PSE) server application on a Succession Server Platform Foundation Software (SSPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server where PSE resides

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

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

5 Stop the 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.

You have completed this procedure.

Starting the PSE server application on an SSPFS-based server

Application

Use this procedure to start the Patching Server Element (PSE) server application on a Succession Server Platform Foundation Software (SSPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server where PSE resides

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

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

5 Start the 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.

You have completed this procedure.

Completing the CS 2000 Management Tools upgrade

The supported upgrade paths to the (I)SN08 release are listed below. Follow the link associated with the release you upgraded from.

- Completing the upgrade from (I)SN06.2 to (I)SN08 on page 782
- Completing the upgrade from (I)SN07 to (I)SN08 on page 786

Completing the upgrade from (I)SN06.2 to (I)SN08

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)SN08 Post-upgrade checklist

	Activities	√	Procedures
1	Configure the NPM for automatic patch file delivery. Only perform this activity if the NPM is on this server, and you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS). ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Configuring NPM for automatic patch file delivery on page 790.
2	Verify ownership of files in the NPM filesystem.		Execute the following commands: **find /data/npm/Au -type f ! -user npm -name "*ptch*p" -ls** **find /data/npm/Au -type f ! -group maint -name "*ptch*p" -ls** **find /data/npm/database ! -user npm -ls** **find /data/npm/database ! -group maint -ls** **find /data/npm/reports ! -user npm -ls** **find /data/npm/reports ! -group maint -ls** **find /data/npm/logs -type f ! -user npm -ls** **find /data/npm/logs -type f ! -group maint -ls** **find /data/npm/logs -type l ! -user root -ls** **find /data/npm/logs -type l ! -group other -ls** **find /data/npm/pfrs ! -user npm -ls** **find /data/npm/pfrs ! -group maint -ls** **find /data/npm/backup ! -user npm -ls** **find /data/npm/backup ! -group maint -ls** **ls -ld /data/npm/*|grep ^d|grep -v "npm maint"**
3	Restore NPM data. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS		Perform procedure Restoring NPM data on page 795.

(I)SN06.2 to (I)SN08 Post-upgrade checklist

	Activities	√	Procedures
4	Intall the QCA software package on a separate server. ***Note:*** Only perform this activity if you want QCA redundancy. You must have another server that is running the (I)SN08 release of SSPFS.		Perform procedure Installing the QCA software package on a separate server on page 803
5	Verify the upgrade was successful.		Perform procedure Verifying the upgrade was successful on page 805.
6	Back up the (I)SN08 CS 2000 Management Tools server. ***Note:*** It is not necessary to perform this activity in a two-server configuration.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.
			Perform procedure Performing a backup of APS audio files to tape on page 619 or Performing a backup of APS audio files to CD or DVD on page 621.
7	Upgrade the ABS application on the CS 2000 Management Tools server.		Perform procedure Upgrade the ABS software on a CS2000 Management Tools Server on page 809.
8	Add the Audio Media Server to the Integrated EMS topology. Specify the SN08 load for the AMS although it will still be at SN06.2 at this point.		Refer to the Integrated EMS Configuration Management document, NN10330-511.
9	Start the Core Element Manager (CEM).		Perform procedure Starting and stopping the Core Element Manager (CEM) on page 817.

(I)SN06.2 to (I)SN08 Post-upgrade checklist

	Activities	√	Procedures
10	Edit the object properties in the IEMS for the CS 2000 Management Tools SSPFS platform and applications you just upgraded to reflect the new software version.		Refer to either of the procedures that follow to update the software version in the Device Version field. • Editing and viewing object properties using Java Web Client • Editing and viewing object properties using Web Client
11	Upgrade the next component in the end-to-end upgrade.		Refer back to Component Upgrade order on page 5.

Completing the upgrade from (I)SN07 to (I)SN08

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)SN07 to (I)SN08 Post-upgrade checklist

	Activities	√	Procedures
1	Configure the NPM for automatic patch file delivery. Only perform this activity if the NPM is on this server, and you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS). ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Configuring NPM for automatic patch file delivery on page 790.
2	Verify ownership of files in the NPM filesystem.		Execute the following commands: **find /data/npm/Au -type f ! -user npm -name "*ptch*p" -ls** **find /data/npm/Au -type f ! -group maint -name "*ptch*p" -ls** **find /data/npm/database ! -user npm -ls** **find /data/npm/database ! -group maint -ls** **find /data/npm/reports ! -user npm -ls** **find /data/npm/reports ! -group maint -ls** **find /data/npm/logs -type f ! -user npm -ls** **find /data/npm/logs -type f ! -group maint -ls** **find /data/npm/logs -type l ! -user root -ls** **find /data/npm/logs -type l ! -group other -ls** **find /data/npm/pfrs ! -user npm -ls** **find /data/npm/pfrs ! -group maint -ls** **find /data/npm/backup ! -user npm -ls** **find /data/npm/backup ! -group maint -ls** **ls -ld /data/npm/*|grep ^d|grep -v "npm maint"**

(I)SN07 to (I)SN08 Post-upgrade checklist

	Activities	√	Procedures
3	Restore NPM data. ***Note:*** Skip this activity if the NPM is installed on a seperate SSPFS-based server with the IEMS.		Perform procedure Restoring NPM data on page 795.
4	Intall the QCA software package on a separate server. ***Note:*** Only perform this activity if you want QCA redundancy. You must have another server that is running the (I)SN08 release of SSPFS.		Perform procedure Installing the QCA software package on a separate server on page 803
5	Verify the upgrade was successful.		Perform procedure Verifying the upgrade was successful on page 805.
6	Back up the (I)SN08 CS 2000 Management Tools server. ***Note:*** It is not necessary to perform this activity in a two-server configuration.		Perform procedure Performing a backup of oracle data on an SSPFS-based server on page 566.
			Perform procedure Performing a backup of file systems on an SSPFS-based server on page 572.
			Perform procedure Performing a backup of APS audio files to tape on page 619 or Performing a backup of APS audio files to CD or DVD on page 621.
7	Upgrade the ABS application on the CS 2000 Management Tools server.		Perform procedure Upgrade the ABS software on a CS2000 Management Tools Server on page 809.
8	Add the Audio Media Server to the Integrated EMS topology. Specify the SN08 load for the AMS although it will still be at SN06.2 at this point.		Refer to the Integrated EMS Configuration Management document, NN10330-511.

(I)SN07 to (I)SN08 Post-upgrade checklist

	Activities	√	Procedures
9	Complete the Integrated EMS upgrade. ***Note:*** Skip this activity if the IEMS is installed on a separate SSPFS-based server.		Clear the Java Web Start Client cache on the client workstation using procedure "Clearing the JWS cache on a client workstation" in *ATM/IP Security and Administration*, NN10402-600. Check that the user groups and user lists are imported correctly using procedure Listing all groups and users in *Integrated EMS Security and Administration*, NN10336-611.
10	Edit the object properties in the IEMS for the CS 2000 Management Tools SSPFS platform and applications you just upgraded to reflect the new software version.		Refer to either of the procedures that follow to update the software version in the Device Version field. • Editing and viewing object properties using Java Web Client • Editing and viewing object properties using Web Client
11	Upgrade the next component in the end-to-end upgrade.		Refer back to Component Upgrade order on page 5.

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 configuring the Patch File Receipt System (PFRS). You can configure PFRS using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

Once the PFRS is configured, patches are automatically delivered to the NPM database and retrieved for processing on a daily basis.

An option is provided to delete patch files from the drop-off server after they have been retrieved.

Prerequisites

To configure the PFRS, you need the following information:

- 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.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

At the NPM CLUI

2 Configure the PFRS by typing

```
npm> setpfrs <drop-off server> <userID> <delete patches>
```

and pressing the Enter key.

where

drop-off server
is the IP address or hostname of the drop-off server where patch files are to be delivered

userID
is the user ID that will be used to connect to the drop-off server

password
is the password associated with the user ID that will be used to connect to the drop-off server

delete patches
is either Y or N to indicate whether you want the patch files to be deleted from the drop-off server after they have been retrieved

Note: The user ID must have read, write, and overwrite privileges in the FTP user's default directory on this server.

Example response:

```
Enter password for drop box:
```

3 When prompted, enter the password associated with the user ID that will be used to connect to the drop-off server.

Example response:

```
WARNING: You are about to set/reset the Patch
File Retrieval System settings. If these values
are incorrect they may interfere with automatic
delivery of patches to this site.

Do you wish to continue Yes (Y) or N (N)?
```

4 When prompted, confirm you want to continue if acceptable by typing

y

and pressing the Enter key.

5 Review the PFRS settings if required by typing

```
npm> viewpfrs
```

and pressing the Enter key.

You have completed this procedure.

Using the NPM GUI

At your workstation

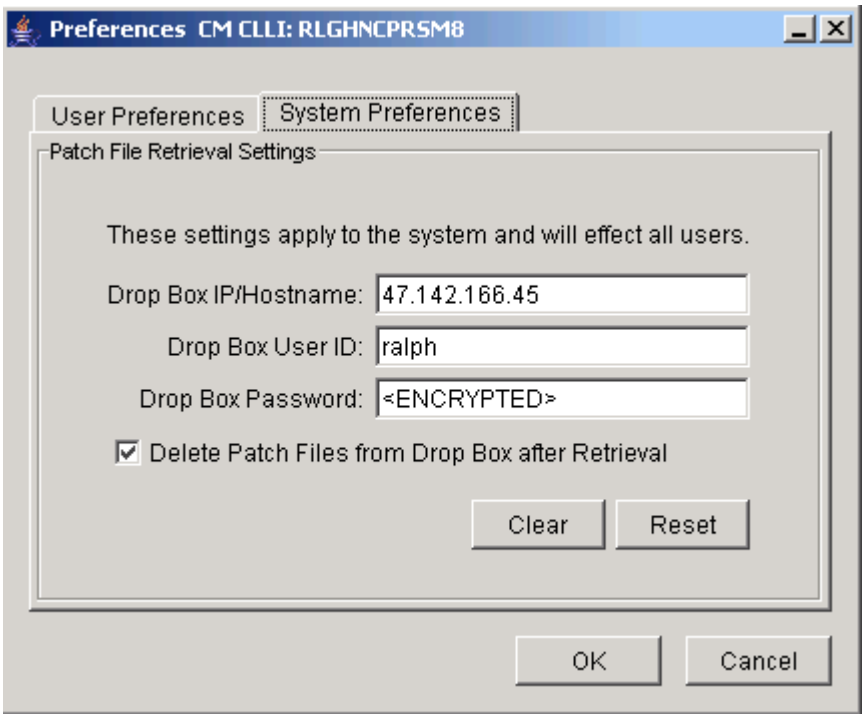
1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

At the NPM GUI

2 On the **Edit** menu, click **Preferences...**.

The Preferences window is displayed.

3 Click the **System Preferences** tab.



4 In the **Drop Box IP/Hostname** field, enter the host name or IP address of the drop-off server where patch files are to be delivered.

5 In the **Drop Box User ID** field, 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.

6 In the **Drop Box Password** field, enter the password associated with the user ID that will be used to connect to the drop-off server.

7 Click the **Delete Patch Files from Drop Box after Retrieval** box if you want the patch files to be deleted from the drop-off server after they have been retrieved, otherwise, leave it blank.

8 Click **OK** to complete the PFRS configuration.

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 576.

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 797.

Prerequisites

The SSPFS and CS2M software upgrades are complete.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the SSPFS-based server where the 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 576, 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 1951, for each set you recorded.

b Restore all user-defined report definitions using procedure Defining reports using the NPM on page 1968, 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 Defining a task using the NPM on page 1957, for each patch you recorded.

e Restore any modifications you made to the SystemPlan using procedure Defining a plan using the NPM on page 1977.

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 797
- Restoring NPM patch files from CD/DVD (Sun Netra 240 only) on page 800

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:

- for a Sun Netra t1400, you need the NPM patch file archive tape
- for a Sun Netra 240, you need the NPM patch file archive CD or DVD

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)

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

Restoring NPM patch files from tape (Sun Netra t1400 only)

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

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

b When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

4 Stop the NPM server application if it is running. If required, refer to procedure "Stopping the NPM server application" in document *ATM/IP Security and Administration*, NN10402-600.

5 Re-initialize the NPM database. If required, refer to procedure "Initializing the NPM database" in document *ATM/IP Security and Administration*, NN10402-600.

6 Insert the NPM patch file archive tape into the drive.

7 Rewind the tape by typing

```
# mt rewind
```

and pressing the Enter key.

8 Access the NPM patch file directory by typing

```
# cd /data/npm/Au
```

9 Restore the NPM patch files to the /data/npm/Au directory by typing

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

and pressing the Enter key.

10 Rewind and eject the tape by typing

```
# mt offline
```

and pressing the Enter key.

11 Remove the tape from the drive.

12 Start the NPM server application. If required, refer to procedure "Starting the NPM server application" in document *ATM/IP Security and Administration*, NN10402-600.

13 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Restoring NPM patch files from CD/DVD (Sun Netra 240 only)

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

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

b When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

4 Stop the NPM server application if it is running. If required, refer to procedure “Stopping the NPM server application” in document *ATM/IP Security and Administration*, NN10402-600.

5 Re-initialize the NPM database. If required, refer to procedure “Initializing the NPM database” in document *ATM/IP Security and Administration*, NN10402-600.

6 Insert the NPM patch file archive CD/DVD into the drive.

7 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.

8 Eject the CD or DVD from the drive as follows:

a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the CD by typing

eject cdrom

and pressing the Enter key.

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

/etc/init.d/volmgt stop

/etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

9 Start the NPM server application. If required, refer to procedure "Starting the NPM server application" in document *ATM/IP Security and Administration*, NN10402-600.

10 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to 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 Log in 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.

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.

Verifying the upgrade was successful

Application

Use this procedure to verify the upgrade of the CS 2000 Management Tools was successful.

Prerequisites

The CS2M software has been upgraded.

Action

Perform the following steps to complete this procedure.

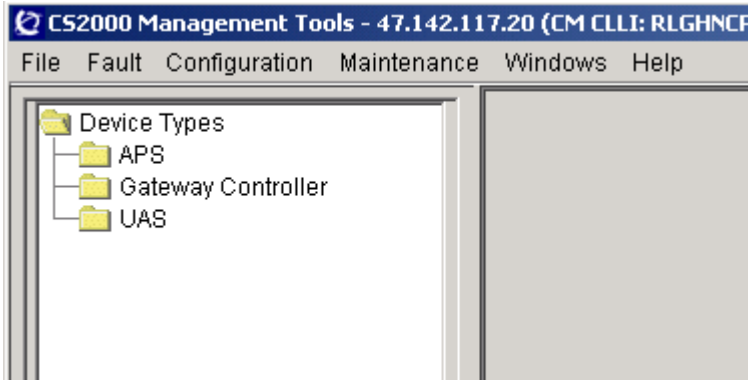
ATTENTION

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” in document *ATM/IP Fault Management*, NN10408-900.

At your workstation

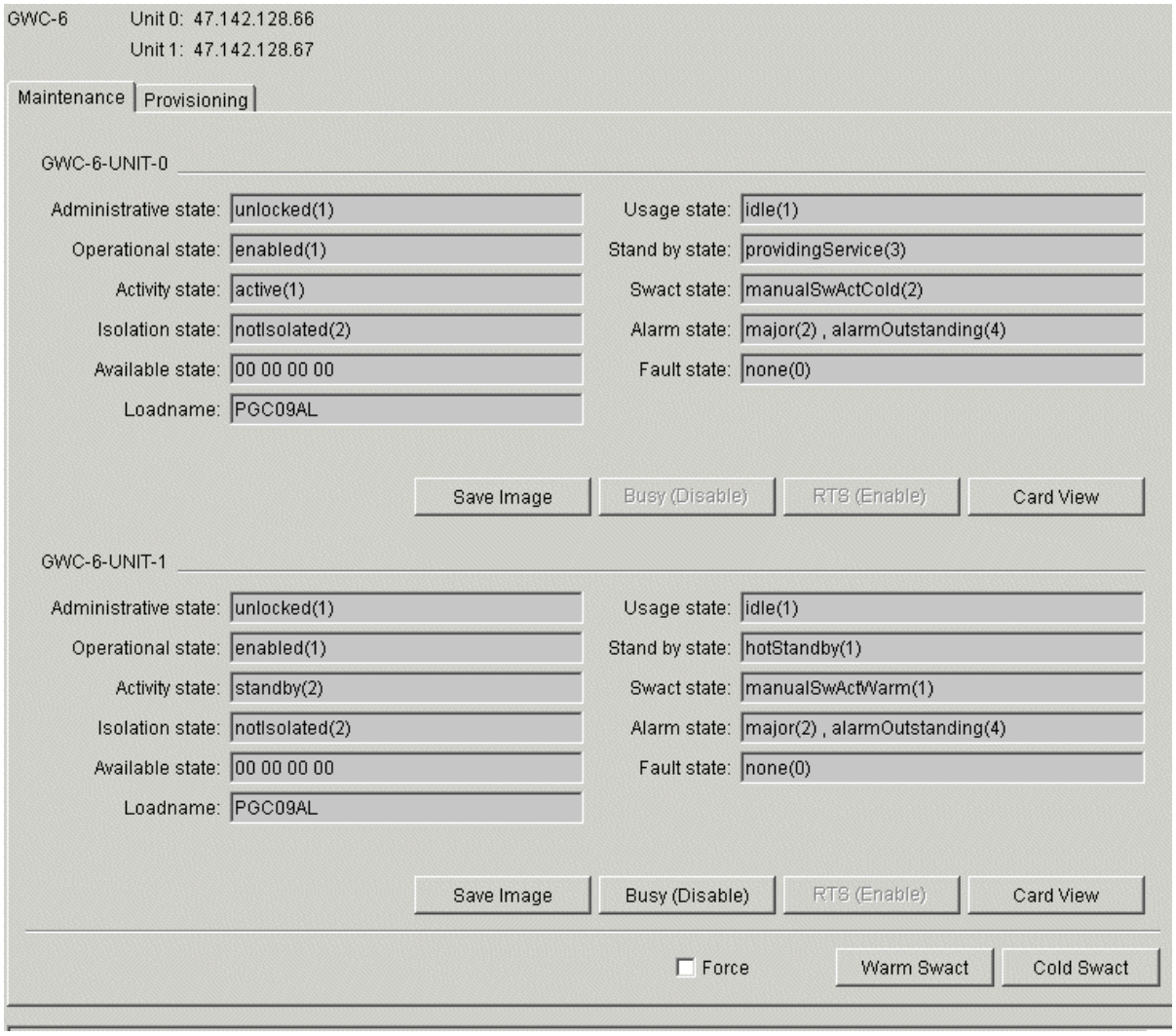
1 Launch the CS2000 Management Tools application GUI, and ensure the topology is displayed correctly as shown in the figure that follows. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

This verifies correct restoration of the database.



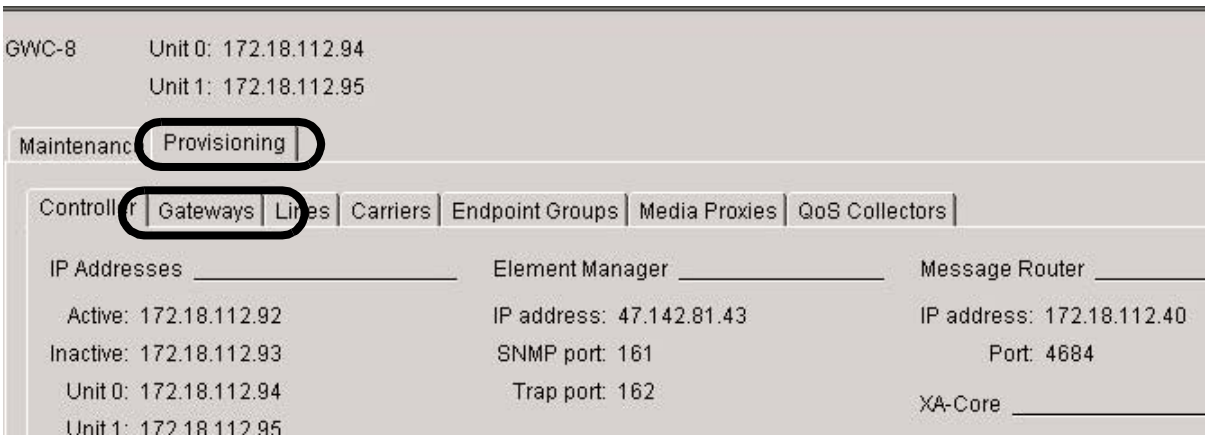
2 Click **GatewayController**, then select a GWC from the list, and ensure correct maintenance states are displayed for the active and inactive units as shown in the figure that follows.

This verifies GWC SNMP communication.



3 Click the **Provisioning** tab, then the **Gateways** tab as shown in the figure that follows, and then click **Retrieve All** to retrieve all subtending gateways.

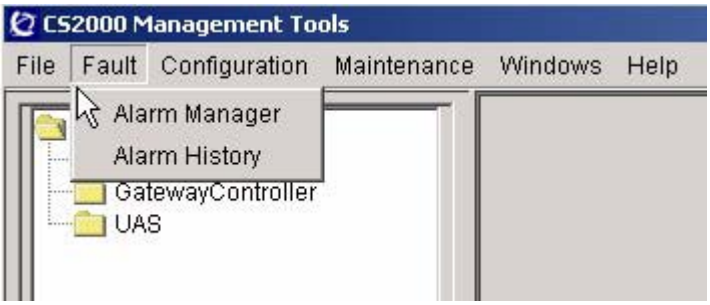
This verifies correct restoration of the database.



4 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.

5 From the **Fault** menu, click **Alarm Manager** as shown in the figure that follows, and verify alarms show up when a maintenance attempt is performed on a GWC unit.



6 Connect to OSSGate. If required, refer to procedure "Connecting to OSSgate" in document *ATM/IP Security and Administration*, NN10402-600.

7 Query a provisioned line (line solutions) or trunk (trunk solutions). If required, refer to the corresponding procedures in document *OSSgate User's Guide*, NE10004-512.

This verifies the SDM OSS APS, DDMS, and core communication path.

8 For line solutions, launch the line maintenance manager (LMM) application GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866. Post, busy, and return a line to service. If required, refer to the corresponding procedures in document *ATM/IP Fault Management*, NN10408-900.

This verifies the SDM - DMA, BMI, and core communication path.

9 For trunk solutions, launch the trunk maintenance manager (TMM) application GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866. Post, busy, and return a trunk to service. If required, refer to associated procedures in document *ATM/IP Fault Management*, NN10408-900.

This verifies the SDM - DMA, BMI, and core communication path.

10 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. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

11 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Upgrade the ABS software on a CS2000 Management Tools Server

Use this procedure to install or upgrade the alternate boot server (ABS) software on the SSPFS-based server that is hosting the CS 2000 Management Tools.

ATTENTION

Nortel recommends that all upgrades be made using the ESD method, see Installing Using ESD on page 1596. ABS upgrades require considerably more user intervention and are therefore more vulnerable to errors.

When you install the USP ABS on the CS 2000 Management Tools server, you must export the X-Windows display of the CS 2000 Management Tools 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 CS 2000 Management Tools 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 CS 2000 Management Tools server, 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 physical access to the CD-ROM on the CS 2000 Management Tools server, do the following:

- **a** Place the USP CD in the CD-ROM drive of the CS 2000 Management Tools server.
- **b** Establish a telnet connection with the CS 2000 Management Tools server.
- **c** Login to the CS 2000 Management Tools server as *root.*
- **d** Enter **cd /cdrom/cdrom0**.
- **e** Enter **ls** and ensure that you see the file `install.bin` listed.
- **f** Proceed to step 4.

2 If you are accessing the CS 2000 Management Tools server CD-ROM from a remote workstation, do the following:

a Establish a telnet connection with the CS 2000 Management Tools server.

b Login to the CS 2000 Management Tools server 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 CS 2000 Management Tools server 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 If you are accessing the CS 2000 Management Tools server from a local PC (with a CD-ROM drive) located on the same subnet, do the following:

a Telnet to the CS 2000 Management Tools server. Type:

Start -> Run -> Type: telnet <CS 2000 Management Tools server IP Address>

b Login as maint

<maint password>

Switch to user root:

Type: su - root

password: <root password>

c Type: cd /data/usp

Type: mkdir absCD

Type: ls (ensure that the absCD folder is present)

Type: chmod -R 775 absCD

Type: chown -R FIELD:maint2

AbsCD

d Check to ensure permissions are set correctly:

drwxrwxrwx 2 FIELD maint2

date *time* absCD

Type: ls -l

e You may minimize the Telnet session.

f Place the USP CD in the local PC.

Note: Some firewalls will block FTP access and interfere with an FTP session.

g Open an FTP session using the following settings:

Parameter	Value
Session/Profile Name:	CS 2000 Management Tools server
Host Address:	<CS 2000 Management Tools server IP address>
User Name:	FIELD
Password:	SERVICE
Turn off Enable Directory Caching and Passive Mode. (These options are available in most FTP programs.)	

h During the FTP session use the download and upload protocols specified in the following table

File extension:	Protocol:
dtd xml txt	ASCII
All other files	binary

i Double click on the "CS 2000 Management Tools server".

A new Explorer window appears.

j Click on the CDROM and expand the directory structure.

Ensure that the CS 2000 Management Tools server has the /data/usp/absCD directory expanded (nothing is currently there).

k Copy the Prewinnt, Program and redist folders and all files from the local PC CDROM to the CS 2000 Management Tools server in the absCD folder:

i Right click on the one of the folders and drag it over the CS 2000 Management Tools server absCD folder. Choose the Copy Here option from the pop-up menu.

ii Repeat this step for each folder (Prewinnt, Program and redist). You will see the Hummingbird FTP File Transfer window while coping the files.

l Copy all files from the CDROM root directory:

i Double-click on the CDROM and highlight ALL files (right window)

ii Drag and drop onto the absCD folder (CS 2000 Management Tools server)

Note: DO NOT copy the Folders that were completed in step k above.

m Check the CS 2000 Management Tools server /absCD folder to ensure that all files and the Prewinnt, Program and redist folders (and sub-folders) exist.

n Close the Explorer window.

o This ends the procedure.

4 Install the new version of the ABS software on the CS 2000 Management Tools server:

a Ensure that your X-Windows server software is running and that host access permissions are allowed for the CS 2000 Management Tools server. Refer to your X-Windows server software manual for details.

b Login to the CS 2000 Management Tools server as *field.*

c Once logged in, change to the root user (*su root).*

d 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.

e Enter **export DISPLAY**. To confirm the export, enter **echo $DISPLAY**.

f If this is the first time an ABS has been installed on this CS 2000 Management Tools server, proceed to step j.

g If you are upgrading from:

i USP8/SN06:
Enter **cd /data/usp/ntssgusp/abs** and then enter:
./Uninstall_ABS &

ii USP9/SN07 and later:
Enter **cd /data/usp/ntssgusp** and then enter:
./Uninstall_Universal_Signaling_Point &

It may take 2 to 3 minutes for the application to launch and be fully populated with data.

iii When the uninstall wizard opens, click **Next**, then choose **Complete uninstall** or enter **1** if you are in the console mode.

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 CS 2000 Management Tools server CD-ROM from a remote workstation, enter **cd /cdrom/cdrom0**. If you have direct access to the CS 2000 Management Tools, enter **cd /data/usp/absCD**.

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 d through f:

```
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 CS 2000 Management Tools server. Refer to your X-Windows software manual for details.

If the errors persist, contact your Nortel Networks support representative.

l When the Introduction panel appears, click **Next**.

m On the Package Selection panel, select the **USP Software Loads and ABS Manager** package. If you will be using the CS 2000 Management Tools 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**.

5 Launch your web browser.

6 In the Address field, enter the name or IP address of the SSPFS-based server where the CS 2000 Management Tools are installed.

The Application Launch Point page appears.

7 Click **Application Launcher**.

The Login window appears.

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

The Application Launch Point appears.

9 Verify there is only one USP application link and that it is functional.

If	Do
multiple USP application links are present	step 10
only one USP link is present, but it is not functional	step 10
only one USP link is present, and it is functional	step 11

10 Execute step 4g to uninstall the software, then repeat step 4 excluding step 4g, to reinstall the software.

11 Verify the new version of the ABS software on the CS 2000 Management Tools server:

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 CS 2000 Management Tools server.

c Ensure that the DISPLAY environment variable is set up correctly. Repeat steps 4d through p 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**. You must enter the password for the ABS for the login to go through.

12 If you are installing the software on the CS 2000 Management Tools server from a remote workstation, enter **rm -rf /data/usp/absCD** to delete the temporary files.

13 Remove the USP Software CD-ROM disk from the drive using the **eject cdrom** command. The installation is complete.

Starting and stopping the Core Element Manager (CEM)

Application

Use this procedure to start or stop the Core Element Manager (CEM).

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

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

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server
is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration

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

b When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

4 Verify the status of the CEM by typing

```
# servman query -status -group CEM
```

and pressing the Enter key.

5 Use the following table to determine your next step

If you want to	Do
start CEM	step 6
stop CEM	step 7

6 Start the CEM by typing

```
# servstart CEM
```

and pressing the Enter key.

Example response:

```
CEM server successfully started
```

Go to step 8

7 Stop the CEM by typing

```
# servstop CEM
```

and pressing the Enter key.

Example response:

```
CEM server successfully stopped
```

8 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Multiservice Switch (MSS) 15000/20000

Before upgrading the Multiservice Switch 15000

Perform the required prerequisite upgrade as follows:

Network	MSS 15000/20000 applies to:	Previous Upgrade
ATM	PT-AAL1	CS 2000 Core Manager on page 303
	UA-AAL1 and PT-AAL2	CS 2000 Management Tools and Clients (CMT) on page 523
IP	PT-IP and UA-IP[1]	CS 2000 Management Tools and Clients (CMT) on page 523
Tri-Modal	all applications	CS 2000 Management Tools and Clients (CMT) on page 523

1.Includes IP International: PT-IP and UA-IP

After upgrading the Multiservice Switch 15000

Perform the next required upgrade as follows:

Network	MSS 15000/20000 applies to:	Next Upgrade
ATM	PT-AAL1 and UA-AAL1	Peripheral Modules on page 1065
	PT-AAL2	SAM21 Shelf Controller on page 1280
IP	PT-IP[1]	Peripheral Modules on page 1065
	UA-IP[2]	Media Gateway (MG) 9000 Manager on page 1103
Tri-Modal	all applications	Peripheral Modules on page 1065

1.Includes IP International: PT-IP
2.Includes IP International: UA-IP

About the Multiservice Switch 15000

The Nortel Networks Multiservice Switch 15000 node provides an ATM-based switching platform that can be used to build the ATM network core for PT-AAL1, UA-AAL1, and Tri-modal solutions. The node provides the ATM core with general routing and ATM switching as well

as connectivity for a variety of services including voice, multimedia, and data.

PT-AAL1 and UA-AAL1 application procedures begin with AAL1 applications on page 822.

In a UA-IP solution the Multiservice Switch 15000 or Multiservice Switch 20000 serves as the edge router to aggregate MG 9000 and MG 15000 traffic within an office.

UA-IP and PT-IP application procedures begin with with IP Applications on page 934.

Upgrading a Nortel Networks Multiservice Switch 15000/20000 consists of three basic phases:

- Preparation: the phase during which information is gathered and software is downloaded.
- Migration: the phase during which pre-HSM checks are made, the migration occurs, post-HSM checks are made,
- New feature activation: the phase during which new mandatory features are activated, problems are fixed, and the migration is rolled back if required.

AAL1 applications

MSS15000/20000 PT-AAL1 and UA-AAL1 applications

The migration phase describes what happens on the node during a hitless software migration and is divided into two parts to reflect the two migration options available:

- HSM from the Multiservice Switch 15000 node using MDM Command Console.
- HSM using MDM Succession ATM Software Migration (SASM) tool

Using the SASM tool to perform an HSM provides an automated way to perform an HSM which reduces the chance of errors and increases the speed and efficiency of the software migration.

Software migration

An upgrade to a Nortel Multiservice Switch 15000 node is also known as a hitless software migration. During an upgrade of the Packet Trunking - AAL1 (PT-AAL1) and Universal Access AAL1 (UA-AAL1) solutions' components, the nodes must be upgraded so that you have access to new, enhanced, or corrected software applications.

An operator can choose to perform a software migration from either the Nortel MDM Command Console or the MDM Succession ATM Software Migration (SASM) tool.

This section describes the overall hitless software migration process. For overview information on performing a hitless software migration from the MDM Command Console, see What happens to the node during a hitless software migration on page 857. For overview information on performing a hitless software migration from the SASM, see Performing HSM using MDM SASM on page 916.

Upgrade software to add new functionality to Nortel Multiservice Switch 15000 nodes by activating a new version of software.

Prerequisites to performing a software upgrade

CAUTION
Calls in the process of being set up are dropped
This strategy removes inactive 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.

CAUTION
Loss of stable SVC connections may occur
When you perform the hitless software migration, a loss of SVC connections may occur. Although stable SVC calls should remain active in a redundant processor configuration, exercise caution when performing this upgrade.

CAUTION
The < ch pr > command used for the application of the 'migrated to' release patches could fail when migrating from PCR6.1.1 to a later release with patches
The following steps must be followed in order to ensure a successful migration from PCR6.1.1 to a later release with patches.

1. Ensure that the node to be migrated is patch current by applying and activating all applicable patches in the most recent patch baseline for PCR6.1.1. If the application of the full baseline patchlist is not feasible, then, as a minimum, either patch base7T1044A (for MSS 7400) or patch baseFT1044A (for MSS 15000/20000) must be applied and activated.

2. Download the software to migrate to including the patches.

3. Proceed with the software migration including the patch avl and required patchlist.

- Nortel MDM software is backwards compatible and can manage the current and previous releases of Nortel Multiservice Switch hardware. However, MDM software is not necessarily forward compatible. As a result, you should upgrade MDM servers before upgrading the nodes they manage. To upgrade MDM servers, see NN10185-461 *Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*.
- If you have DS-1 IMA interfaces using the Edgelink100 MUX, ensure that you use the Edgelink100 MUX software (R3.3) during the SN08 upgrade. Contact Telco Systems to get the Edgelink100 MUX software and upgrade procedures: http://www.telco.com/products/Transport/M13Multiplexers/EdgeLink100/
- While the CS2000 Core Manager is being upgraded, a short interruption of OAM&P management occurs if the SDM is in the OAM flow to the OSS. To upgrade the CS2000 Core Manager, see NN10060-461, *CS2e Upgrades*.
- Make sure you have MAP-level access to the CS2000 Manager and the SAM 21 if you have *Pbg* Components configured.

- Ensure that all configuration changes from the Global Bulletin System (GBS) and the 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 NN10070-461 *Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1*.
- The Multiservice Switch 15000 nodes in your network must be upgraded one at a time to ensure that no service interruption occurs. For in-band OAM topologies, you must upgrade the nodes in the following sequence:
  - upgrade all the remote nodes first
  - upgrade the Multiservice Switch 15000 Gateway node that is not preferred. For more information about preferred and non-preferred gateways, see NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP* and In-band OAM quick reference on page 932.
  - upgrade the preferred Multiservice Switch 15000 Gateway node last. For more information about preferred and non-preferred gateways, see NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP*.
- You need an extensive knowledge of Unix, Multiservice Switch software, and Carrier Voice over IP portfolio architecture.
- You need a valid node user ID configured for local access as well as, access to ftp, fmip, telnet and the Nortel MDM server.
- You need a:
  - user ID for Web support (see Download release notes on page 831)
  - user ID for root access to the MDM tools.
  - MDM user ID for software download.
  - user ID for general access to MDM.
  - Multiservice Switch 15000 node 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.

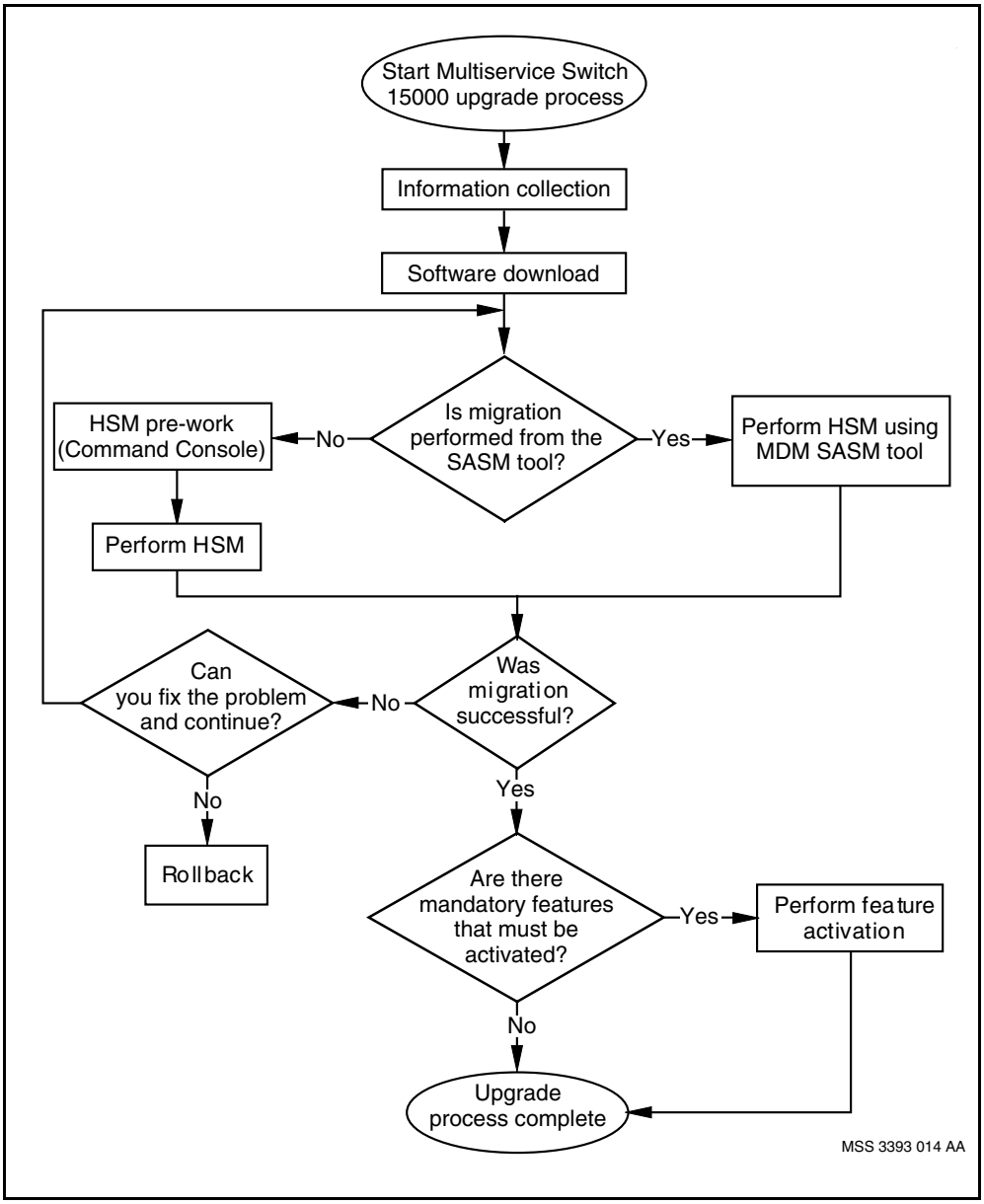
- Nortel recommends that you perform the tasks involving commands issued from the command line using the MDM Command Console tool rather than a Telnet session. For more information on using the Command Console, see 241-6001-804 *Nortel Multiservice Data Manager Workstation Utilities*.
- Ensure that all 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.
- The nodes must be connected to the 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 the *Nortel Multiservice Switch Release Notes* 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 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 Multiservice Switch 15000 software upgrade task flow on page 827 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. See the section on removing unused software in NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*.

Multiservice Switch 15000 software upgrade task flow

The figure Multiservice Switch 15000 software upgrade task flow on page 827 shows you the sequence of tasks you need to perform to upgrade software. To link to any procedure, go to the list that follows the task flow chart.

Multiservice Switch 15000 software upgrade task flow



Work flow navigation

- Information collection on page 829
- Downloading and backing up Multiservice Switch software on page 836
- HSM (Command Console) pre-work on page 864 for migrations performed from the Command Console
- HSM (Command Console) activation on page 884 or HSM (MDM SASM tool) activation on page 913
- Feature activation on page 927
- “Rollback” in NN10070-461 *Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1*

Information collection

Collect information to identify and avoid any compatibility issues that could prevent a software migration from completing successfully.

Prerequisites to information collection

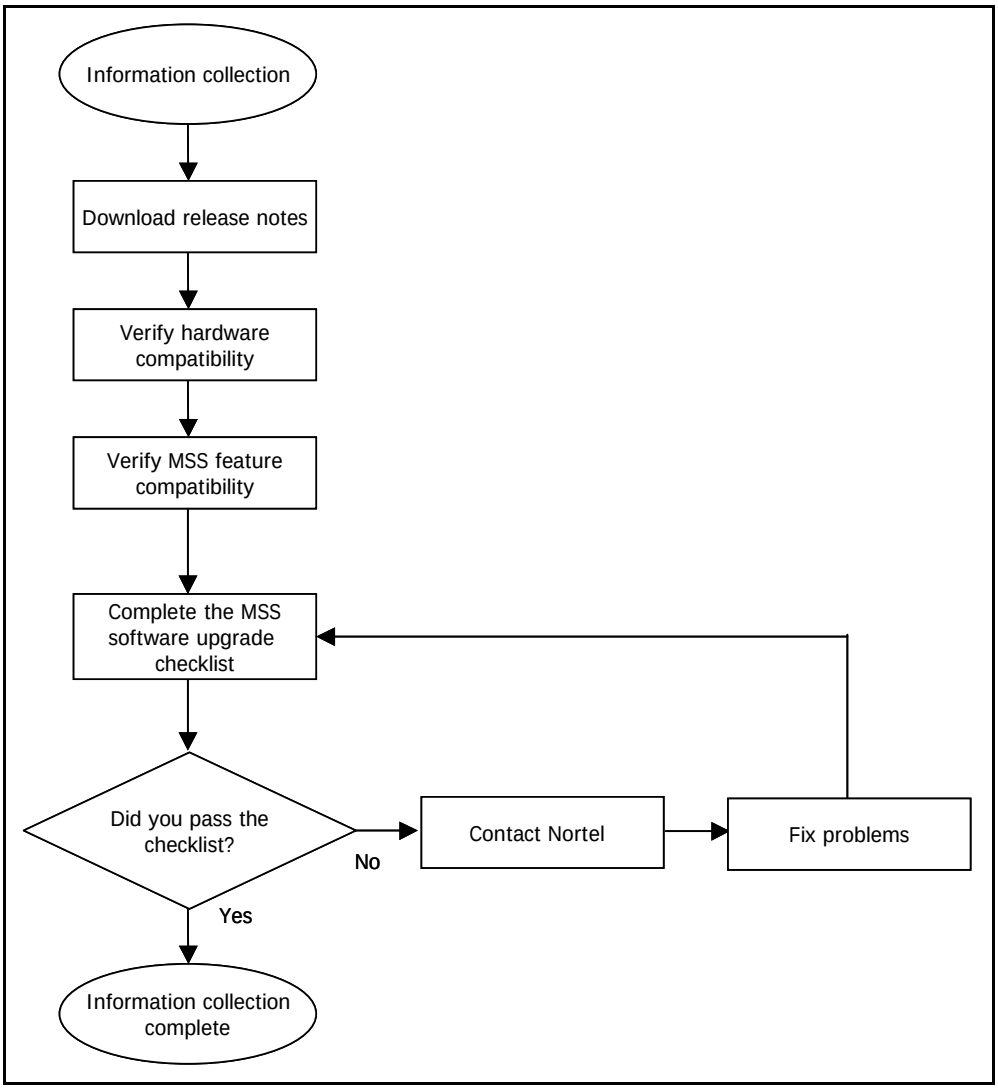
Ensure you have:

- determined the order in which you will upgrade the Nortel Multiservice Switch nodes in your network
- determined that the Nortel MDM servers have already been upgraded
- confirmed which release of software is active on the node
- determined an upgrade path to identify which release you are migrating to
- confirmed that the node is operating without known errors or failures.

Information collection task flow

The task flow shows you the sequence of tasks you perform to collect information about the upgrade. To link to any procedure, go to Work flow navigation on page 831.

Information collection task flow



Work flow navigation

- Download release notes on page 831
- Verify hardware compatibility on page 832
- Verify node feature compatibility.
- Complete the software upgrade checklist on page 833

Download release notes

Download the release notes for Nortel Multiservice Switch in Carrier Voice over IP PT/UA-AAL1 solutions to collect specific information affecting hardware and services for each of Multiservice Switch equipment software release (PCRs) and Multiservice Switch for Carrier Voice over IP software releases involved in the migration.

From your browser

1. Go to the Nortel public website.

   http://*www.nortel.com/*
2. In the section titled Support & Training, click *Technical Documentation*.
3. Click *Passport* from the list of products.
4. Click the *Documentation* link under Passport 15000 for Succession PT/UA-AAL1.
5. A security screen appears requesting your user ID and password.
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.

1. Note the product engineering codes (PECs) of all the processor cards used in your node.

   d shelf card/* prc

2. Review the hardware compatibility section in the *Nortel 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 Multiservice Switch Release Notes* for each release in the migration path.

Verify node feature compatibility

Verify the node's compatibility with the new software to confirm that your configuration of services and features will not be negatively affected by the software migration.

1. Create a list of all the applications loaded on the node.

   d -p sw lpt/* fl, log

2. Refer to the *Nortel 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 compatibility between your existing features and your migration path, contact your Nortel Service Representative before beginning the migration.

Complete the software upgrade checklist

Complete this software upgrade checklist to confirm that all potential complications have been considered and eliminated. Use the information gathered while performing the Work flow navigation on page 831.

Multiservice Switch software upgrade checklist

Task	Yes	No	Date and Comments
A migration order has been established for all the Multiservice Switch 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 applications, features and software.			
Migration operator has complete knowledge of all software versions in the migration.			
The *Nortel Multiservice Switch Release Notes* for all 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.			
Network statistical data is collected. (Install NetRx if required. See http://*www.nortel.com*)			

Multiservice Switch software upgrade checklist

Task	Yes	No	Date and Comments
Multiservice Switch hardware is compatible with all releases in the migration plan.			
Multiservice Switch 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 MDM server acting as an SDS.			
The software version patches to be applied have been downloaded and installed on the MDM server acting as an SDS.			
All configuration changes from the Global Bulletin System (GBS) and the Method of Procedure (MOP) are reflected on the node before performing the upgrade.			
The file system is synchronized 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?			
Enter “display software avlist” to find the software version. The software version currently running on the node is:			
Enter “display software patch” to find the current patches. The current patches running on the node are:			
The intended software after the migration is:			

Multiservice Switch software upgrade checklist

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 are:			

Downloading and backing up Multiservice Switch software

Before you can begin your upgrade, ensure that the correct version of Nortel Multiservice Switch software and the correct patches have been downloaded to the Nortel 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 nodes.

Prerequisites to software download and backup

Ensure that:

- within the PT-AAL1 and UA-AAL1 solutions, one of the Nortel MDM servers has been configured as a software distribution site (SDS). The server acting as the SDS manages, stores, and provides access to Nortel Multiservice Switch software and patches. To upgrade your Multiservice Switch nodes, you must download the required software from this server to the nodes.
- the download of the software and patches onto the server acting as the SDS and the download of the software and patches from this server to the nodes can be done at any time prior to the hitless software migration. 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 and ip. If your nodes have been configured with in-band OAM or support for MG9000 Internode ESA, you will also have the wanDte application. If patches have been applied, you will also have the patch application provided you are starting at SN07. The application version list must not contain any additional applications.

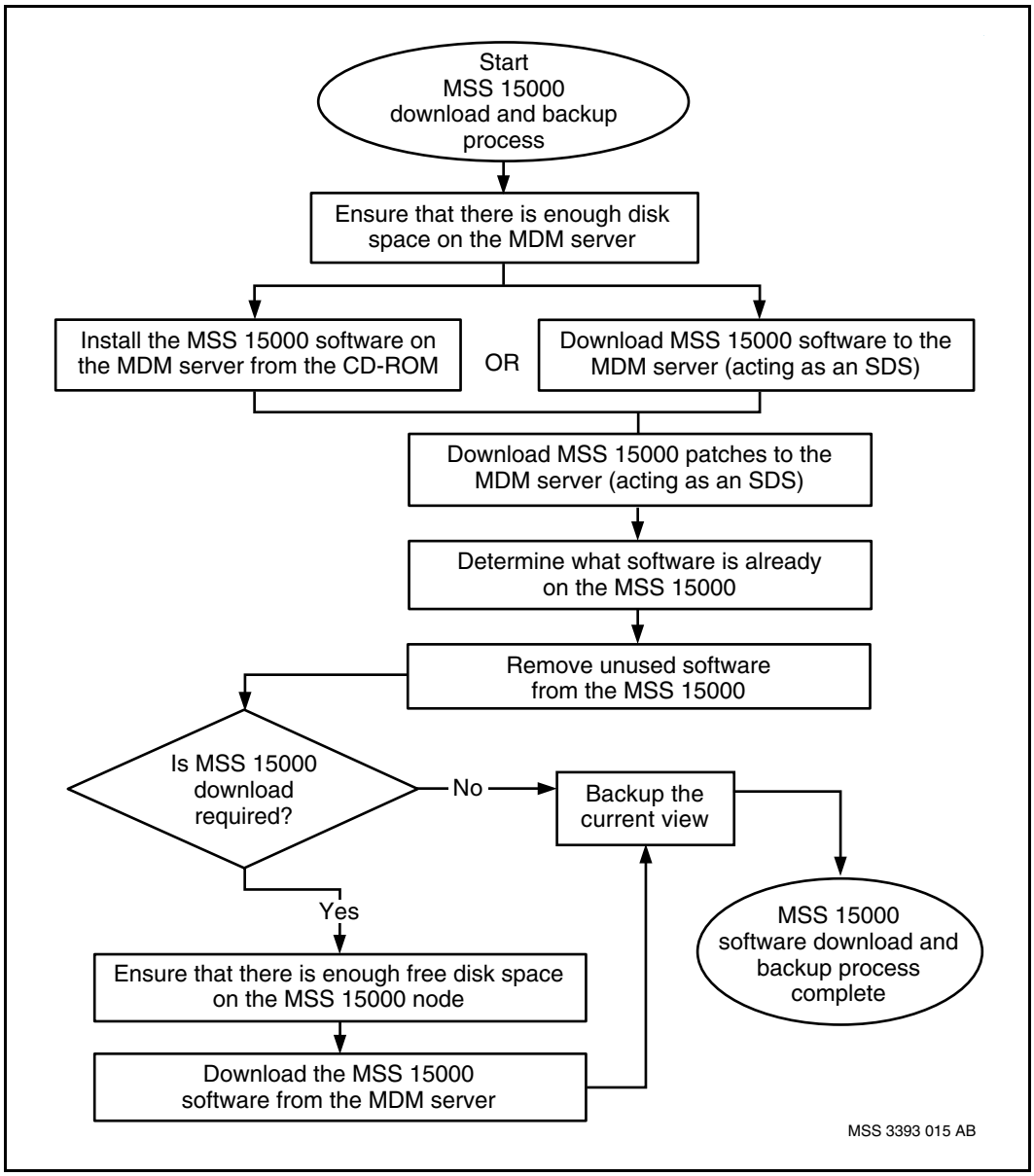
  Note: There is a prerequisite patch for migration from SN06.2 to SN08. Patch baseFT420A_CE01S3H must be applied in SN06.2 before upgrading to SN08 to allow patch activation in SN08. Patch baseFT420A_CE01S3H is available on www.nortel.com under Support & Training / Software Downloads / Product Family: select Passport / Product: select Multiservice Switch 15000 for Succession PT/UA-AAL1.

Software download and backup provisioning views task flow

This task flow shows you the sequence of tasks you need to perform to configure the Nortel MDM as an SDS, download the Nortel Multiservice Switch software and patches to the server, and finally to download the software and patches to the nodes.

Note: These procedures are located in two documents. Four are in this document, and the remaining procedures are in NN10600-270 *Nortel 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 840
- Download the software to the server from the Nortel website on page 841 or
- Download software patches to the server from the website on page 843
- Install the software on the server from a CD-ROM on page 846
- “Determining what software is already on the node” in NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*
- “Removing unused software from the node” in NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*
- Ensuring that there is enough free space on the node on page 848
- Download the software from the server on page 850
- Back up the current view on page 854

Ensuring that there is enough disk space on the server

Before downloading the required software and patches to the Nortel MDM acting as the SDS, verify that the server has sufficient disk space to hold the software release.

Note: Keep the patch AV on the SDS. Nortel recommends that at least one SDS be available with the current software on the MSS.

Prerequisites

Ensure that the:

- Nortel Multiservice Switch 15000 software has approximately 300 Mbytes of space. See the *Nortel Multiservice Switch Release Notes* to verify the disk space required for this release.

From the MDM acting as the SDS

1 Log in.

2 Determine how much disk space is available on the partition containing the Multiservice Switch software:

df -k /localdisk/pp15ksw/software

Note: This directory path assumes that the user ID configured to access the software on the SDS 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 300 Mbytes.

4 If there is not 300 Mbytes of space, remove files from the 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, atm, ip). 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 log in 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 the Nortel website

After verifying that the Nortel MDM server acting as the SDS has sufficient disk space, you can begin to download the Nortel Multiservice Switch software from the 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 Nortel Web access account with a user name and password. Contact your Nortel customer representative for more information on accessing the site.
- Refer to the software downloads area of the website (*www.nortel.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 MDM server.
- Ensure that there is enough disk space on the server.

From the MDM server acting as the SDS

1 Log in.

2 On the web, go to *www.nortel.com*.

3 From Support & Training, select *Software Downloads*.

4 Under the Product Families link, select the family *Passport*.

5 Under the Passport 15000 for Succession PT/UA-AAL1 (Now known as: Multiservice Switch 15000 for Succession PT/UA-AAL1 section), select *Software*.

The Software Downloads window opens.

6 Select the version of the release software you want to download.

A Log In window opens.

a When prompted to log in, enter your user name and password for the web access log in.

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.

7 Click the load name listed beside the File Download heading.

A Save As dialog opens.

8 Specify a folder in the home directory of the MDM user to indicate where you want the patch placed. This is typically:

/localdisk/pp15ksw/software

9 Click **Save**.

10 On the server, change directories to the directory containing the software (This is the same directory you specified in step 8.):

cd /localdisk/pp15ksw/software

11 Uncompress the software file:

uncompress <load_name>.tar.Z

12 Untar the software file:

tar -xvf <load_name>.tar

13 Repeat step 7 through step 13 for every software file you want to download.

14 Remove the tar file: **rm -r <swload_name>.tar**

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 the website

In addition to the main software release, you may need to download patches from the Nortel website to the MDM server, which is acting as the SDS. When you download the patches from this website, a copy of the patches is placed in the specified directory.

As of SN07, all MSS patches are delivered as a single application version (Av), the Patch Av. The Patch Av includes all the patches associated with a given software version. Reset and TAP patches are delivered with the Patch Av. If you have enabled Patch auto-application, MSS TAP patches will be automatically applied, however, reset patches are not eligible for auto-application and must be manually applied. The Patch Av must not be confused with a patched Av, however, a Patch Av can include any patches that have been built specifically for a patched Av based on the release.

The Patch Av ensures that your switches have access to the complete set of TAP and Reset patches at a given level. The Patch Av does not need to be provisioned in the Sw avList to view the patches contained within it, however, it must be provisioned in the Sw avl to be added to the Sw patchList. If you choose to display the patches for the patch Av, all the patches for all the Avs (base, atmNetworking, ip, and so forth) are displayed. If you choose to display the patches for the base Av, all the patches on the CP disk for that SW level will be displayed.

The Patch Av tracks the patches for each software level. The AD file contains a list of Patch Version files for that software level. Each Patch Version (PV) file reflects the status of patches when the PV file is created and displays which patches are calculated and applied. The status of the patches on the switch is tracked in version files within the Patch Av. Refer to NN10600-272 *Nortel Multiservice Switch 7400/15000/20000 Upgrading Software* for more information about patching.

Prerequisites

- You need an account with a user name and password. Contact your Nortel customer representative for more information on accessing the website.
- Refer to the software downloads area of the website (*www.nortel.com*) to determine the software patches that you must install on the node. If there are no patches listed for this release, it means that there are no patches currently required for this release.
- Verify which Nortel Multiservice Switch software and patches are available on the MDM server.

- Ensure that there is enough disk space on the server.
- Regular software has been downloaded.

From the MDM server acting as the SDS

1 Log in.

2 On the web, go to *www.nortel.com*.

3 From Support & Training, select *Software Downloads*.

4 Under the Product Families link, select the family *Passport*.

5 Under the Passport 15000 for Succession PT/UA-AAL1 (Now known as: Multiservice Switch 15000 for Succession PT/UA-AAL1) section, select *Software*.

The Software Downloads window opens.

6 Click the patch that you want to download.

The Software Downloads: Software Detail Information window opens.

a When prompted to *Login* enter your user name and password for the web access log in.

Note: If there are no patches listed for this release, there are no patches currently required for this release. You can move on to the next task in the upgrade process.

7 Select the patch name listed beside the File Download heading.

A Save As dialog is displayed.

8 Specify a folder in the home directory of the MDM user to indicate where you want the patch placed. This is typically:

/localdisk/pp15ksw/software

9 Click *Save*.

10 On the server, change directories to the directory containing the patch (This is the same directory you specified in step 8.):

cd /localdisk/pp15ksw/software

11 Uncompress the patch file:

uncompress <patch_name>.tar.Z

12 Untar the patch:

tar -xvf <patch_name>.tar

13 Repeat step 6 through step 13 for every patch you need.

14 Remove the tar file.

Variable values

Variable	Value
<patch_name>	The name of the patch that you want to download.

Install the software on the server from a CD-ROM

An alternative to downloading the software from the server acting as the SDS, is to install the software from Nortel Multiservice Switch CD-ROM using the installation program.

Prerequisites

- You need a copy of Nortel Multiservice Switch SPCR6.1 software CD. Contact your Nortel customer representative for information on how to order a CD.
- You need the IP address of the Nortel 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 the website on page 843.

From the MDM server that is the acting SDS

1 Log in to the server.

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 Multiservice Switch 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 MDM server.

10 Eject the CD from the CD-ROM drive:

eject cdrom

Ensuring that there is enough free space on the node

Before downloading Nortel Multiservice Switch software and patches from the server, ensure that the node has sufficient disk space to download the software applications.

Prerequisites

- Ensure that there is sufficient space to download the software files for the following applications: base, networking, atmNetworking and ip. If your nodes have been configured with in-band OAM or support for MG9000 Internode ESA, you will also have the wanDte application. If patches have been applied, you will also have the patch application. The application version list must not contain any additional applications. The amount of space required for the (up to) six applications is approximately 250 Mbyte.
- If you need to upgrade the fabric card firmware with this release, you will 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 the *Nortel Multiservice Switch Release Notes* and the software downloads area of Nortel website (*www.nortel.com*) to determine the software load and patches that you must install, and the amount of disk space required. See the section on determining which software is already on the node in NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*.

From the node

1 Log in to the 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 250 Mybte.

Note 1: If your nodes have been configured with in-band OAM, you need to allocate additional space for the wanDte application.

Note 2: 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 using the **tidy Software** command. See the section on removing unused software in NN10600-270 *Nortel 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 *Nortel Multiservice Data Manager Management Data Provider*.

Download the software from the server

Before beginning the hitless software migration, you need to download the software from the Nortel MDM server acting as the SDS, to the nodes.

Prerequisites

- Download the software to the server from the Nortel website on page 841 or install the software from a CD-ROM.
- Download software patches to the server from the website on page 843.
- Perform the procedure “Ensuring that there is enough free space on the file system” in NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*.
- You need to download the software files for the following applications: base, networking, atmNetworking and ip. If your nodes have been configured with in-band OAM or support for MG9000 Internode ESA, you will also have the wanDte application. If patches have been applied, you will also have the patch application. The application version list must not contain any additional applications.
- 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 firmware on page 899.
- Refer to the software downloads area of Nortel (*www.nortel.com*) website to determine the software load and patches that you must install on the node. If there are no patches listed for this release, it means that there are no patches currently required for this release.

  VoA patches are located on *www.nortel.com under* Support & Training/Software Downloads/Product Family: select Passport/select product: Multiservice Switch 15000 for Succession PT/UA-AAL1.
- You need the IP address of the MDM server acting as the SDS.
- You need the user ID that has read access to the node and the associated password for that user ID. This is the user ID for the folder specified in step 8 of Download software patches to the server from the website on page 843.
- If you are using the CLI to perform this upgrade, we recommend that you use the MDM Command Console tool. For more information on opening the Command Console, see 241-6001-804 *Nortel Multiservice Data Manager Workstation Utilities*.
- Support for multiservices is not available.

From the node

1 Log in to the node using 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 (if your nodes have been configured with in-band OAM)
- fabric_CF01S1E
- patch_CF01S1E

Nortel Multiservice Switch system downloads any patches associated with the application versions you specify.

Sample output

```
> set  Software Download avListToDownload ! base_CF01S1E
networking_CF01S1E ip_CF01S1E wanDte_CF01S1E atmNetworking_CF01S1E
Sw Dld

ok              2005-01-07 14:46:46.14
```

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 the Nortel website (*www.nortel.com*) were downloaded:

list Software ApplicationVersion/patch_CF01Sxxx Patch/*

Variable values

Variable	Value
<application_version>	A space-separated, case sensitive list of application versions. Download the new version of the base, networking, atmNetworking and ip. If your nodes have been configured with in-band OAM or support for MG9000 Internode ESA, you will also have the wanDte application. If patches have to be applied, you will also have the patch application. The application version list must not contain any additional applications. If you need to upgrade the fabric card firmware with this release, download the fabric application. For more information, see Upgrade the fabric firmware on page 899.
i960	An attribute indicating that the i960 processor type is being used. This attribute is always required.
<ipAddress>	The IP address of the MDM server acting as the SDS.
<password>	The password for the <userid> of the MDM server acting as the SDS.

Variable values

Variable	Value
PPC	An attribute indicating that the PowerPC processor type is being used. This attribute is always required.
<userid>	The <userid> for a MDM account that contains the Multiservice Switch software to be downloaded The value is usually pp15ksw.

Back up the current view

Save a view from a node using the MDM Backup and 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 MDM server or another node. It can also be a Software Distribution Site (SDS) configured to store backed-up node service data.
- Verify that the backup site has enough space to accommodate the backup. For more information, see NN10600-272 *Nortel Multiservice Switch 7400/15000/20000 Upgrading Software*.
- The MDM Backup and 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 MDM Backup and Restore tool backs up only the node's configuration data. It does not back up the software.
- The Backup server, the Restore server, the Backup Provider, and the Restore Provider must all be running on the MDM server for the MDMBackup and Restore tool to function properly. Using the 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 *Nortel Multiservice Data Manager 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 Multiservice Switch 7400/15000/20000 Software Installation* for information on making them the same.
- The 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.

CAUTION

This procedure backs up all views currently stored on each node and should be done during a maintenance window.

From the node

1 Log in with the appropriate permissions.

2 Display on-switch provisioning to determine which files you need to back up:

display -o prov

The *commitedFileName* is the view you need to save. The *committedFileName* and the *currentViewFileName* should be the same.

Sample output

```
1> d prov
Prov
adminState = unlocked
operationalState = enabled
usageState       = idle
provisioningActivity = none
activityProgress     = n/a
standbyCpActivity    = none
standbyCpActivityProgress = n/a
committedFileName         = BASE_ENG01_7_0_9.full.005
currentViewFileName       = BASE_ENG01_7_0_9.full.005
lastUsedFileName          = BASE_ENG01_7_0_9.full.005
provisioningSession       =
provisioningUser          = none
checkRequired             = no
confirmRequired           = no
editViewName              = BASE_ENG01_7_0_9.full.005
editViewAddedComponents   = 0
editViewDeletedComponents = 0
editViewChangedComponents = 0
```

3 Log in to an MDM server using a root user ID.

4 Open an MDM window:

/opt/MagellanNMS/bin/nmstool &

The copyright dialog and the MDM window open.

5 Click **OK** to close the copyright dialog.

6 From the MDM window, select Configuration > MSS > Administration > MSS Service Data Backup/Restore.

The MSS Service Data Backup/Restore window opens.

7 Click **Add ...**.

8 Select the device(s) to be backed up by selecting the groups and/or nodes located in the Device Groups panel.

9 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.

10 Enter the appropriate user ID and password to authenticate for the selected device(s).

11 Click **OK**.

The added devices now appear in the **Device List** of the main MSS Backup and Restore window.

12 Click **Backup** to start the backup procedure for all the devices listed in the Device List of the main MSS Backup and Restore window.

This will proceed to backup all the views currently stored on each node, and should be done during a maintenance window.

13 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.

HSM overview

This section describes Nortel Multiservice Switch hitless software migration, along with its associated processes. While an HSM must be preceded by pre-migration checks and followed by post-migration checks, these are not described in this overview. For information on pre-migration checks, see HSM (Command Console) pre-work on page 864. For information on post-migration checks, see Verify the success of HSM on page 907.

What happens to the node during a hitless software migration

Nortel supports hitless software upgrades on Nortel Multiservice Switch 15000 nodes used in Carrier Voice over IP Packet Trunking - AAL1 and Carrier Voice over IP Universal Access - AAL1 solutions. During a hitless software migration, the node 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.

Migration must be activated with the *-pause* option, so that when the migration shelf is ready, the migration will pause. When the operator issues the *continue prov* command, the active CP and FPs shut down and the migration shelf becomes the new active shelf.

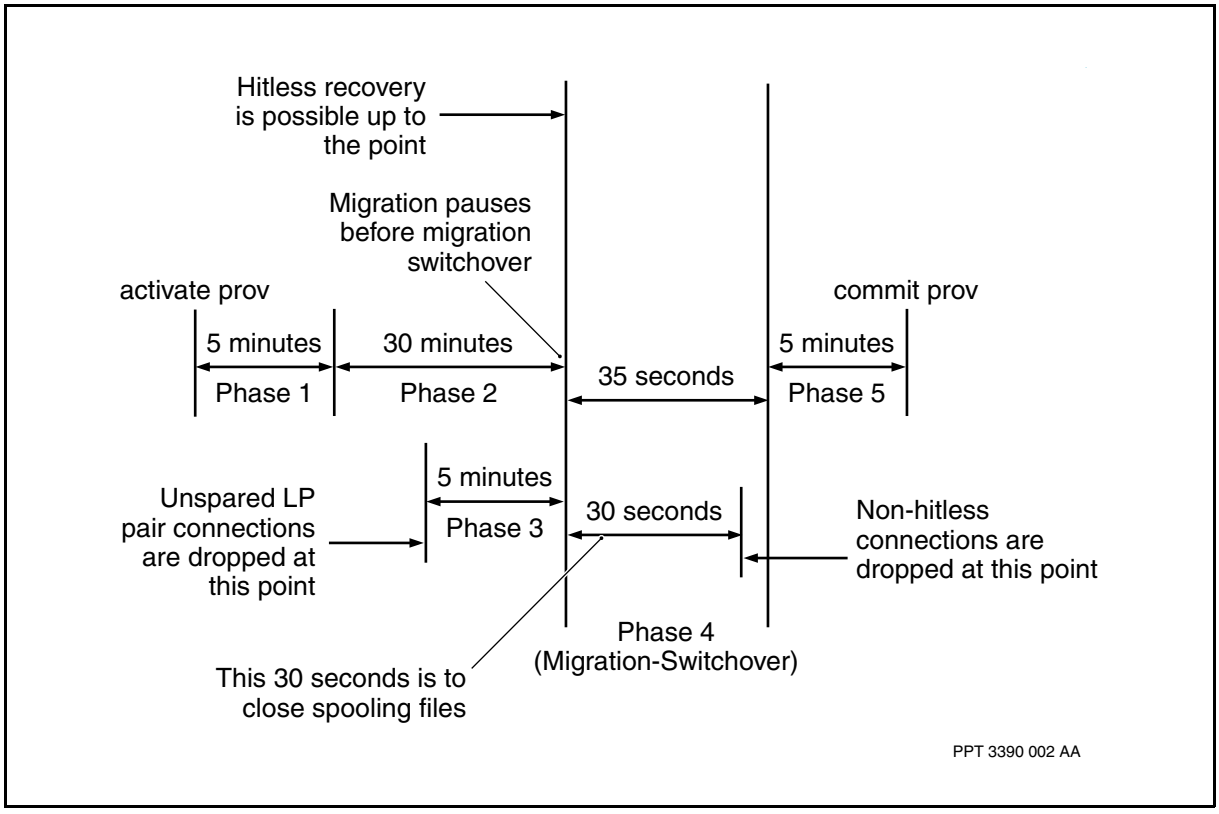
> ***Note:*** If a problem is detected by the system, the process pauses automatically allowing the operator to stop migration or fix the problem and continue.

The five phases of a hitless software migration are as follows:

- Phase 1 — Preparation of the CP on page 859
- Phase 2 — CP migration on page 859
- Phase 3 — FP migration on page 860
- Phase 4 — Migration switchover on page 861
- Phase 5 — Post-migration on page 863

Refer to the figure Multiservice Switch hitless software migration phases on page 858 for more information about the phases.

Multiservice Switch hitless software migration phases



Phase 1 — Preparation of the CP

As the hitless software 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

After the system raises the SET warning alarm to complete phase 1, the following occurs:

1. The migrating CP is reset to load new software and start up in migration mode.

   The operator can activate migration with the *-pause* option to halt migration before a migration switchover occurs. If activated, migration pauses regardless of any fault conditions to allow the operator to verify control channel recovery to the Communication Server 2000 and any Multiservice Gateways.
2. The LED of the migrating CP eventually changes to fast, pulsing green.
3. The new provisioning view migrates to the migrating CP.
4. Committed formats of the migrated view are saved on the migrating CP.
5. 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:

a 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.

b For FPs that fit neither of 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.

6 Provisioning data is delivered within the migrating CP.

7 Applications that run on the CP, such as ATM routing, 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

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 on the migrating FPs eventually change to fast, pulsing green or to solid green.

3 Provisioning data is delivered on the migrating FPs.

4 On 16pOC3SmIrATM FP cards with Pbg components, the software on the migration active card enables the SONET ports and the inter-card sharing bus on unprotected SONET interface pairs to allow the active card to resume carrying traffic for unprotected lines connected to the inactive card.

5 The migrating FPs are loaded with dynamic data for switched services, such as ATM SVCs.

Note 1: There are two conditions that initiate an automatic pause when the *-pause* option is activated. The first condition exists when port bridging is configured on 16pOC3SmIrATM FP cards in the node, and migration switchover is about to begin. This allows the operator to confirm that the Communication Server 2000, MG4000s, and MG9000s have recovered their control channels prior to a

migration switchover. A *continue prov* command issued by the operator allows the migration switchover to continue.

The second 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 prov* command to continue with the migration switchover, or *stop prov* to stop the software migration.

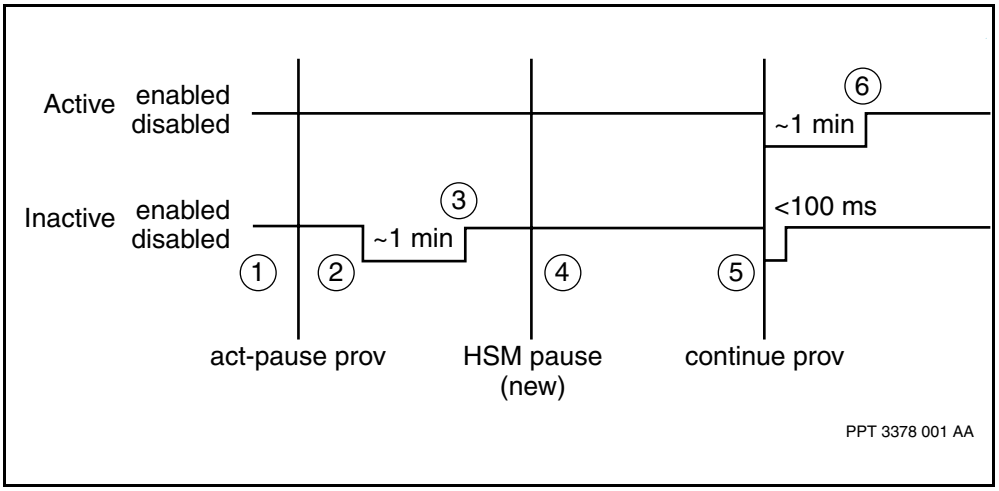
Note 2: After a *continue -force prov* command is issued, the system does not pause again.

Phase 4 — Migration switchover

After the system notifies the active CP that phase 3 is complete, the following occurs:

1 If the provisioning command was activated with the *-pause* option, (in the figure, Migration switchover of Pbg SONET interfaces on page 862, this is the circled point 1) migration pauses to allow Communication Server and Multiservice Gateways to recover control channels using the inactive (or migration active) card. In the figure, “Migration switchover of Pbg SONET interfaces” (page 862), the paused migration is indicated at the circled point 4.

Migration switchover of Pbg SONET interfaces



Note: In the figure, Migration switchover of Pbg SONET interfaces on page 862 circled points 2 and 3 indicate FP migration activity described in the previous section.

2 After the operator confirms that channel recovery is complete, the operator issues the *continue prov* command to stop the service on the active card and start the service on the migration active shelf. In the figure, Migration switchover of Pbg SONET interfaces on page 862 this is indicated at circled point 5.

3 In all other migration scenarios, migration switchover begins when the CPs close all spooled files. For example, alarms and security logs.

4 All processors in the service and migration shelves are notified to switchover.

5 Processors within the service shelf reset to load new software.

6 The CP and FPs in the migration shelf become the service shelf. FPs providing switched services, such as ATM SVCs, re-establish signalling and routing functions. The CP and FPs with the new software start providing service.

7 All sparing panels are switched over.

8 Final port initialization is completed.

9 The shelf becomes one when all CPs and FPs are running the new software. The shelf is no longer logically split into two parts.

Phase 5 — Post-migration

After all the CPs and FPs are running the new software and phase 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 permanent connections at maximum call setup rate. 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 after the operator commits the new provisioning view.

HSM (Command Console) pre-work

Complete the HSM pre-work before you proceed with a software upgrade. If Internode ESA is configured for your network, you must also complete the procedure Pre-work for HSM with AAL1 support of MG9000 Internode ESA on page 881.

Prerequisites

Before doing an HSM, ensure that the auto-patch script (ppautopatch) is not running and that it does not run during the HSM. Issue the following commands on both MDM servers where a ppautopatch script could be configured to run for the node being upgraded:

1 **touch /opt/MagellanNMS/cfg/private/noppautopatchrun**

2 **ps -ef | grep ppautopatch**

If the second command returns only one response, such as the following, proceed with the HSM:

```
ps -ef | grep ppautopatch

root 6453 29431 0 09:10:53 pts/11 0:00 grep
ppautopatch
```

If the second command returns one or more additional responses, such as the following, then the script ppautopatch is running.

```
ps -ef | grep ppautopatch

root 2112 282 0 Dec 03 ? 13:50 ppautopatch -download
-host 47.1.2.3 -huser pp15ksw pp15ksw -apply -nodes
OFFICE1 -nuser config config -max_duration 1 h

root 6453 29431 0 09:10:53 pts/11 0:00 grep
ppautopatch
```

Note 1: The script does not typically take a long time to run so, in general, Nortel recommends waiting until all ppautopatch scripts are finished before starting the HSM.

Note 2: On an MDM that manages nodes in more than one Carrier Voice over IP office, a running script may not necessarily include the node to be upgraded (refer to the -nodes parameter value for the

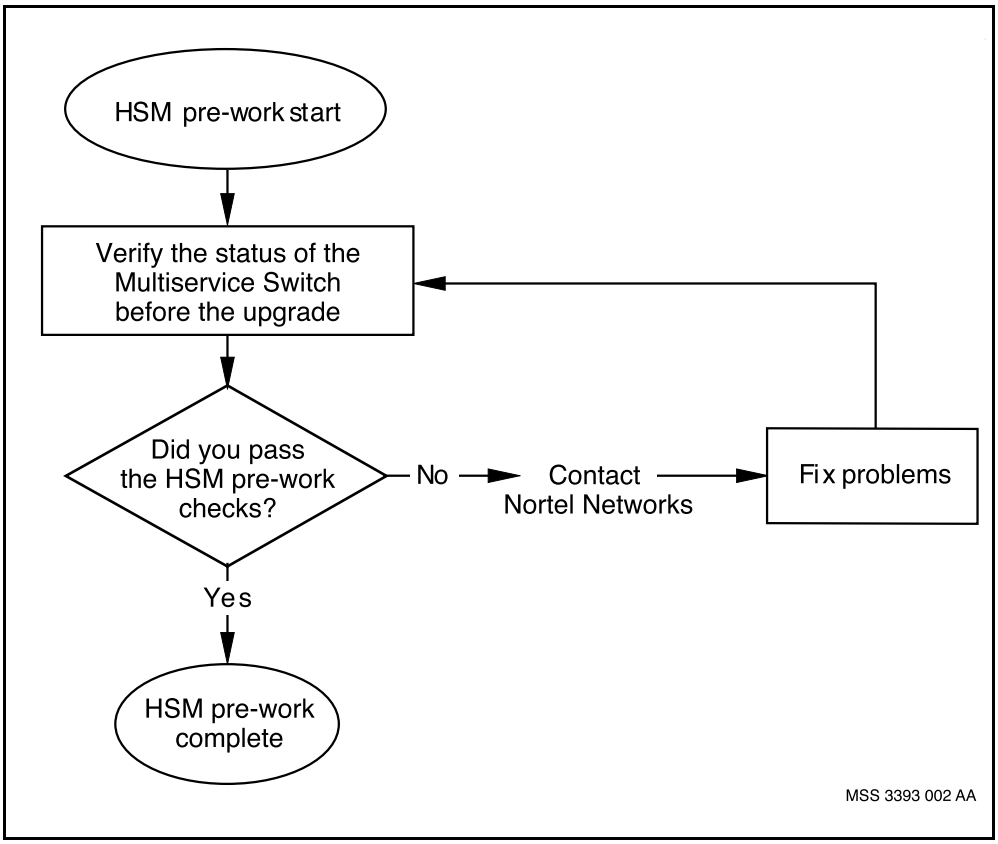
ppautopatch script). If you are sure that none of the running scripts pertain to the node being upgraded, proceed with the HSM.

Note 3: The noppautopatchrun file should be deleted on both MDM servers after the HSM is completed. If performing HSM on a series of nodes from the same MDM, do not remove the file until after all the HSM's have been performed.

HSM pre-work task flow

The task flow shows the sequence of tasks you need to perform prior to performing the HSM.

HSM pre-work task flow



Work flow navigation

- Verify the status of the node before the upgrade on page 866
- Pre-work for HSM with AAL1 support of MG9000 Internode ESA on page 881

Verify the status of the node before the upgrade

Verify the status of the Nortel Multiservice Switch node before upgrading to ensure that the node does not have any alarms raised on it and that it has been configured correctly. In addition, by recording the current status, you can compare it to the status following the upgrade to verify that the upgrade proceeded correctly.

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.
- 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 the MDM 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 there is no provisioning activity occurring on the control processors by verifying that the provisioningActivity value is none:

display prov provisioningActivity

4 Ensure that there is no provisioning activity occurring on the control processors by verifying that the standbyCpActivity value is none:

display prov standbyCpActivity

5 Ensure that there is no provisioning activity occurring on the control processors by verifying that the standbyCpActivityProgress value is n/a:

display prov standbyCpActivityProgress

6 Ensure that there is no provisioning activity occurring on the control processors by verifying that there is either no value for t*he provisioningSession* or, that the value is the same as the value for the MDM session:

display prov provisioningSession

Note: To find the value of the MDM session, issue the **me** command. An empty value or a value the same as your session is the expected response.

7 Ensure that there is no provisioning activity occurring on the control processors by verifying that the *editViewAddedComponents* value is 0:

display prov editViewAddedComponents

8 Ensure that there is no provisioning activity occurring on the control processors by verifying that the editViewDeletedComponents value is 0:

display prov editViewDeletedComponents

9 Ensure that there is no provisioning activity occurring on the control processors by verifying that the *editViewChangedComponents* value is 0:

display prov editViewChangedComponents

10 Verify the status of the 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:

```
5> display shelf fabriccard/* osistate
Shelf Fabriccard/*


-------------------------------------------------------------------------------------------
|Card |osiAdmin|osiOper|osiUsage|osiAvail|osiProc |osiCntrl |osiAlarm |osiStby   |osiUnkn
-------------------------------------------------------------------------------------------
|x    |unlck   |ena    |activ   |        |        |         |         |nset      |false
|y    |unlck   |ena    |activ   |        |        |         |         |nset      |false
|
```

11 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 sample shows output for this command:

```
3> display Lp/* osistate
Lp/*


-------------------------------------------------------------------------------------------
|Card |osiAdmin|osiOper|osiUsage|osiAvail|osiProc |osiCntrl |osiAlarm |osiStby  |osiUnknw
-------------------------------------------------------------------------------------------
|0    |unlck   |ena    |activ   |        |        |         |         |serv     |false
|1    |unlck   |ena    |activ   |        |        |         |         |serv     |false
|2    |unlck   |ena    |activ   |        |        |         |         |serv     |false
|3    |unlck   |ena    |activ   |        |        |         |         |serv     |false
|8    |unlck   |ena    |activ   |        |        |         |         |serv     |false
|9    |unlck   |ena    |activ   |        |        |         |         |serv     |false
```

12

CAUTION
Possibility of a non-hitless software migration
Any card that does not have equipment protection enabled will undergo a regular 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* 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

The cards that are currently providing service should have a Standby Status value of *serv*. All standby function processors should have a value of *hot* indicating *hot standby*. The osiAvail should be empty. All of the shelf card spared services should be enabled and free of alarms.

For cards configured with *Pbg* components, the values for osiOper and osiAvail should be enabled and empty respectively, for both FPs in the 1+1 pair.

If hitless ATM routing is activated, the standby control processor must have a value of *hot* indicating *hot standby*. If hitless ATM routing is not activated, the standby control processor must have a value of *cold* indicating *cold 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:

```
4> display Shelf Card/* SpServ

Shelf Card/* SpServ
-------------------------------------------------------------------
Card|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osi
    | min |per | age |   l   |       |   l   |   m   |tby | kr
-------------------------------------------------------------------
   0|unlck|ena |activ|       |       |       |       |serv|fal
   1|unlck|ena |activ|       |       |       |       |hot |fal
   8|unlck|ena |activ|       |       |       |       |serv|fal
   9|unlck|ena |activ|       |       |       |       |hot |fal
  10|unlck|ena |activ|       |       |       |       |serv|fal
  11|unlck|ena |activ|       |       |       |       |hot |fal
  14|unlck|ena |activ|       |       |       |       |hot |fal
  15|unlck|ena |activ|       |       |       |       |serv|fal
```

13 Verify that there are no shelf hardware failures:

display sh hardware

```
d sh hardware

Shelf
   hardwareFailures =
ok   2004-09-09 20:03:32.53
```

14 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|osiAdmin|osiOper|osiUsage|osiAvail|osiProc|osiCntr|osiAlarm|osiStby|osiUnkn
-------------------------------------------------------------------------------------
|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
|8   | 1   |unlck   |ena    |busy    |        |       |       |nSet    |false
|8   | 2   |unlck   |ena    |busy    |        |       |       |nSet    |false
|8   | 13  |unlck   |ena    |busy    |        |       |       |nSet    |false
|9   | 0   |unlck   |ena    |busy    |        |       |       |nSet    |false
|9   | 1   |unlck   |ena    |busy    |        |       |       |nSet    |false
|9   | 3   |unlck   |ena    |busy    |        |       |       |nSet    |false
|9   | 13  |unlck   |ena    |busy    |        |       |       |nSet    |false
```

15 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
|900   |unlck   |ena     |busy    |        |       |        |        |nSet   |false
```

16 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:

```
4> display atmif/* uni sig/(operatingMode = normal) osistate

AtmIf/* Uni Sig
-------------------------------------------------------------
|AtmIf|osiAd|osiO|osiUs|Response
|     | min |per | age |
-------------------------------------------------------------
|    60|unlck|ena |activ|
|    61|unlck|ena |activ|
|    62|unlck|ena |activ|
|    63|unlck|ena |activ|
|   200|unlck|ena |activ|
|   201|unlck|ena |activ|
|   202|unlck|ena |activ|
|   203|unlck|ena |activ|
|   204|unlck|ena |activ|
|   205|unlck|ena |activ|
|   206|unlck|ena |activ|
|   207|unlck|ena |activ|
|   208|unlck|ena |activ|
|   300|unlck|ena |activ|
```

17 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    |
```

18 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|ena |idle |
    48|unlck|ena |idle |
    49|unlck|ena |idle |
    55|unlck|ena |idle |
    59|unlck|ena |activ|
    63|unlck|ena |activ|
   100|unlck|ena |activ|
   101|unlck|ena |activ|
   212|unlck|dis |idle |
```

19 Display the *Laps* components to identify any Laps components that have any faults or a manual override associated with them.

display Laps/*

To view the following hidden attributes: *osiUnknw, osiStby, osiAlarm, osiCntrl, osiProc, osiAvail, mmAlarm, pfAlarm* and *timeUntilRestore*, use the following command:

display -noTabular Laps/*

The *Laps* component should be unlocked and enabled.

The following shows a sample output for this command:

```
7> display Laps/*
-------------------------------------------------------------------------------
 Laps |osiAd|osiO|osiUs|neRxLi|neReq |neReqC|feReq |feReqC|sdOnLin|switchover
      | min |per | age |  ne  |      | han  |      | han  |  es   |
-------------------------------------------------------------------------------
  200 |unlck|ena |busy |protec|doNotR|workin|noRequ|protec|       |
  201 |unlck|ena |busy |protec|doNotR|workin|noRequ|protec|       |
  202 |unlck|ena |busy |protec|doNotR|workin|noRequ|protec|       |
  203 |unlck|ena |busy |protec|doNotR|workin|noRequ|protec|       |
  600 |unlck|ena |busy |workin|noRequ|protec|noRequ|protec|       |
  601 |unlck|ena |busy |workin|lockou|protec|noRequ|protec|       |
  602 |unlck|ena |busy |protec|manual|workin|doNotR|workin|       |
ok              2004-05-27 11:32:05.76
```

20 If *neReq* has a value of manual, you have a manual override. For each *Laps* component listed in the output, remove the manual overrides related to the automatic selection of the active line of a link protected by line automatic protection switching (LAPS):

clear Laps/<laps_inst>

Issuing this command clears the effects of the **protectionLockout Laps** and the **switch Laps** commands and ensures that all higher priority commands are nulled before the migration.

21 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:

```
17> display Laps/* Sts/0
Laps/* Sts/0
  Use -noTabular to see the many hidden attributes.
-------------------------------------------------------------------------------------------
---
Laps  |osiAdmin|osiOper|osiUsage|snmpOperstate|lop |ais |rfi |slm |txAis|txRdi |pefs
|pcv
-------------------------------------------------------------------------------------------
--
|201  |unlck   |ena    |busy    |up           |off |off |off |off |off  |off   |4374  |
|202  |unlck   |ena    |busy    |up           |off |off |off |off |off  |off   |4374  |
|801  |unlck   |ena    |busy    |up           |off |off |off |off |off  |off   |3597  |
|802  |unlck   |ena    |busy    |up           |off |off |off |off |off  |off   |3605  |
|803  |unlck   |ena    |busy    |up           |off |off |off |off |off  |off   |4359  |
```

22 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
```

23 If *Pbg* components have been configured, verify that the *sts/0* component is enabled, unlocked, and free of alarms:

display pbg/* sts/0 osiState

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *Pbg* components must be enabled and free of alarms.

The following shows sample output for this command:

```
1> display pbg/* sts/0 osistate
Pbg/* Sts/0
-----------------------------------------------------------------
| Pbg |osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|     | min |per | age |   1   |       |   1   |   m   |tby | knw
-----------------------------------------------------------------
|  800|unlck|ena |busy |       |       |       |       |nSet|false
|  801|unlck|ena |busy |       |       |       |       |nSet|false
```

24 If *Pbg* components have been configured, verify that the *Pbg* components are enabled, unlocked, and free of alarms:

display pbg/* osiState

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *Pbg* components must be enabled and free of alarms.

The following shows sample output for this command:

```
2> display pbg/* osistate
Pbg/*
-----------------------------------------------------------------
| Pbg |osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|     | min |per | age |   1   |       |   1   |   m   |tby | knw
-----------------------------------------------------------------
|  800|unlck|ena |busy |       |       |       |       |nSet|false
|  801|unlck|ena |busy |       |       |       |       |nSet|false
```

25 If *Pbg* SONET components have been configured, verify that the components are enabled, unlocked, and free of alarms:

display lp/* bso/* osiState

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *BridgedSonet* components must be enabled and free of alarms.

The following shows sample output for this command:

```
6> display lp/* bso/* osistate
Lp/* Bso/*
-------------------------------------------------------------------
|Lp|Bso|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|  |   | min |per | age |   1   |       |   1   |   m   |tby | knw
-------------------------------------------------------------------
| 8|  1|unlck|ena |busy |       |       |       |       |nSet|false
| 9|  0|unlck|ena |busy |       |       |       |       |nSet|false
```

26 If *DS3* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

d 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:

```
43> d lp/* ds3/* osiState
Lp/* DS3/*
-----------------------------------------------------------------------------------
|Lp|DS3|osiAdmin|osiOper|osiUsage|osiAvail|osiProc|osiCntr|osiAlarm|osiStby|osiUnknw
-----------------------------------------------------------------------------------
|10|  0|unlck   |ena    |busy    |        |       |       |        |nSet   |false
```

27 If *DS1* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

d 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:

```
44> d lp/* ds3/* ds1/* osiState
Lp/* DS3/* DS1/*
-------------------------------------------------------------------------------
|Lp|DS3|DS1|osiAdmin|osiOper|osiUsage|osiAvail|osiProc|osiCntr|osiAlarm|osiStby|osiUnkn
-------------------------------------------------------------------------------
|10|  0|  1| unlck  |ena    |busy    |        |       |       |        |nSet   |false
|10|  0|  2| unlck  |ena    |busy    |        |       |       |        |nSet   |false
|10|  0|  3| unlck  |ena    |busy    |        |       |       |        |nSet   |false
|10|  0|  4| unlck  |ena    |busy    |        |       |       |        |nSet   |false
|10|  0|  5| unlck  |ena    |busy    |        |       |       |        |nSet   |false
|10|  0|  6| unlck  |ena    |busy    |        |       |       |        |nSet   |false
|10|  0|  7| unlck  |ena    |busy    |        |       |       |        |nSet   |false
|10|  0|  8| unlck  |ena    |busy    |        |       |       |        |nSset  |false
```

28 If *DS3 DS1 Chan* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

d 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:

```
13> d lp/* ds3/* ds1/* chan/* osistate

Lp/* DS3/* DS1/* Chan/*
-------------------------------------------------------------------------------
|Lp|DS3|DS1|Chan|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|  |   |   |    | min |per | age |   l   |       |   l   |   m   |tby | knw
-------------------------------------------------------------------------------
|14|  0|  1|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  2|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  3|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  4|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  5|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  6|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  7|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  8|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  0|  9|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1| 17|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1| 18|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1| 19|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1| 20|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1| 21|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1| 22|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1| 23|   0|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1| 24|   0|unlck|ena |busy |       |       |       |       |nSet|false
ok              2004-05-27 11:38:17.78
```

29 If *DS3 IMA* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

d 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:

```
14> d lp/* ds3/* ima/* osistate
Lp/* DS3/* Ima/*
-------------------------------------------------------------------------------------------
|Lp|DS3|Ima|osiAdmin|osiOper|osiUsage|osiAvail|osiProc|osiCntr|osiAlarm|osiStby|osiUnknw
-------------------------------------------------------------------------------------------
|10|  0|  0|unlck   |ena    |busy    |        |       |       |        |nSet   |false
|4|   1|  0|unlck   |ena    |busy    |        |       |       |        |nSet   |false
```

30 If *DS3 IMA LINK* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

d lp/* ds3/* ima/* lk/* osistate

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *DS3 IMA LINK* components must be enabled and free of alarms.

The following shows sample output for this command:

```
Lp/* DS3/* Ima/* Lk/*
-------------------------------------------------------------------------------
|Lp|DS3|Ima|Lk|osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|  |   |   |  | min |per | age |   l   |       |   l   |   m   |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|  1|  2| 1|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  2| 2|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  2| 3|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  2| 4|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  2| 5|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  2| 6|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  2| 7|unlck|ena |busy |       |       |       |       |nSet|false
|14|  1|  2| 8|unlck|ena |busy |       |       |       |       |nSet|false
ok              2004-05-27 11:39:30.16
```

31 If the node being migrated relies on OAM Ethernet connectivity, verify that the value is available:

display Lp/0 Oamenet/0 activeStatus

Note: If the node is using in-band OAM, you need to have an Ethernet connection to the gateway node. You may have an Ethernet connection to the remote node for emergency access.

32 If the node being migrated relies on OAM Ethernet connectivity, verify that the value is available:

display Lp/0 Oamenet/0 standbyStatus

33 Optionally, display, ping, and record information about the IP accessibility of the node to verify the reachability of the node after the migration.

list ac ipaccess/*

The following shows sample output for this command:

```
8> list ac ipaccess/*
Ac IpAccess/58.183.182.10
Ac IpAccess/58.138.191.21
```

34 If you have configured in-band OAM or internode ESA, verify that the *Atmmpe* components are unlocked, enabled, and active:

display Atmmpe/* osiState

The following shows sample output for this command:

```
25> display atmmpe/* osiState

AtmMpe/*
-------------------------------------------------------------------
|AtmMpe|osiAd|osiO|osiUs|Response
|      | min |per | age |
-------------------------------------------------------------------
|     0|unlck|ena |activ|
ok             2004-05-27 11:39:30.16
```

35 If you have configured in-band OAM or internode ESA, verify that the *Ac* components are unlocked, enabled, and active:

display Atmmpe/* Ac/* osiState

The following shows sample output for this command:

```
24> display atmmpe/* ac/* osiState

AtmMpe/* Ac/*
-------------------------------------------------------------------
|AtmMpe|Ac  |osiAd|osiO|osiUs|Response
|      |    | min |per | age |
-------------------------------------------------------------------
|     0|   1|unlck|ena |activ|
```

36 If you have configured in-band OAM, verify and record information about the accessibility of the chosen MDM server from the node. In conjunction with step 37 ensure that both MDM servers are connected by way of different gateway nodes and

that hop 1 in the output for this step is different from the output for step 37:

ping -trace -ip(<MDM1 IP>) Vr/0 Ip Icmp

Take the MDM server addresses in step 33 and verify that there are diverse routes to each one, and that you are able to reach it.

For a description of chosen and alternate MDM servers, see step 33.

The following shows sample output for this command:

```
8> ping -trace -ip(47.135.211.28) Vr/0 Ip Icmp
Vr/0 Ip Icmp
   IP Trace Route for 47.135.211.28:
   Path taken:
     Hop 1:   58.142.129.1    (time = 1ms)
     Hop 2:   58.142.204.145  (time = 2ms)
     Hop 3:   58.142.204.141  (time = 17ms)
     Hop 4:   58.142.205.201  (time = 1ms)
     Hop 5:   58.142.205.1    (time = 1ms)
     Hop 6:   58.255.4.145    (time = 27ms)
     Hop 7:   58.130.255.105  (time = 27ms)
     Hop 8:   58.131.49.10    (time = 27ms)
     Hop 9:   58.129.255.210  (time = 88ms)
     Hop 10:  58.129.255.58   (time = 30ms)
     Hop 11:  58.135.211.28   (time = 25ms)
```

37 If you have configured in-band OAM, verify and record information about the accessibility of the alternate server from the node. In conjunction with step 36 ensure that both MDM servers are connected by way of different gateway nodes:

ping -trace -ip(<MDM2 IP>) Vr/0 Ip Icmp

Take the MDM server addresses in step 33 and verify that there are diverse routes to each one, and that you are able to reach it.

The following shows sample output for this command:

```
8> ping -trace -ip(47.135.211.40) Vr/0 Ip Icmp
Vr/0 Ip Icmp
   IP Trace Route for 47.135.211.40:
   Path taken:
     Hop 1:   58.142.129.1    (time = 0ms)
     Hop 2:   58.142.204.145  (time = 3ms)
     Hop 3:   58.142.204.141  (time = 16ms)
     Hop 4:   58.142.205.201  (time = 1ms)
     Hop 5:   58.142.205.1    (time = 0ms)
     Hop 6:   58.255.4.145    (time = 26ms)
     Hop 7:   58.130.255.105  (time = 27ms)
     Hop 8:   58.131.49.10    (time = 26ms)
     Hop 9:   58.129.255.210  (time = 83ms)
     Hop 10:  58.129.255.58   (time = 28ms)
     Hop 11:  58.135.211.40   (time = 48ms)
```

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.

Pre-work for HSM with AAL1 support of MG9000 Internode ESA

If the MSS15000 is configured to support MG9000 InterNode ESA, you must also check the state of the following additional components:

1 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|
|ESA               |unlck|ena |activ|
```

2 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
|ESA             |9K_1_ESA            |unlck |ena |activ
|ESA             |9K_2_ESA            |unlck |ena |activ
|ESA             |9K_3_ESA            |unlck |ena |activ
|ESA             |9K_4_ESA            |unlck |ena |activ
|ESA             |PP_D6_1000_ESA      |unlck |ena |activ
|ESA             |PP_D6_1001_ESA      |unlck |ena |activ
|ESA             |PP_D7_800_ESA       |unlck |ena |activ
```

3 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|
|ESA             |unlck|ena |activ|
```

4 Verify that the static routes are up.

The osiOper (operational state) of all static routes are *ena* (enabled).

display Vr/* Ip static routeEntry/* operationalState

The following shows sample output for this command:

```
> display Vr/* Ip static routeEntry/* operationalState

Vr/* Ip Static Route/*,*,*
-------------------------------------------------------------
|       Vr        |     addr       |     mask       |tos|osiO
|                 |                |                |   |per
-------------------------------------------------------------
|ESA              |10.0.16.0       |255.255.240.0   |  0|ena
|ESA              |10.0.32.0       |255.255.240.0   |  0|ena
```

5 Verify that all *Nexthop* components under static routes have an operational status of enabled:

display Vr/ESA Ip static route/*Nh/* operationalState

The following shows sample output for this command:

```
   >
   Vr/ESA Ip Static Route/*,*,* Nh/*
-------------------------------------------------------
   | addr          | mask            |tos    | Nh          |osiO
   |               |                 |       |             |per

   |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
```

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

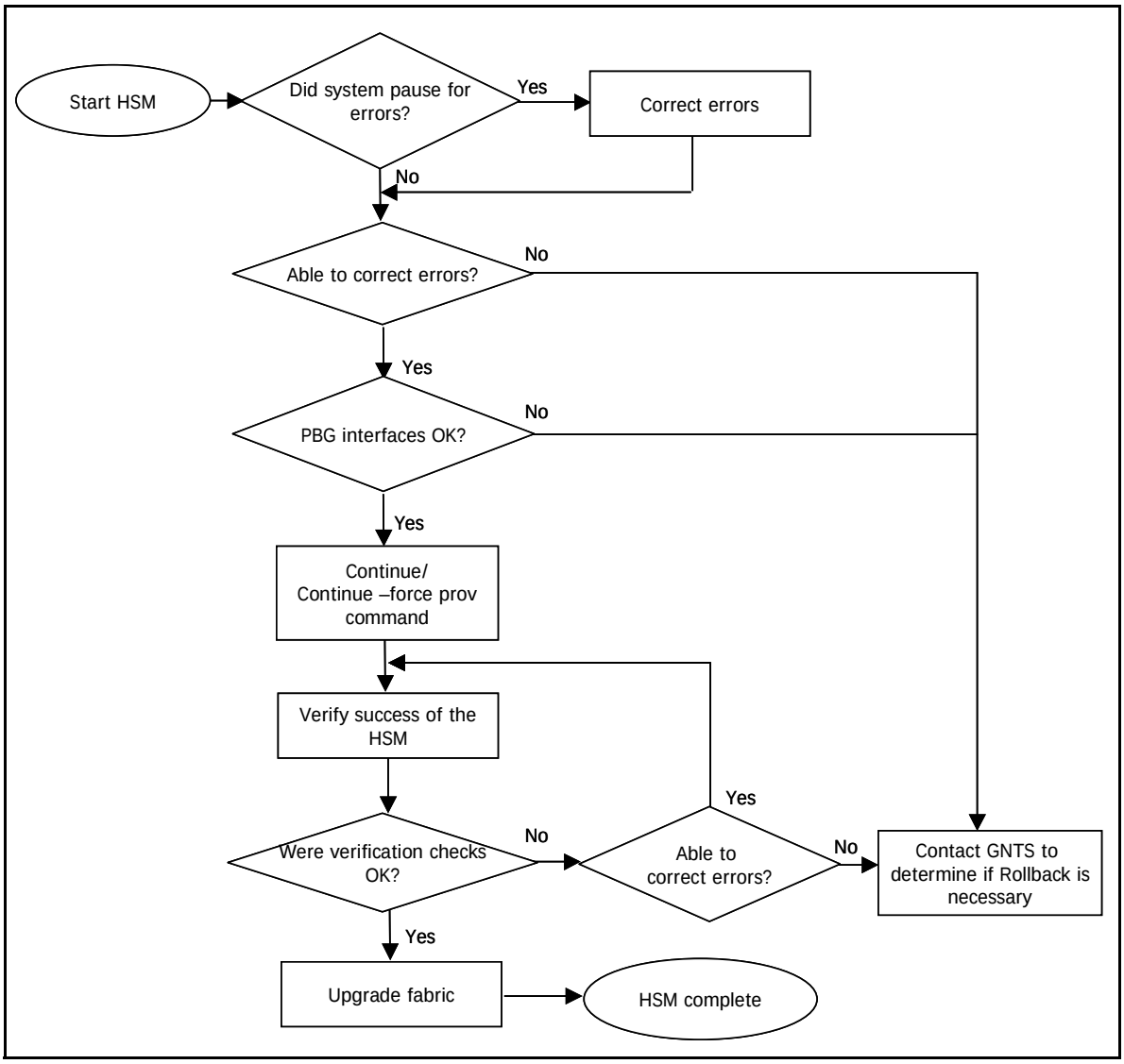
- Complete the HSM pre-work. See HSM (Command Console) pre-work on page 864 for more information.
- For in-band OAM configurations, upgrade all Nortel Multiservice Switch 15000 nodes in the network in the following sequence:
- Upgrade all the remote nodes first.
- Upgrade the non-preferred Gateway node next.
- Upgrade the preferred Gateway node last.

Note: For a quick reference to key relationships needed to understand in-band OAM migration, see In-band OAM quick reference on page 932. For a description of in-band OAM, see NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP*.

HSM task flow

The task flow shows the sequence of procedures you must perform to execute the HSM.

HSM task flow



Work flow navigation

- HSM (Command Console) pre-work on page 864
- Perform HSM using Command Console on page 886
- Upgrade the fabric firmware on page 899
- Verify the success of HSM on page 907
- Stop the HSM using Command Console on page 911

Perform HSM using Command Console

Upgrade a Nortel Multiservice Switch 15000 node 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 in process of being setup are dropped
This strategy removes inactive 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 firmware on page 899 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 Nortel MDM Command Console tool server rather than through a Telnet session. Using the Command Console ensures that you remain connected to the node and monitor the CP switchover. For more information on opening the Command Console, see 241-6001-804 *Nortel Multiservice Data Manager Workstation Utilities*.
- The node 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.

- To prevent outages during the hitless software migration, ensure that the links between the CS2000 Manager and the node are configured in two groups that have been distributed between the shelves to create redundancy.

  Note: This does not apply if the CS2000 Manager is configured for Port Bridging.

- 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 extensive knowledge of Unix, Multiservice Switch software, and the Carrier Voice over IP portfolio architecture.
- You need to add the following applications to the application version list: base, networking, atmNetworking, and ip. If your nodes have been configured with in-band OAM, you will also need to add the wanDte application. The application version list must not contain any additional applications.
- Refer to the software downloads area of Nortel Web site (*www.nortel.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 Log in with the appropriate permissions.

2 Enter provisioning mode so that you can issue the appropriate commands:

start prov

Sample output

```
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

Sample output

```
7> display -c Sw Avl
Sw avList = base_CF01S1E,  patch _CF01S1E
    networking_CF01S1E,   atmNetworking_CF01S1E,
     ip_CF01S1E
```

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, ip, networking, and atmNetworking. If your nodes have been configured with in-band OAM, you will also need to load the wanDte application. Do not add any other applications to the application version list.

Note: Do not set the software applications for the fabric. Refer to Upgrade the fabric firmware on page 899 for more information about upgrading the fabric firmware.

Sample output

```
PROV 26> set Sw Avl !
base_CF01S1E,  ip_CF01S1E,  networking_CF01S1E
atmNetworking_CF01S1E,  patch_CF01S1E
Sw
ok 2001-08-09 18:05:09.94
```

Note: You may need to set a different list of software application versions.

6 Check that the new applications are in the application version list and that, other than the load name, the applications are the same as those listed in step 4:

display Software avList

Sample output

```
PROV 2> display Software AvList
Sw
 avList = base_CF01S1E,       ip_CF01S1E,
      networking_CF01S1E,        atmNetworking_CF01S1E,
      patch_CF01S1E
```

7 Display software patchlist:

display software patchlist

8 If there are patches on the load you need to remove, remove those patches. See *Nortel Multiservice Switch Release Notes* to determine the software patches required, and apply the patches needed for SN08:

set Software patchlist ! <patches>

9 Verify the patches that are going to be applied:

display software patchlist

Sample output

```
PROV 2> d  Sw patchlist
Sw
patchlist = atmNetworkingFT032A, baseFT173A, baseFT
 baseFT173A, baseFT172A,
```

10

CAUTION
Potential interruption of calls in progress
The software upgrade for the Multiservice Switch 15000 shelf 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, the node will go through a normal software migration that is not hitless and all calls on the node will be interrupted.

If more than one provisioning change has occurred, repeat step 3 and then perform the procedure Verify the status of the node before the upgrade on page 866.

Verify that the *editViewChangedComponents* attribute indicates that you have made only one provisioning change:

display -o prov

Sample output

```
36> display -o pr
Prov
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   provisioningActivity = none
   activityProgress     = n/a
   standbyCpActivity    = none
   standbyCpActivityProgress = n/a
   committedFileName         = CE01S1B_Complete.full.004
   currentViewFileName       = CE01S1B_Complete.full.004
   lastUsedFileName          = CE01S1B_Complete.full.004
   provisioningSession       = Nmis Fmip Session/2
   provisioningUser          = dominicr
   checkRequired             = yes
   confirmRequired           = no
   editViewName              = none
   editViewAddedComponents   = 0
   editViewDeletedComponents = 0
   editViewChangedComponents = 1
   currentJournal            = 0
   journalDisabledReason     = not disabled
   restorePossible           = no
ok             2004-05-27 11:57:37.75
```

11

CAUTION
Proceeding with a non-hitless software migration
The node will go through a normal 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 this step. If you cannot fix the problem, stop the migration.

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.
```

Sample output

```
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.
```

Note: 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.

12 Save the edit view with portable formats:

save -f(<filename>) -portable prov

13 Apply the changes:

activate -pause prov

Always use the **activate -pause prov** command. The software migration activation pauses before migration switchover occurs and displays the message shown in the sample output.

Note: The system can pause for one of two reasons: the system has found a fault, or an operator issued a pause command. In case of a fault, refer to the NN10198-912 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP*. If the system pauses because the operator has used the **-pause** command, the operator can issue **continue -prov** command to continue the HSM. In the example below, the system has paused due to a fault.

Sample output with the pause option

```
PROV 151> activate -pause prov

--- Response 149 continued ...
The software migration is paused, pause reason:
Details:
On Card 1: Pausable Alarm recvd;
ACTIVATE -PAUSE PROV operator command.

To resume, type Continue Prov. To stop, type Stop Prov.
```

Note: 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**).

14

CAUTION
Before issuing a continue prov command, perform the following:
Before issuing a **continue pro**v command, perform steps 14 to 17. Steps 14 to 17 must always be done in a paused state.

In a migration where the *Pbg* components have been configured, verify that all CCMT logs are cleared from the MAP. (Determine that the CS2000 Core Manager CCMT links and the SAM21 SC H.248 and OAM channels that went out of service when migration started, are re-established).

See “Tools and utilities” for the “CS2000 Core Manager” and “Media Gateway 9000 Manager” in the *Carrier Voice over IP Fault Management* document for Wireline Universal Packet Access (UA-AAL1) and for Packet Trunking (PT-AAL1).

15 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 contain *degrad*. All of the *Laps* components must be enabled and free of alarms.

Sample output

```
      15> display laps/* osistate

Laps/*
-------------------------------------------------------------------------
|Laps  |osiAd|osiO|osiUs|osiAvai|osiProc|osiCntr|osiAlar|osiS|osiUn
|      | min |per | age |   l   |       |   l   |   m   |tby | knw
-------------------------------------------------------------------------
|   60|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|   61|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|   62|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|   63|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|  201|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|  202|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|  203|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|  204|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|  205|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|  206|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|  211|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|  212|unlck|ena |busy |degrad |       |       |minor  |nSet|false
|  213|unlck|ena |busy |degrad |       |       |minor  |nSet|false
```

16 In a migration where the *Pbg* components have been configured, verify that the *sts/0* component is enabled, unlocked, and free of alarms:

display pbg/* sts/0 osiState

17 In a migration where the *Pbg* components have been configured, verify that the *Pbg* components are enabled, unlocked, and free of alarms:

display pbg/* osiState

18

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 911.

CAUTION
Exercise caution when using the continue -force prov command
Contact Nortel 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: After the CP switchover during the hitless software migration, connectivity between the node and 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 MSS 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`

19 To monitor the progress of the migration, enter the following command:

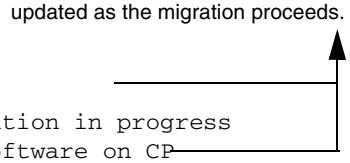
display -o prov

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 in (see step 20). If you are using 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 2.

Sample output

```
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
```



20 If using Telnet, when prompted, log in to the node with the appropriate permissions.

21 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

Sample output

```
 3> confirm prov
Prov
   Activation confirmed. Rollback will not occur.
```

22 Enter provisioning mode: **start prov**

Sample output

```
 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.
```

23 Check that the edit view is the same as the current view:

copy prov

The message should confirm that both views are the same.

24 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 NN10070-461 *Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1*.

25 If the semantic check passes, save, activate, confirm and commit the view:

save prov

activate prov

confirm prov

commit prov

Sample output

```
 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.

26 Exit provisioning mode once 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. The applications required for Carrier Voice over IP VoA are base, networking, atmNetworking, and ip. If the nodes have been configured with in-band OAM, the wanDte application must also be present. The application version list must not contain any additional applications
<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 the Nortel Web site (*www.nortel.com*)

Upgrade the fabric firmware

You can upgrade the fabric firmware installed on Nortel 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.

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 Multiservice Switch Release Notes.*
- The new fabric card firmware must be downloaded from the Nortel MDM server acting as the software distribution site (SDS). For more information on how to download from the SDS, see NN10600-272 *Nortel 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.
- Nortel Multiservice Switch 15000 nodes must contain two fabric cards. A single fabric card shelf cannot be upgraded hitlessly.
- 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 node

1 Display the attributes of the fabric card banks:

display Shelf FabricCard/<n> banks

The following shows sample output for this command in a SN06 to SN08 upgrade:

Sample output

```
 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
```

The following shows sample output for this command in a SN07 to SN08 upgrade. If the output is:

"recommendedVersionToInstall = Fabric software version is up to date".

a fabric upgrade is not required.

2 Verify that the required fabric firmware version has been downloaded to the node:

list Sw Av/Fabric_<version>

Sample output

```
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 the software to the server from the Nortel website on page 841.

3 Verify both fabrics are enabled and unlocked:

display Shelf FabricCard/*

Sample output

```
3> d sh fa/* state
Shelf FabricCard/*
-------------------------------------------------------------------------
|FabricCard|osiAd|osiO|osiUs|osiAvai|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
ok            2004-02-23 23:26:38.95
```

4 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.

Sample output

```
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
ok              2004-02-23 23:14:57.86
```

5 Verify that the fabric ports on the cards are unlocked and enabled:

display Shelf Card/* fabricPort/* state

Sample output

```
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
|   6|y         |unlck|ena |activ|       |       |       |       |nSet|false
|   7|x         |unlck|ena |activ|       |       |       |       |nSet|false
|   7|y         |unlck|ena |activ|       |       |       |       |nSet|false
ok             2004-02-23 23:32:58.28
```

6 Lock the fabric card to be upgraded:

lock Shelf FabricCard/<n>

Sample output

```
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
Int: 1/0/2/29063; bcsBus.cc; 752; ""
```

7 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.

Sample output

```
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
```

8 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

Sample output

```
8> d sh fa/x banks
Shelf FabricCard/x
fixedBankVersion = 8.2
writableBankVersion = 9.4
recommendedVersionToInstall = Fabric software version is up to date.
activeBank                  = writable
bankOnShelfRestart          = writable
downloadProgressPercent     = 100 %
writableBankStatus          = loaded
ok                    2004-02-24 13:10:01.43
```

9 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

Sample output

```
9> start shelf fabriccard/x test
Shelf FabricCard/x Test
   Test started.


9> start 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 fabric 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 Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* to interpret the test results.

10

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.

11 Repeat step 3 through step 10 for the other fabric card.

12 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 switch the 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 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 step 7.

Verify the success of HSM

After completing the upgrade, verify that 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. If you are uncertain, contact GNTS for help deciding.

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 866
- Perform HSM using Command Console on page 886

From the node

1 Log in with the appropriate permissions.

2 Compare the status of the logical processors with the status recorded in step 11 of the procedure Verify the status of the node before the upgrade on page 866:

display Lp/* osistate

3 Compare the status of equipment protection with the information you gathered in step 12 of the procedure Verify the status of the node before the upgrade on page 866:

display Shelf Card/* SparedServices

4 Compare the status of the shelf hardware with the information you gathered in step 13 of the procedure Verify the status of the node before the upgrade on page 866.

display sh hardware

5 Compare the status of the SONET ports with the status recorded in step 14 of the procedure Verify the status of the node before the upgrade on page 866:

display Lp/* sonet/* osistate

6 Compare the status of the ATM interfaces with the status recorded in step 15 of the procedure Verify the status of the node before the upgrade on page 866:

display Atmlf/* osistate

7 Compare the status of the *UNI* signalling components with the status recorded in step 16 of the procedure Verify the status of the node before the upgrade on page 866:

display atmif/* uni sig/(operatingMode = normal) osistate

8 Compare the status of the *PNNI* signalling components with the status recorded in step 17 of the procedure Verify the status of the node before the upgrade on page 866:

display Atmlf/* Pnni Sig osistate

9 Compare the status of the *ILMI* signalling components with the status recorded in step 18 of the procedure Verify the status of the node before the upgrade on page 866:

display atmif/* uni ilmi/(operatingMode = addressRegEnabled) osistate

10 Compare the status of the *Laps* components with the status recorded in step 22 of the procedure Verify the status of the node before the upgrade on page 866:

display Laps/* osistate

11 If configured, compare the status of the *Pbg* signalling components with the status recorded in step 23 of the procedure Verify the status of the node before the upgrade on page 866:

display pbg/* sts/0 osiState

12 If configured, compare the status of the *Pbg* components with the status recorded in step 24 of the procedure Verify the status of the node before the upgrade on page 866:

display pbg/* osiState

13 Compare the status of the *BSo* components with the status recorded in step 25 of the procedure Verify the status of the node before the upgrade on page 866:

display Ip/* BSo/* osiState

14 If configured, compare the status of *DS3* components with the information you gathered in step 26 of the procedure Verify the status of the node before the upgrade.:

display Ip/* ds3/* osiState

15 If configured, compare the status of *DS1* components with the information you gathered in step 27 of the procedureVerify the status of the node before the upgrade on page 866:

display Ip/* ds3/* ds1/* osiState

16 If configured, compare the status of *DS3 DS1* channel components with the information you gathered in step 28 of the procedure Verify the status of the node before the upgrade on page 866:

display lp/* ds3/* ds1/* chan/* osiState

17 If configured, compare the status of *DS3 IMA* components with the information you gathered in step 29 of the procedure Verify the status of the node before the upgrade on page 866:

display lp/* ds3/* ima/* osistate

18 If configured, compare the status of *DS3 IMA LINK* components with the information you gathered in step 30 of the procedure Verify the status of the node before the upgrade on page 866:

display lp/* ds3/* ima/* lk/* osiState

19 Compare the status of the Ethernet connection with the information you gathered in step 31 of the procedure Verify the status of the node before the upgrade on page 866:

display Lp/0 Oamenet/0 activeStatus

20 Compare the status of the Ethernet connection with the information you gathered in step 32 of the procedure Verify the status of the node before the upgrade on page 866:

display Lp/0 Oamenet/0 standbyStatus

21 Compare the status of IP access with the information you gathered in step 33 of the procedure Verify the status of the node before the upgrade on page 866:

display ac ipaccess/*

22 If you have configured in-band OAM, ensure that the MDM servers can display OAM data received by way of both the preferred and non preferred Gateway nodes.

23 If you have configured in-band OAM or internode ESA, compare the status of the *Atmmpe* components with the information you gathered in step 34 of the procedure Verify the status of the node before the upgrade on page 866:

display Atmmpe/* osiState

24 If you have configured in-band OAM or internode ESA, compare the status of the *Ac* components with the information you gathered in step 35 of the procedure Verify the status of the node before the upgrade on page 866:

display Atmmpe/* Ac/* osiState

25 If you have configured in-band OAM, compare the accessibility of the chosen MDM server from the node with the information you gathered in step 36 of the procedure Verify the status of the node before the upgrade on page 866. In conjunction with this step, ensure that both MDM servers are connected by way of different Gateway nodes.

ping -trace -ip(<MDM1 IP>) Vr/0 Ip Icmp

26 If you have configured in-band OAM, compare the accessibility of the alternate MDM server from the node with the information you gathered in step 37 of the procedureVerify the status of the node before the upgrade on page 866. In conjunction with step ensure that both MDM servers are connected by way of different Gateway nodes.

ping -trace -ip(<MDM2 IP>) Vr/0 Ip Icmp

27 In multi-shelf configurations, compare the information you gathered in the procedure Verify the status of the node before the upgrade on page 866. It is recommended that you repeat the steps in this procedure on adjacent nodes in addition to the upgraded node. This verification procedure ensures that the far end links of the migrating node are operating correctly, and can handle a switchover.

28 If you have inhibited the ppautopatch file from running, remove the noppautopatchrun file on all MDM servers configured for auto-patching on the MSS/MG15000 node.

From the MDM:

a Log in as root.

b Remove the file as follows:

```
rm
/opt/MagellanNMS/cfg/private/noppautopatchru
n
```

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 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.

In order 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 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, or if the system pauses, you can roll back to the view before the software application version list has changed with no system impact.

Note: If the system pauses you must issue either the **continue prov** command or the **stop prov** command.

Prerequisites

CAUTION
Service outage
If you issue the **stop prov** command after the migration-switchover phase, it will cause a service outage.

From the node

1 Stop the migration:

stop prov

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 884.

```
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
```

HSM (MDM SASM tool) activation

Perform the HSM by setting the application version list, setting the patchlist, and activating the provisioning changes. When the activation completes, the node will be running the new software.

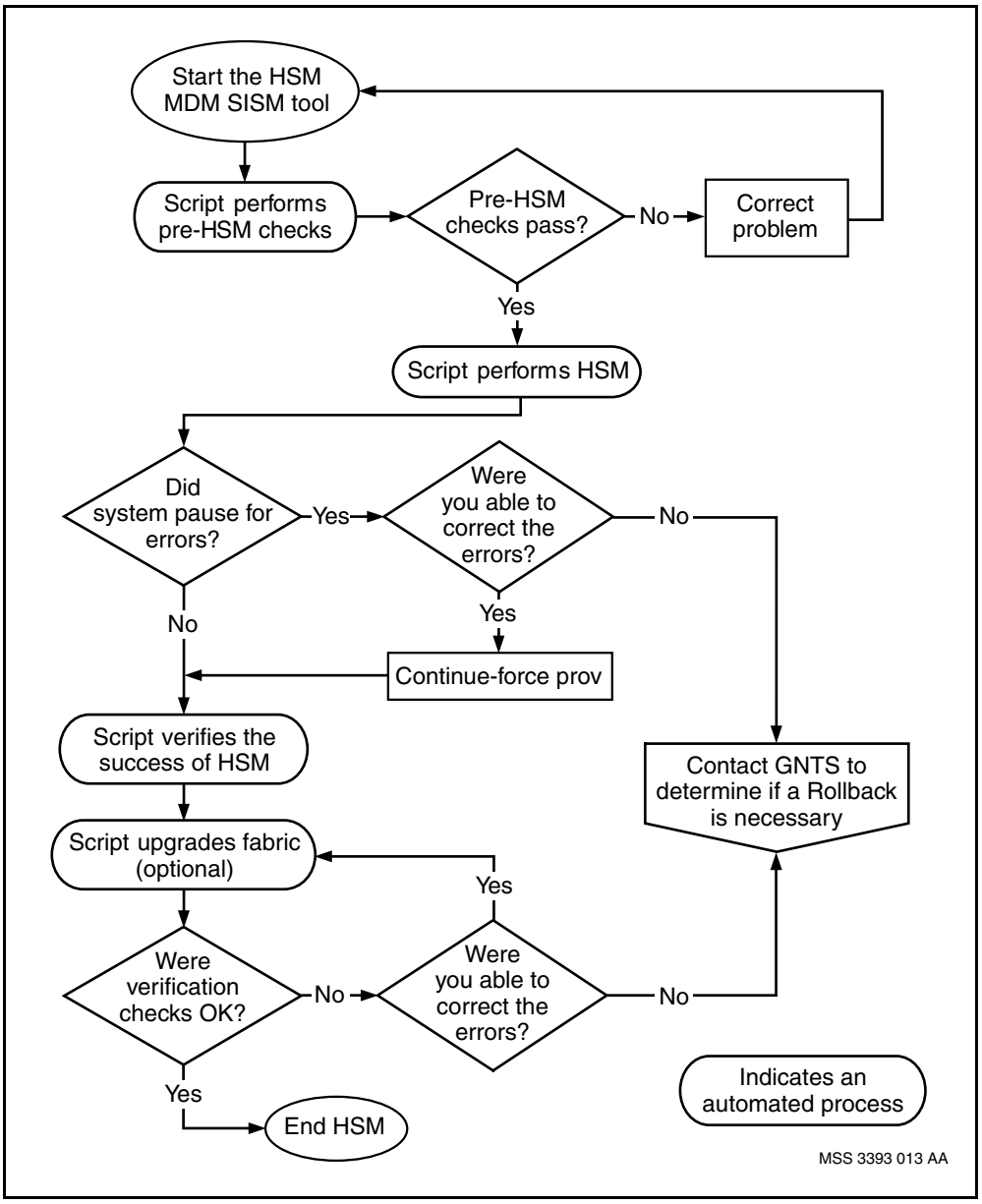
Prerequisites

- Refer to Prerequisites on page 864 in HSM (Command Console) pre-work on page 864.
- For in-band OAM topologies, upgrade all Nortel Multiservice Switch 15000 nodes in the network in the following sequence:
  - upgrade all the remote nodes first
  - upgrade the non-preferred Gateway node next
  - upgrade the preferred Gateway node last

HSM task flow

The task flow shows you the sequence of tasks you need to perform to execute the HSM.

HSM task flow



Work flow navigation

The following aspects of the HSM are automated by the Carrier Voice over IP ATM Upgrade script:

- Start HSM using SASM tool on page 916
- Pre-HSM verification checks on page 921
- HSM activation on page 921
- Post-HSM verification and Fabric upgrade on page 923
- HSM script completion and final steps on page 924

The final portion of the HSM is manually controlled by the operator:

- Stop the HSM using MDM SASM tool on page 926

Performing HSM using MDM SASM

Perform HSM using the Nortel MDM GUI tool SASM to upgrade the Multiservice Switch node.

Prerequisites

- If MG9000 Internode ESA is provisioned on the MSS15000, perform the manual pre-check procedure, Pre-work for HSM with AAL1 support of MG9000 Internode ESA on page 881 before you launch the SASM tool.
- Have the correct software load and patches downloaded to the MDM server.

Start HSM using SASM tool

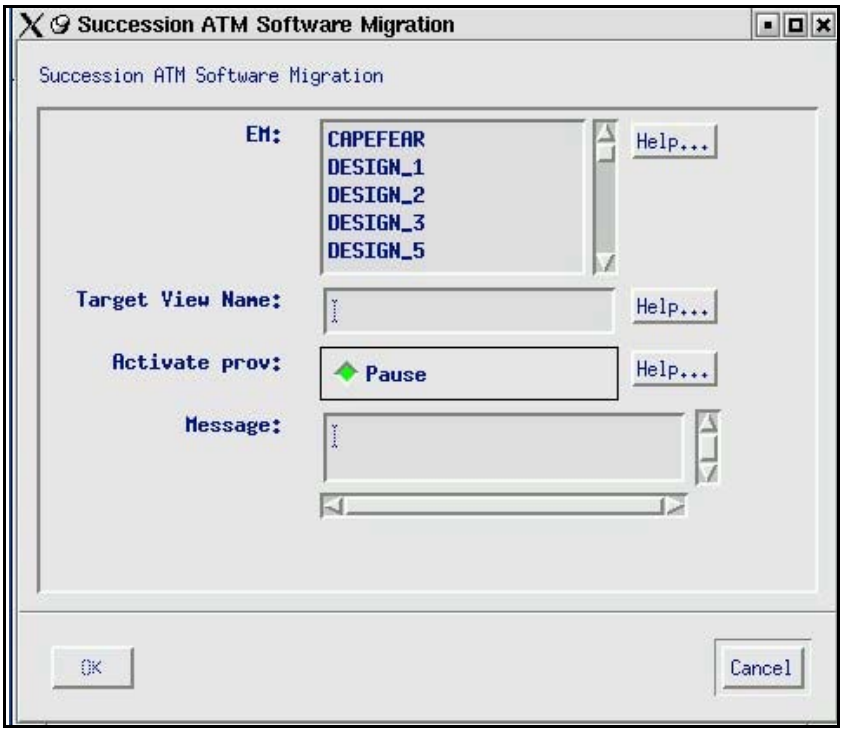
From the MDM window

1 Choose Configuration > MSS > Administration > Succession ATM Software Migration.

Alternatively, from the MDM Command Console, type:

$ /opt/MagellanNMS/bin/succession_atmsw_migr

The Succession ATM Software Migration window opens.



2 In the EM field, select the name of the node you want to upgrade.

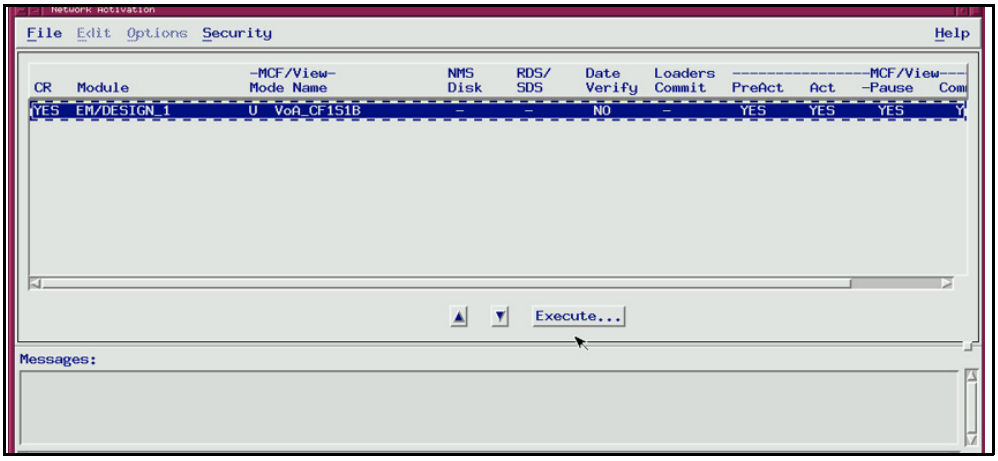
3 In the View field, enter the new target view name without the view type or version in the name (for example, CF01S1B_April_24).

The target view name must be 20 characters or less and be composed of numbers, letters and underscore. Use a consistent naming convention because this name is used when saving the current view and to create the view that will be activated for the software migration.

4 Click **OK**.

The Component Information Viewer opens.

The Network Activation window opens.



The Network Activation tool launches automatically in Hitless Software Migration mode with the network activation file already loaded. The network activation file contains one network activation record defined specifically for Carrier Voice over IP software migration activation. The record must be selected before you click **Execute**.

5 From the MDM window, choose Fault > Alarm Display: Log.

The Alarm Display window opens.

6 Ensure the appropriate filters are turned on, including the filter for the target node, and that Format is set to full. Set filter to on. For more information on how to filter alarms, see “Filtering alarms” in 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

7 From the MDM window, choose Fault > Alarm Display: Active.

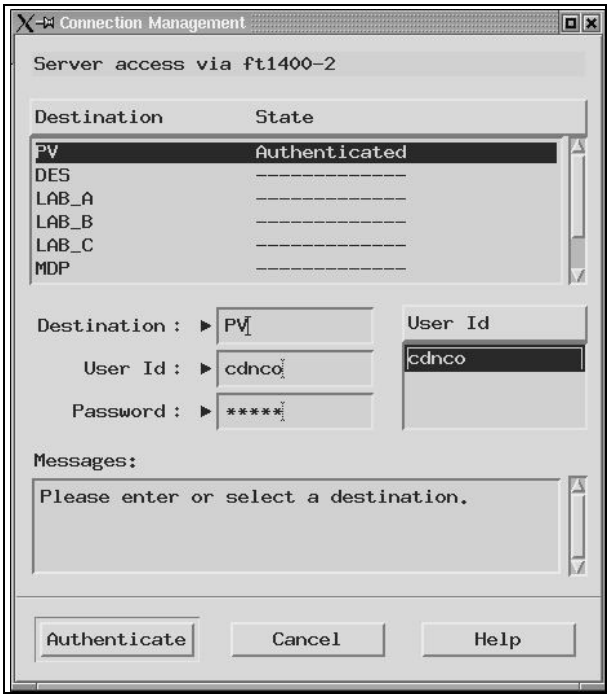
The Alarm Display window opens.

8 Ensure the appropriate filters are turned on, including the filter for the target node, and that Format is set to full. Set filter to on. For more information on how to filter alarms, see “Filtering alarms” in 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

Note: You should monitor any alarms against the *prov* component (specifically 7000 0033, 7000 0034, and 7000 0035) and the *prov migration* component. You should also monitor 7012 0204 against the *Lp* component. This alarm indicates that the LP cannot achieve its expected migration switchover behaviour.

9 From the Network Activation tool, select **Group Authenticate** from the Security menu.

The Connection Management Dialog opens.



10 Enter or select the node’s group name, and enter a valid user ID and password for the group. (Your user ID must have a minimum impact of System Admin and minimum scope of network.)

11 Click **Authenticate**.

Authentication takes place. If authentication is successful, the dialog closes.

Note: If your user ID does not have sufficient permissions to perform the upgrade, you must exit and restart the SASM tool

using an ID that has a minimum impact of System Admin and minimum scope of network.

After you authenticate with the group that contains the node to be migrated, you can use the Component Information Viewer to display the attributes of the provisioned components and later after the migration starts, monitor the progress of the migration. See 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

12 In the Network Activation tool window, click **Execute**.

A confirmation dialog opens.

13 Click **OK** to proceed with the activation.

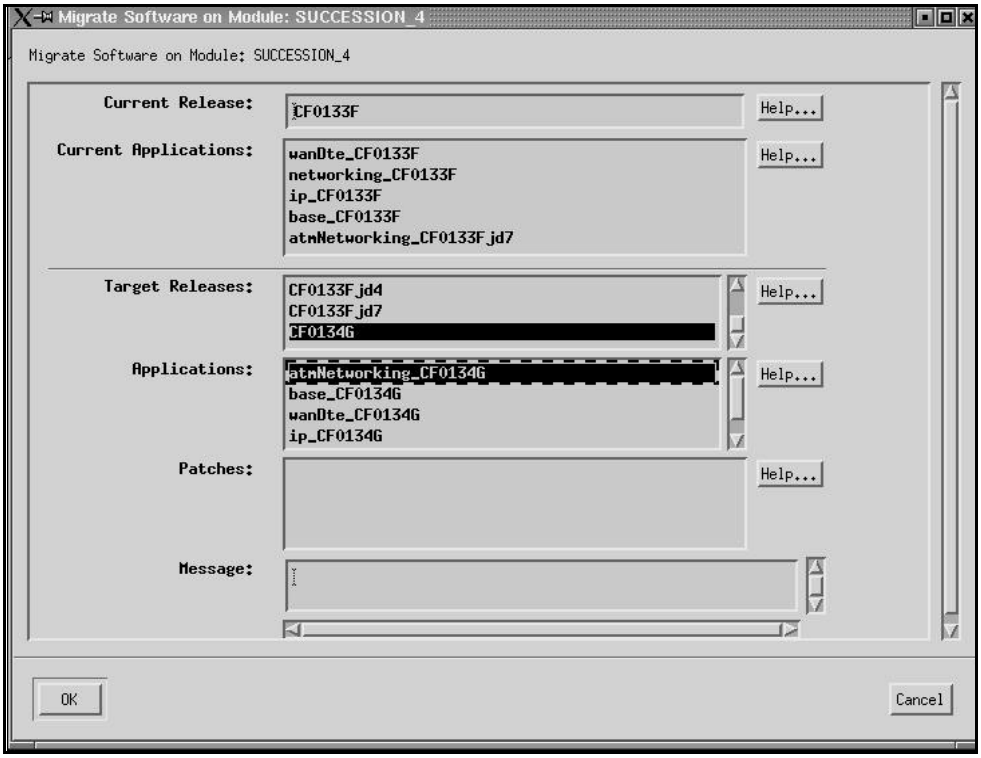
On the Network Activation tool, the **Execute** button changes to grey and can no longer be selected.

The activation begins. Information about the activation is written into the log file: `/opt/MagellanNMS/data/log/nat/nat_<nodename>_<timestamp>.log`.

As each process is performed, the corresponding field in the record turns from blue to green. If the action completes successfully, the field turns from green to blue and the next field turns green. If an action fails, the entire record turns red or yellow according to the severity of the error. While execution is underway, **Execute** is replaced by a **Stop** button that can be used to halt execution.

A window opens displaying the results of the pre-check and post-check commands. If a fault is found, the operator can stop the script (for example, if there is a fault on a component and the the operator wants to fix it), fix the problem and repeat the process until all problems are corrected.

The Migrate Software on Module window opens.



14 In the Migrate Software on Module window, select the target release.

15 In the Migrate Software on Module window, select the software version that is the destination software version. Verify that the application version selected matches the application version in the Current Applications field.

16 Select the required patches from the patch list.

Note: When migrating from a pre-SN07 release (SN06, SN06.2) to SN07, patches cannot be specified. Refer to step 8 in procedure Perform HSM using Command Console on page 886 for more details on how to apply patches in SN08.

17 If you would like to proceed with the migration, click **OK**.

18 The script progresses to the pre-activation stage and executes pre-HSM verification checks.

Note: You should monitor the *prov* component using the Component Information Viewer. While the activation is in progress, you should monitor for alarms from the node using the MDM alarm display. The migration should be stopped if unexpected warnings or alarms appear.

Pre-HSM verification checks

1 Monitor the pre-HSM verification.

While the record is executing the pre-HSM portion of the script, information is displayed and you may be prompted to continue with the software migration or to abort the software migration.

Note: The Command Console CLI response format is different from the SASM tool GUI command response format because the SASM format is optimized for automated processing. The information presented is the same.

Error messages can occur for various reasons, for example: if another operator is also provisioning or if there are warnings or errors from the check prov and so forth.

For information on how to handle these error messages, see "Impact of an error condition on a HSM using the SASM tool" in NN10070-461 *Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1*.

HSM activation

1 At the completion of the pre-activation portion of the script, you are asked if you want to continue with the software migration. If you would like to proceed, press **Enter**.

The migration takes place. The number of calls and components that have been provisioned on the node determine how long the activation takes.

Monitor the status of the node and the status of the migration. To monitor the progress of the migration, use the Component Information Viewer to display the attributes of the provisioning component. You can continue to do this until you lose connectivity to the node, which is when the originally active CP begins to load the new software. The MDM server automatically reconnects to the node when possible.

While the activation is in progress, monitor the alarms from the node using the MDM Alarm Display. If unexpected warnings or alarms appear, stop the migration. Refer to What happens to the node during a hitless software migration on page 857 for more information.

2 When the software migration pauses, you are prompted to either stop the migration or continue the migration.

The software migration will pause because the **-pause** option is mandatory or, there is something wrong with the application during the software migration (Phases 1 to 3).

a When the software migration has paused and *Pbg* components have been provisioned, perform steps 15 to 17 from the procedure Perform HSM using Command Console on page 886. If the CS2000 and SAM21 connections have returned to service, click **Continue**.

b Review the Migration Visible Alarms to determine whether or not you should continue the migration. Click the appropriate button to continue or stop.

CAUTION
Contact GNTS before continuing during a migration pause
Contact Nortel Global Networks Technical Support (GNTS) for advice or assistance before continuing if the software migration pauses due to a Migration Visible Alarm.

Post-HSM verification and Fabric upgrade

After the HSM activation phase and commit phase are complete, the Network Activation tool starts the post-HSM verification portion script. After the record has executed the post-HSM verification, a fabric card firmware upgrade is performed on each fabric card if required.

Information on the result of the fabric card firmware upgrade and fabric card test is written to the log file. If the first fabric card firmware upgrade does not complete successfully, the second fabric card firmware upgrade is not attempted.

HSM script completion and final steps

When all actions in the record have completed successfully, the entire record turns blue.

1 Double-click on the executed record in the record list to display and review the logged information. Alternatively you can choose Show Status from the record list pop-up menu.

2 Select **Exit** from the File menu to close the Network Activation Tool.

3 Select **Exit** from the File menu to close the Component Information Viewer tool.

4 If you have configured in-band OAM, use step 22 to step 26 inclusive in Verify the success of HSM on page 907 to compare the status of the *Atmmpe* components with the information you gathered in steps 22 to 24 of the procedure Verify the success of HSM on page 907.

5 If **display -o prov** shows a different version number for the `editViewName` from the `committedFileName`, execute the following comments through the `commandConsole`:

```
PROV 3> st pr
Prov
ok              2004-06-01 10:36:06.01

PROV 4> load -file(<committedFileName>) pr
Prov
   Loaded or applied file <committedFileName>.
ok              2004-06-04 10:20:47.36

PROV 5> end pr
Prov
ok              2004-06-01 10:36:09.45
```

The following output shows an example of misaligned `editViewName` and `committedFileName`.

```
Prov
   adminState = unlocked
   operationalState = enabled
   usageState       = idle
   provisioningActivity = none
   activityProgress     = n/a
   standbyCpActivity    = none
   standbyCpActivityProgress = n/a
   committedFileName         = CF0124F_April_27.full.001
   currentViewFileName       = CF0124F_April_27.full.001
   lastUsedFileName          = CF0124F_April_27.full.001
   provisioningSession       =
   provisioningUser          =
   checkRequired             = no
   confirmRequired           = no
   editViewName              = CF0124F_April_27.full.001
   editViewAddedComponents   = 0
   editViewDeletedComponents = 0
   editViewChangedComponents = 0
   currentJournal            = 0
   journalDisabledReason     = not disabled
   restorePossible           = no
```

Stop the HSM using MDM SASM tool

At any decision point during the software migration before the activation phase has begun, the operator can select **Abort** or **Cancel** and the migration stops. The Network Activation and MDM Component Information Viewer windows can be closed by selecting **File** and then **Exit**.

During the pre-script phase, you can stop the process by entering **<Ctrl> -C** in the pre-script window.

After the software activation has started and before the migration switchover phase starts, it is possible to abort the software migration hitlessly by clicking the STOP button in the Network Activation tool's main window. The Network Activation tool sends a **stop prov** command to the node and all the tool's processes stop. The success of the stop depends on timing. If the node enters the migration switchover phase before processing the **stop prov** command then it is too late to stop the hitless software migration.

If the system detects a problem during the software migration (phases 1-3), then the hitless software migration automatically pauses before migration switchover occurs. This pause allows you to review the migration visible alarms before continuing or stopping the migration.

To stop the process after the Migration switchover phase has started, click the **Stop** button in the Network Activation Tool main window. Further processing stops on the HSM SASM tool (but not on the node).

Close the SASM tool after stopping an HSM.

- Select **Exit** from the File menu to close the NAT.
- Select **Exit** from the File menu to close the Component Information Viewer window.

To back out after the migration switchover, follow the steps in "Rollback" in NN10070-461 *Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1*.

CAUTION
Non-hitless process
Stopping the process after the HSM switchover is not a hitless process.

Feature activation

The following optional features can be activated:

- Recurring fan alarm enhancement if you are upgrading from SN06 to SN08. If your current release is SN07 or SN08, this feature should already be enabled.
- setting the Solution release name identification

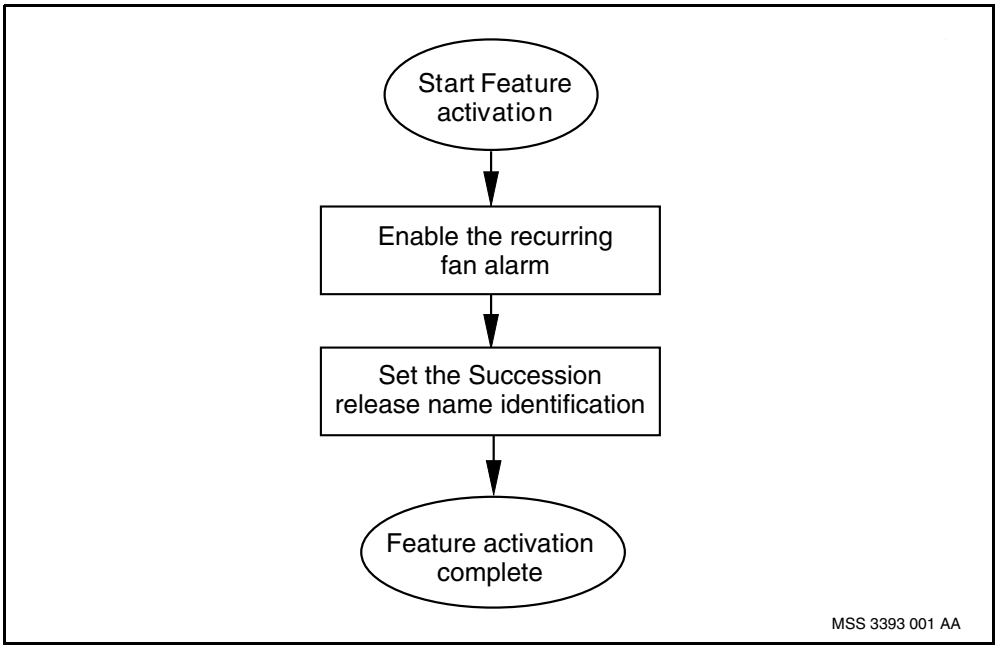
Prerequisites

- Complete the HSM. See HSM (Command Console) activation on page 884 and HSM (MDM SASM tool) activation on page 913 for more information.

Feature activation task flow

The task flow shows you the sequence of tasks you must perform to activate new features.

Feature activation work flow



Work flow navigation

- Enabling the recurring fan failure alarm enhancement on page 928
- Setting the Solution release name identification on page 929

Enabling the recurring fan failure alarm enhancement

In a Carrier Voice over IP solution, Nortel recommends configuring the recurring fan failure alarm on Nortel Multiservice Switch 15000 nodes. If a fan fails, the alarm 7012 0051 is always raised. If the recurring alarm is configured, the alarm is 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 operators' attention to the problem and ensures action is taken before an outage occurs.

Prerequisites

- SN08 software must be running on the node.

From the node

1. Log in with 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 the section "Troubleshooting a software upgrade" in NN10070-461 *Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1*.
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

Setting the Solution release name identification

The *commentText* field of the MSS15000 shelf component contains record release and load information that appears in the following order:

- Solution release
- patchlevel of Nortel 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 Solution (Carrier Voice over IP) release the MDM and MSS15000 are running, you can use the MDM toolset to modify the Solution release name in the *commentText* field of the Multiservice Switch 15000 shelf component for MSS 15000/MG 15000 in a VoIP network. See NN10419-461 *Upgrading Nortel Multiservice Switch 15000 and Media Gateway 15000/20000 in Carrier Voice over IP Networks* for more information.

For MSS15000 in Core ATM networks, migration is done through the SASM tool. When the SASM tool migrates the MSS15000 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 Carrier Voice over IP pre and post scripts to validate the node state before and after the migration. When the post-activation script is finished, the tool prompts the operator to enter the Solution release name.

An alternate way to set the Solution release name on MSS15000 is by using the **Set Shelf Commenttext** command.

Perform either the:

- Setting Solution release name using the Set Shelf CommentText command on page 930 or
- Setting Solution release name for MSS15000 on page 931

Setting Solution release name using Set Shelf CommentText command

Setting Solution release name using the Set Shelf CommentText command

From the node

1 Log in with the appropriate permissions.

2 Display the comment text field:

display Shelf CommentText

The following shows sample output for this command:

```
7> display Shelf CommentText

SN07, MDM 151-09, 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 current text to contain the string “SN08” and leave the remainder of the text unchanged. For example:

"**set Shelf CommentText SN08, MDM 151-09, IM9095 1.01, IM1662 1.35, IM1661 1.04, Spec 2.0**"

Setting Solution release name for MSS15000 using SASM

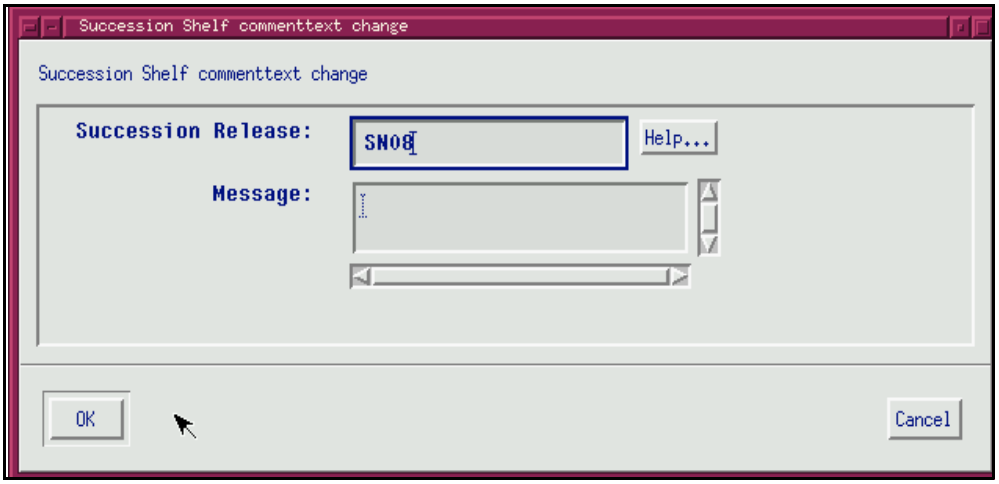
Prerequisites

- The MSS15000 hitless software migration must have been performed using the MDM SASM tool.

Setting Solution release name for MSS15000

From the MDM server

1 The SASM tool post-activation script prompts you for the new Carrier Voice over IP release name to display in the MSS15000 Shelf CommentText. Use the format: SNxx.y.



If you click **Cancel**, the update is cancelled before execution and the MSS15000 Shelf *CommentText* remains unchanged.

2 Click **OK**.

A NAT record is created and the NAT window is displayed for a second time since the start of SASM.

This time it activates the service data (the only change is the S*helf CommentText*) with no pre- and post checks.

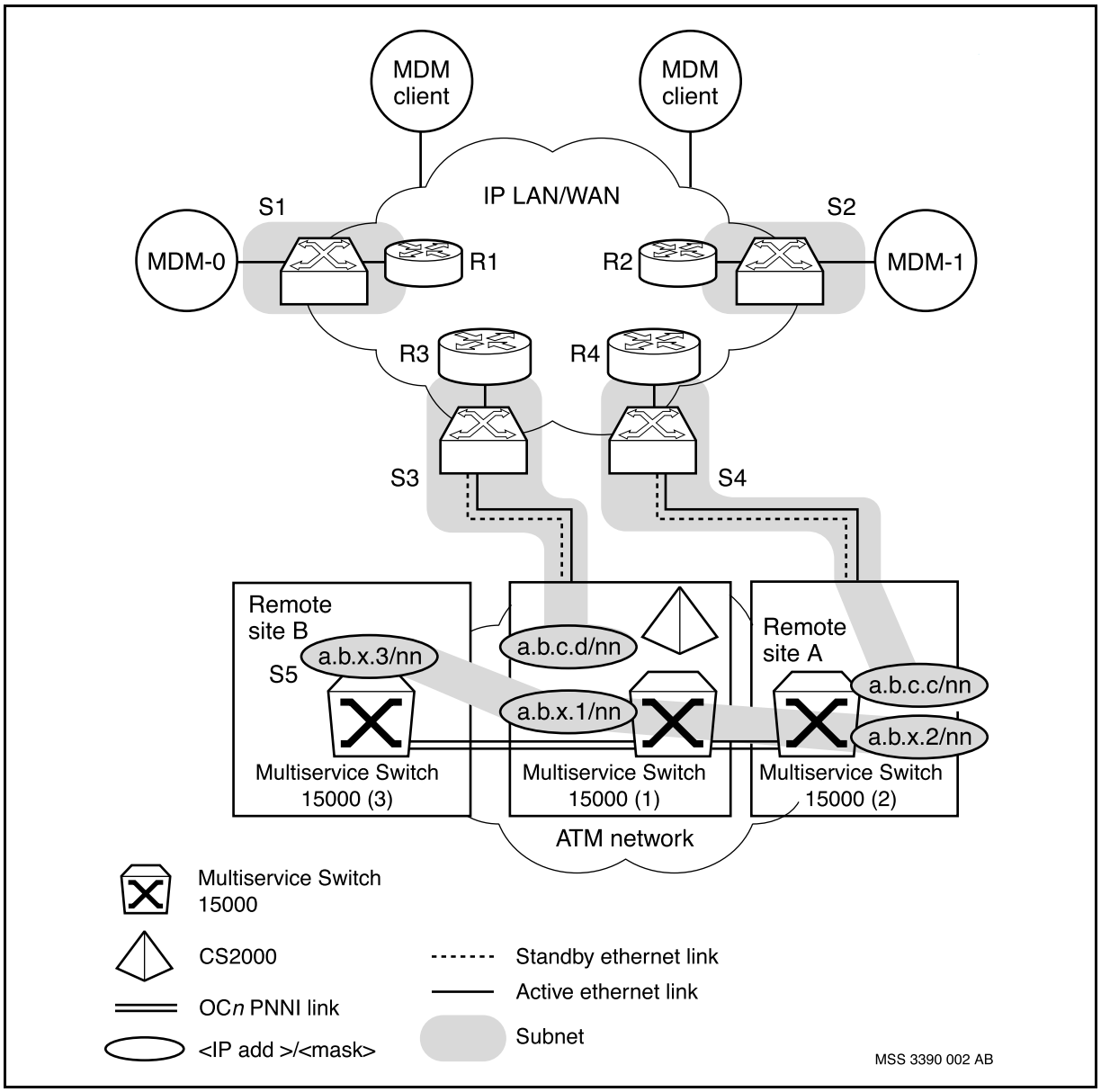
The *Shelf CommentTex*t attribute on the target node is updated with the Solution release name being displayed before the rest of the information in the *Shelf CommentText* field.

In-band OAM quick reference

Key relationships

The figure Sample in-band connectivity topology on page 932, illustrates a typical in-band OAM configuration. A brief description of the items in this diagram and their relationship to each other are provided below.

Sample in-band connectivity topology



MDM-0 and MDM-1

These Nortel Multiservice Data Manager servers are used to manage the Nortel Multiservice Switch network.

The chosen server is the MDM server that the operator uses as a launching point for MDM applications, such as SASM or Command Console.

The alternate server is the other MDM server that could have been used to perform the same set of tasks, except that it was not chosen.

Multiservice Switch -1

This Multiservice Switch 15000 node is in the Office and is a Gateway node using out-of-band connectivity.

From the perspective of 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 MDM-0, S4 represents the subnet to the alternate Multiservice Switch 15000 node.

Multiservice Switch-2 and Multiservice Switch-3

These Multiservice Switch 15000 nodes are Remote nodes using in-band connectivity with Multiservice Switch-1.

S5 represents the in-band OAM subnet. Multiservice Switch-1 has a direct ATMMPE ATM (PVC) connection to every other Multiservice Switch 15000 node.

IP Applications

MSS 15000/20000 UA-IP and PT-IP Applications

The MSS 15000 UA-IP and PT-IP upgrade procedures also apply to upgrading Media Gateway 15000/20000 nodes (formerly known as Packet Voice Gateway).

The migration phase is divided into two parts to reflect the two migration options available:

- HSM from the MSS 15000/MG15000/20000 node using MDM Command Console.
- HSM using MDM Succession IP Software Migration (SISM) tool

Using the SISM tool to perform an HSM is an alternate way to perform an HSM. Automating the Multiservice Switch 15000/20000 and Media Gateway 15000/20000 HSM reduces the chance of errors and increases the speed and efficiency of the software migration.

Software migration

Upgrading a Nortel MSS 15000/MG15000/20000 (A MSS 15000/MG15000/20000 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 Carrier Voice over IP 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) MSS/Media Gateway 15000/20000 nodes, refer to the NN10600-272 *Nortel 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 MDM, see:

- What happens to the node during a hitless software migration on page 970
- Prerequisites to performing a software upgrade on page 935
- Upgrade task flow on page 939

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.

- MDM software is backwards compatible and can manage the current and previous MSS/MG releases. However, MDM software is not necessarily forward compatible. As a result, upgrade MDM servers before upgrading the nodes they manage. To upgrade

servers, see NN10185-461 *Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*.

- If you have DS-1 IMA interfaces using the Edgelink100 MUX, ensure that you use Edgelink100 MUX software (R3.3) during the SN08 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/Media Gateway 15000/20000 in Carrier Voice over IP Networks*, NN10419-461.
- The MSS 15000/MG15000/20000 nodes in your network must be upgraded one at a time to ensure that no service interruption occurs. For in-band OAM topologies, you must upgrade the 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 Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP* and In-band OAM quick reference on page 1063.
  - For all out-of-band OAM configurations, upgrade all the MSS 15000/MG15000/20000 nodes:
    - not physically co-located with the CS2K first
    - physically co-located with the CS2K next
- If the node is being upgraded from SN07 and is patched to support 2 wire Transmit Low Receive High (TLRH) continuity operational test (COT) then the COT will be configured for 4 wire by default after HSM to SN08. Please see Activating 2 wire Continuity operational test (COT) on page 1062 for information on how to re-enable 2 wire TLRH COT.
- You need extensive knowledge of Unix, MSS/MG software, and the Carrier Voice over IP portfolio architecture.

- You need a:
  - user ID for Nortel web support. See Download release notes on page 943
  - user ID for MDM software download
  - user ID for general access to MDM
  - Multiservice Switch user ID configured for local access, and access to FTP, FMIP, Telnet and 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 recommends that you perform the tasks involving commands issued from the command line using MDM Command Console tool rather than a Telnet session. For more information on using the Command Console, see 241-6001-804 *Nortel Multiservice Data Manager Workstation Utilities*.
- 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 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 Multiservice Switch Release Notes* 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 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.

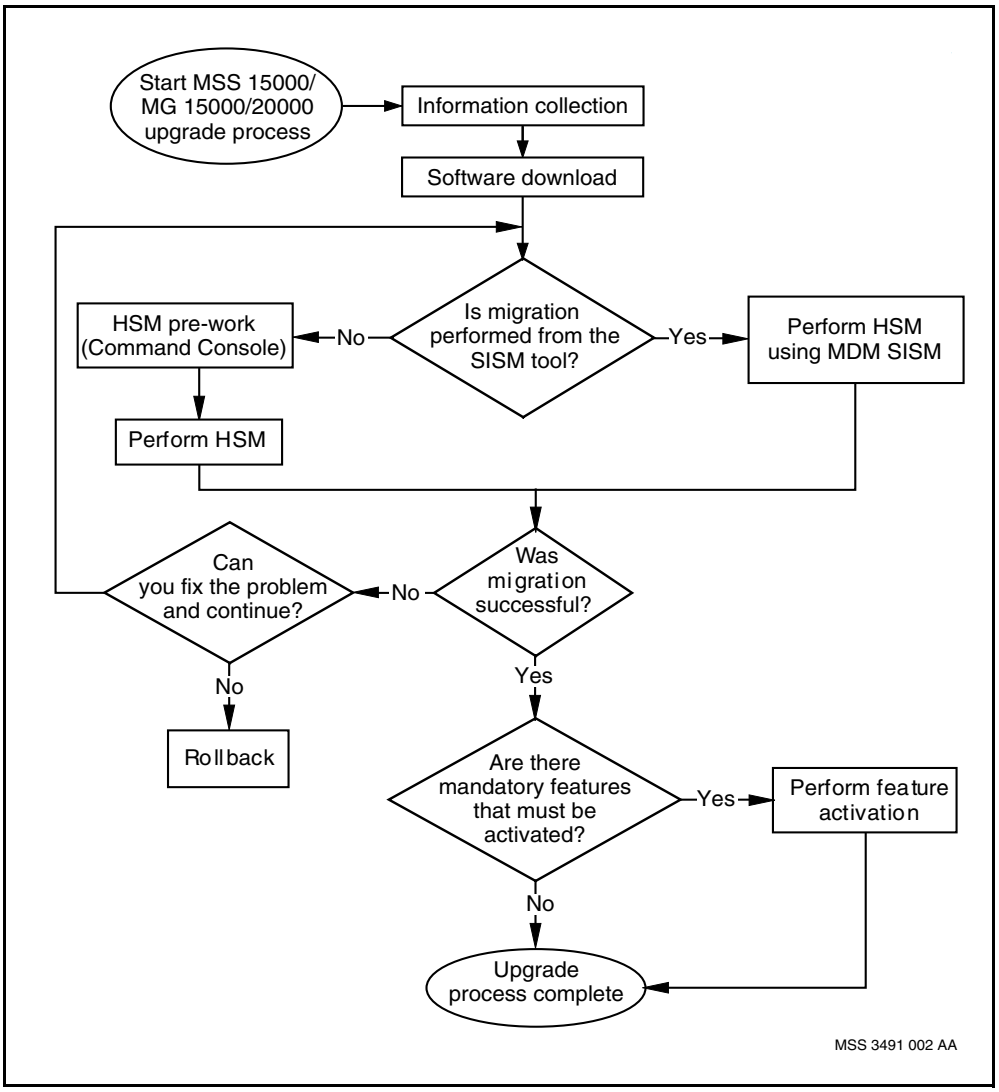
- You must complete the tasks described in the section Upgrade task flow on page 939 before installing additional hardware and configuring additional capabilities.
- Because of the amount of time required to remove old software releases, you may want to do this several days before beginning the upgrade. In particular, running the *tidy Software* command can take several hours to complete. As a result, you may want to run it overnight.
- Ensure you have a backup of the current provisioning view of the Nortel MSS 15000/MG15000/20000 node, see Back up the current view on page 967 for more information.

Upgrade task flow

The figure Upgrade task flow on page 939 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 Multiservice Switch 7400/15000/20000 Upgrading Software* guide.

Upgrade task flow



Work flow navigation

- Information collection on page 941
- Downloading and backing up node software on page 949
- HSM (Command Console) pre-work on page 975 for migrations performed from the Command Console
- HSM (Command Console) activation on page 1004
- Feature activation on page 1056
- “Rollback” in *Upgrading Multiservice Switch 15000/Media Gateway 15000/20000 in Carrier Voice over IP Networks*, NN10419-461

Information collection

Collect information to identify and avoid any compatibility issues that could prevent a software migration from completing successfully.

Prerequisites to information collection

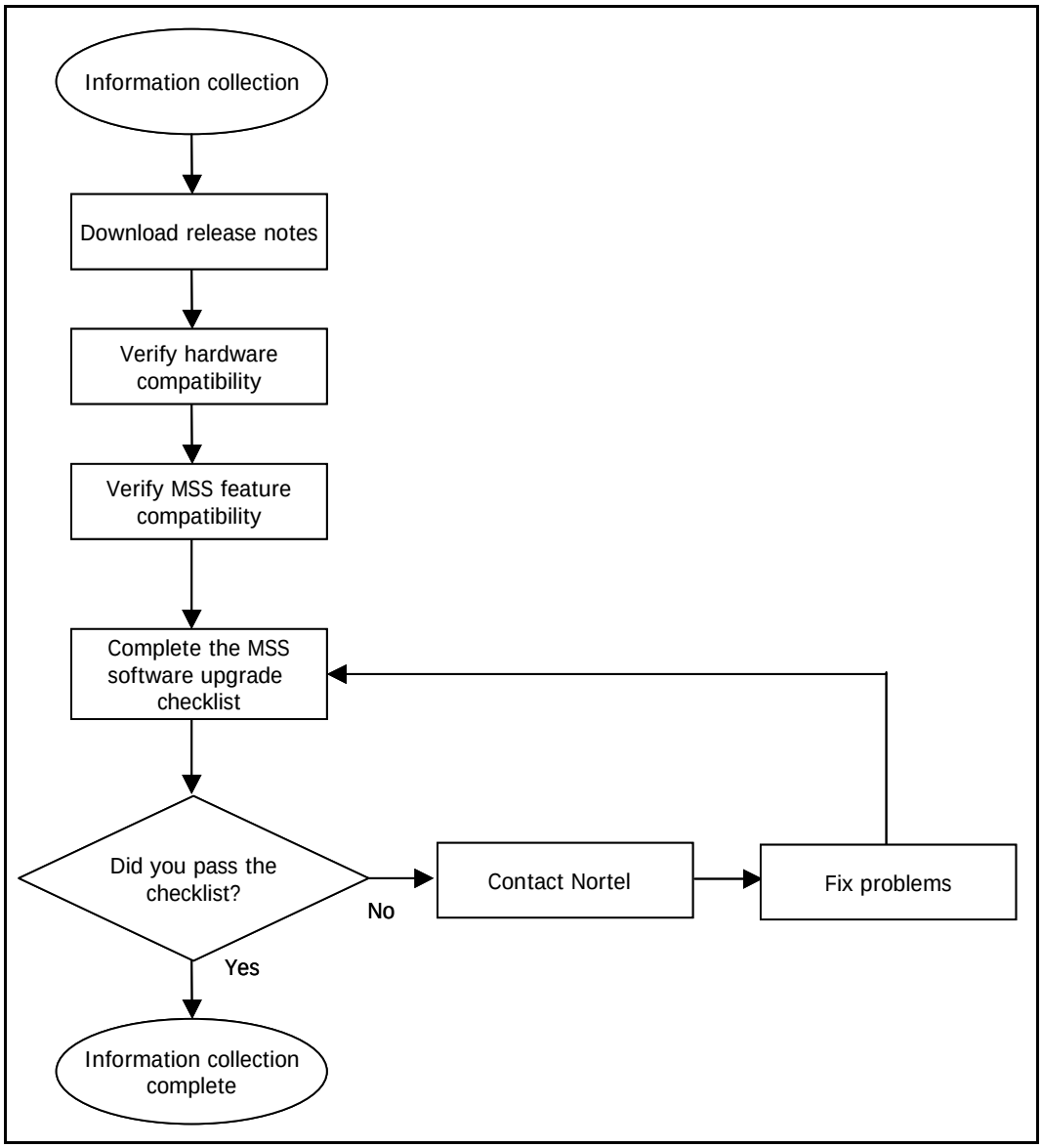
Before you start collecting information, you must:

- determine the order in which the MSS 15000/MG15000/20000 nodes will be upgraded
- determine if the Nortel 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 tasks you perform to collect information about the upgrade. To link to any procedure, go to Work flow navigation on page 942.

Information collection task flow



Work flow navigation

- Download release notes on page 943
- Verify hardware compatibility on page 944
- Verify node feature compatibility on page 945
- Complete the software upgrade checklist on page 946

Download release notes

Download the release notes for MSS 15000/MG15000/20000 in Carrier Voice over IP solutions to collect specific information affecting hardware and services for each of the Multiservice Switch/Media Gateway software release (PCR) and Multiservice Switch for Carrier Voice over IP software releases involved in the migration.

Note: Release notes are required for procedures Verify hardware compatibility and Verify node feature compatibility.

1. Go to the Nortel public website. *http://www.nortel.com/*
2. Click *Support & Training*.
3. Click Technical Documentation.
4. Click Browse product support tab.
5. Click *Product Families*.
6. Click *Passport*.
7. Scroll down to *Passport 15000 Multiservice Switch*.
8. Click *Documentation*.
9. Click *Filter and sort*.
10. Select *Release Notes* from the by Documentation Type menu.
11. Select the release notes for the specified release.

    A security screen appears requesting your user ID and password for web support.
12. Enter your user ID and password.
13. 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 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 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 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 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 941.

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 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 MDM server acting as an SDS.			
The software version patches to be applied have been downloaded and installed on the MDM 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 upgrading, ensure that the correct version of Nortel Multiservice Switch/Media Gateway (MSS/MG) software and the correct patches have been downloaded to the Nortel 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 MSS 15000/MG15000/20000 nodes. The SDS site must be a MDM server for IP.

Prerequisites to software download and backup

Review the prerequisites:

- Within the UA-IP/PT-IP/PT-AAL2/IAC/IAW solutions, one of the MDM servers has been configured as a software distribution site (SDS). The server acting as the SDS manages, stores, and provides access to MSS/MG 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, and ip. If patches have been applied, you will also have the patch application. The application version list must not contain any additional applications.

Note: wanDte, ethernet, pvg, and aal1Ces are not mandatory for all upgrades. Download and activate these in SN08, only if they were present in the pre-SN08 release. For an SN08 to SN08 upgrade, the ipsec application may also be present.

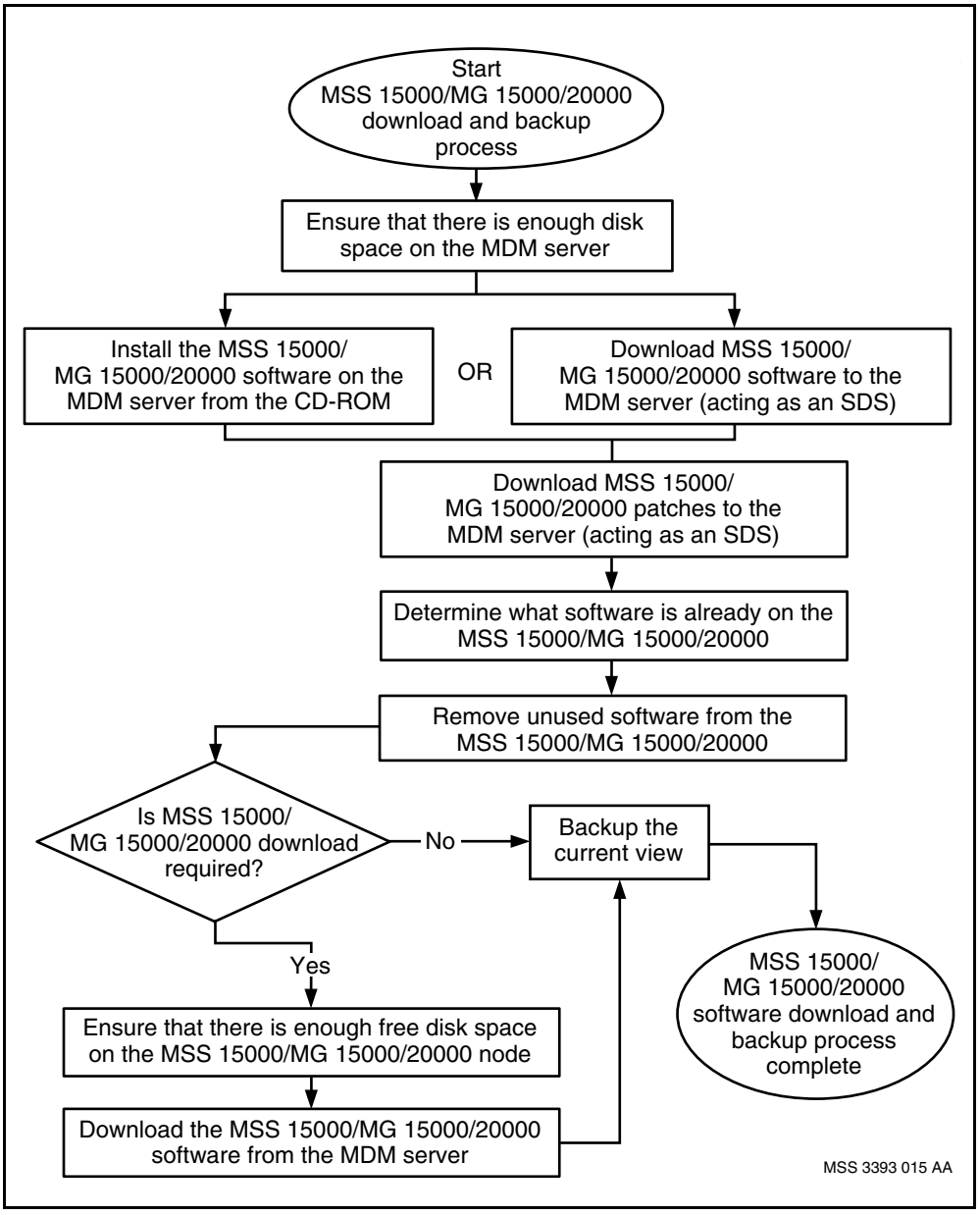
Software download and backup provisioning views task flow

The task flow shows the sequence of tasks to download software and patches to the server acting as the SDS, and then download 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 950.

Two of the procedures are in the NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*. 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 952
- Download the software to the server from Nortel website on page 954
- Download software patches to the server from Nortel website on page 956
- Installing software on the server from CD-ROM on page 959
- “Determining what software is already on the node” in NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*
- “Removing unused software from the node” in NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*
- Ensuring that there is enough free space on the node on page 961
- Download software from the MDM server on page 963
- Back up the current view on page 967

Ensuring that there is enough disk space on the server

Before downloading the required software and patches to the Nortel 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 Multiservice Switch Release Notes* 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 MSS 15000/MG 15000/20000 node using the appropriate permissions.

2 Determine how much disk space is available on the partition containing the MSS/MG 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, aal1Ces, patch and ipsec). 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 website

After verifying that MDM server acting as the SDS has sufficient disk space, you can begin to download the software from Nortel 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 customer representative for more information on accessing the website.
- Refer to the software downloads area of the Nortel website (*www.nortel.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 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.nortel.com*.

3 From Support &Training, select *Software Downloads*.

4 Under the Product Families link, select the family *Passport* or *Succession*.

5 For MSS software in an UA-IP solution from SN07 to SN08 or, from one version of SN08 to another SN08 version in a PT-IP, PT-AAL2, IAC, or IAW solution network, scroll down to the Passport Packet Voice Gateway (PVG) section and select *Software*.

The Software Downloads window opens.

6 Click the version of the release software you want to download.

A Log In window opens.

a Enter your user name and password for the web access login.

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.

7 Click the load name listed beside the File Download heading.

A Save As dialog opens.

8 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/**

9 Click **Save**.

10 On the MDM server, change directories to the directory containing the software (This is the same directory you specified in step 8.):

cd /localdisk/pp15ksw/

11 Uncompress the software file:

uncompress <load_name>.tar.Z

12 Untar the software file:

tar -xvf <load_name>.tar

13 Repeat step 7 through step 12 for every software file you want to download.

14 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 website

In addition to the main software release, you may need to download the patches from Nortel website to the 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 MDM server for IP.

As of SN07, all MSS patches are delivered as a single application version (Av), the patch Av. The patch Av includes all the patches associated with a given software version. Reset and TAP patches are delivered with the patch Av. If you have enabled Patch auto-application, MSS TAP patches will be automatically applied, however, reset patches are not eligible for auto-application and must be manually applied. The patch AV must not be confused with a patched Av, however, a patch AV can include any patches that have been built specifically for a patched Av based on the release.

The patch AV ensures that your switches have access to the complete set of TAP and Reset patches at a given level. The patch AV does not need to be provisioned in the Sw avList to view the patches contained within it, however, it must be provisioned in the Sw avl to be added to the Sw patchList. If you choose to display the patches for the patch Av, all the patches for all the Avs (such as base, atmNetworking, ip) are displayed. If you choose to display the patches for the base Av, all the patches on the CP disk for that SW level will be displayed.

The patch AV tracks the patches for each software level. The AD file contains a list of Patch Version files for that software level. Each Patch Version (PV) file reflects the status of patches when the PV file is created and displays which patches are calculated and applied. The status of the patches on the switch is tracked in version files within the patch AV. Refer to NN10600-272 *Nortel Multiservice Switch 7400/15000/20000 Upgrading Software* for more information about patching.

Prerequisites

- You need an account with a user name and password. Contact your Nortel customer representative for more information on accessing Nortel website.
- Refer to the software downloads area of Nortel website (*www.nortel.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 MSS software and patches are available on the 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.nortel.com*.

3 From Support & Training, select *Software Downloads*.

4 Under the Product Families link, select the family *Passport* or *Succession*.

5 For MSS patches in an UA-IP solution or, to obtain patches for MG 15000/20000 from SN07 to SN08 or, from one version of SN08 to another SN08 version in a PT-IP, PT-AAL2, IAC, or IAW solution network, scroll down to the Passport Packet Voice Gateway (PVG) section and select *Software*.

The Software Downloads window opens.

6 Click the patch that you want to download.

a When prompted to *Login,* enter your user name and password for the web access login.

The Software Downloads: Software Detail Information window opens.

Note: If there are no patches listed for this release, there are no patches currently required for this release. You can move on to the next task in the upgrade process.

7 Click the patch name listed beside the File Download heading.

8 A Save As dialog is displayed.

9 Specify a folder in the home directory of the MDM user to indicate where you want the patch placed. This is typically: */localdisk/pp15ksw/*

10 Click *Save*.

11 On the MDM server, change directories to the directory containing the patch (This is the same directory you specified in step 9.):

cd /localdisk/pp15ksw/

12 Uncompress the patch file:

uncompress <patch_name>.tar.Z

13 Untar the patch:

tar -xvf <patch_name>.tar

14 Repeat step 7 through step 13 for every patch you need.

15 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 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 Multiservice Switch SPCR6.1 software CD. Contact your Nortel customer representative for information on how to order a CD.
- You need the IP address of the Nortel 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 website on page 956.

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/

This is typically: */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, and ip. If patches have been applied, you will also have the patch application. The application version list must not contain any additional applications. The amount of space required for these applications is approximately 350 Mbyte.

  Note: wanDte, ethernet, pvg, and aal1Ces are not mandatory for all configurations. Download and activate these in SN08 only if they were present in the pre-SN08 release. For an SN08 to SN08 upgrade, the ipsec application may also be present.

- 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 Multiservice Switch Release Notes* and the software downloads area of Nortel website (*www.nortel.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 Multiservice Switch 7400/15000/20000 Software Installation*.

From the node

1 Log in to the MSS 15000/MG15000/20000 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 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 *Nortel Multiservice Data Manager Management Data Provider*.

Download software from the MDM server

Before beginning the hitless software migration (HSM), you need to download the software from the Nortel MDM server acting as the SDS for the nodes.

Prerequisites

- Download the software to the server from Nortel website on page 954
- Download software patches to the server from Nortel website on page 956
- You have performed the procedure “Ensuring that there is enough free space on the file system” see NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*.
- Download the software files for the following applications: base, networking, atmNetworking, and ip. If patches have been applied, you will also have the patch application. The application version list must not contain any additional applications.

  Note: wanDte, ethernet, pvg, and aal1Ces are not mandatory for all configurations. Download and activate these in SN08 only if they were present in the pre-SN08 release. For an SN08 to SN08 upgrade, the ipsec application may also be present.

- 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 firmware on page 1021.
- Refer to the software downloads area of Nortel website (*www.nortel.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 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 website on page 954.
- Use the MDM server Command Console tool to perform this upgrade. For more information on opening the Command Console, see 241-6001-804 *Nortel Multiservice Data Manager Workstation Utilities*.

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 SN08 if it is present in the pre-SN08 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 1006.

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 SN08 in a UA-IP, 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 SN08. 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 HSM overview on page 970 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 977 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 SN08.

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 website (*www.nortel.com*) were downloaded:

list Software ApplicationVersion/* Patch/*

Variable values

Variable	Value
<application_versions>	A space-separated, case sensitive list of application versions. You must download the new version of the base, networking, atmNetworking, ip, wanDte, ethernet, pvg, and aal1Ces applications. *Note*: WanDte is not mandatory for all upgrades. It must only be downloaded and activated in SN08 if it is present in the pre-SN08 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 firmware on page 1021.
i960	An attribute indicating that the i960 processor type is being used. This attribute is always required.
<ipAddress>	The IP address of the MDM SDS server.
<password>	The password for the, <userID> on the 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 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 MDM server or another Nortel 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 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 MSS 15000/MG15000/20000 Backup provider, and the MSS 15000/MG15000/20000 restore provider must all be running on the MDM server in order for the Service Data Backup/Restore tool to function properly. Using the 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 *Nortel Multiservice Data Manager 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 Multiservice Switch 7400/15000/20000 Software Installation* for information on making them the same.

- The 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 MDM server.

2 Open a MDM window:

/opt/MagellanNMS/bin/nmstool &

The copyright dialog and the MDM window open.

3 Click **OK** to close the copyright dialog.

4 From the MDM window, select Configuration > MSS > Administration > MSS Service Data Backup/Restore.

The MSS Service Data Backup/Restore window opens.

5 Click **Add ...**.

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 MSS Backup and Restore window.

10 Click **Backup** to start the backup procedure for all the devices listed in the Device List of the main MSS Backup and Restore window.

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.

HSM overview

This section describes Nortel 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 975. For information on post-migration checks, see Verify the success of HSM on page 1029.

What happens to the node during a hitless software migration

Nortel Multiservice Switch 15000/20000 and Media Gateway 15000/20000 nodes support hitless software upgrades in PT-IP, PT-AAL2, IAC, or IAW solutions. Nortel Multiservice Switch 15000 and Media Gateway 15000 nodes support hitless software upgrades in Carrier Voice over IP 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.

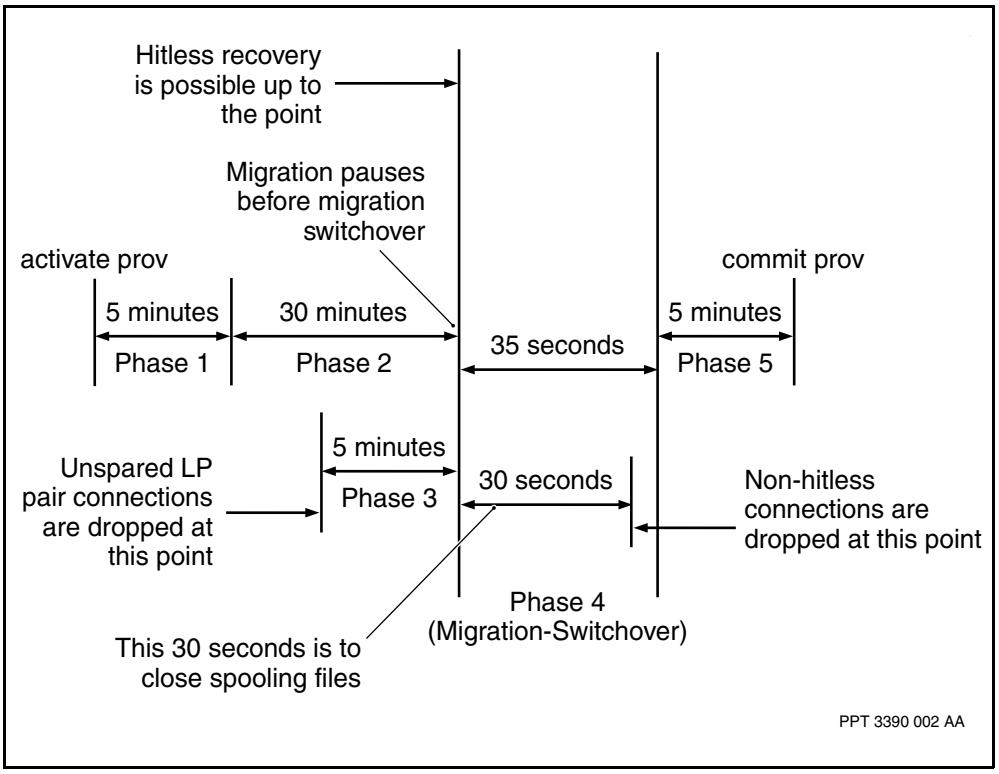
If a problem is detected by the system, the process pauses automatically allowing the operator to stop migration or fix the problem and continue.

The five phases of a hitless software migration are as follows:

- Phase 1 - Preparation of the CP on page 972
- Phase 2 - CP migration on page 972
- Phase 3 - FP migration on page 973
- Phase 4 - Migration switchover on page 974
- Phase 5 - Post migration on page 974

Refer to the figure Hitless software migration phases. on page 971 for more information about the phases.

Hitless software migration phases.



Phase 1 - Preparation of the CP

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

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 or part of an LP group, 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 in a one-for-one sparing model or part of an LP group, 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

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 issue a **stop prov** command to stop the software migration and fix the problem indicated by the alarm which caused the pause and then issue a **continue -force prov** command to continue with the migration switchover.

After a **continue -force prov** command is issued, the system does not pause again.

Phase 4 - Migration switchover

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

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

Before doing an HSM, ensure that the auto-patch script (ppautopatch) is not running and that it does not run during the HSM. Issue the following commands on both MDM servers where a ppautopatch script could be configured to run for the node being upgraded:

1. **touch /opt/MagellanNMS/cfg/private/noppautopatchrun**
2. **ps -ef | grep ppautopatch**

If the second command returns only one response, such as the following, it is ok to go ahead with the HSM:

```
ps -ef | grep ppautopatch

root 6453 29431 0 09:10:53 pts/11 0:00 grep
ppautopatch
```

If the second command returns one or more additional responses, such as the following, then the ppautopatch script is running.

```
ps -ef | grep ppautopatch

root 2112 282 0 Dec 03 ? 13:50 ppautopatch -download
-host 47.1.2.3 -huser pp15ksw pp15ksw -apply -nodes
OFFICE1 -nuser config config -max_duration 1 h

root 6453 29431 0 09:10:53 pts/11 0:00 grep
ppautopatch
```

Note 1: The script does not typically take a long time to run so, in general, Nortel recommends waiting until all ppautopatch scripts are finished before starting the HSM.

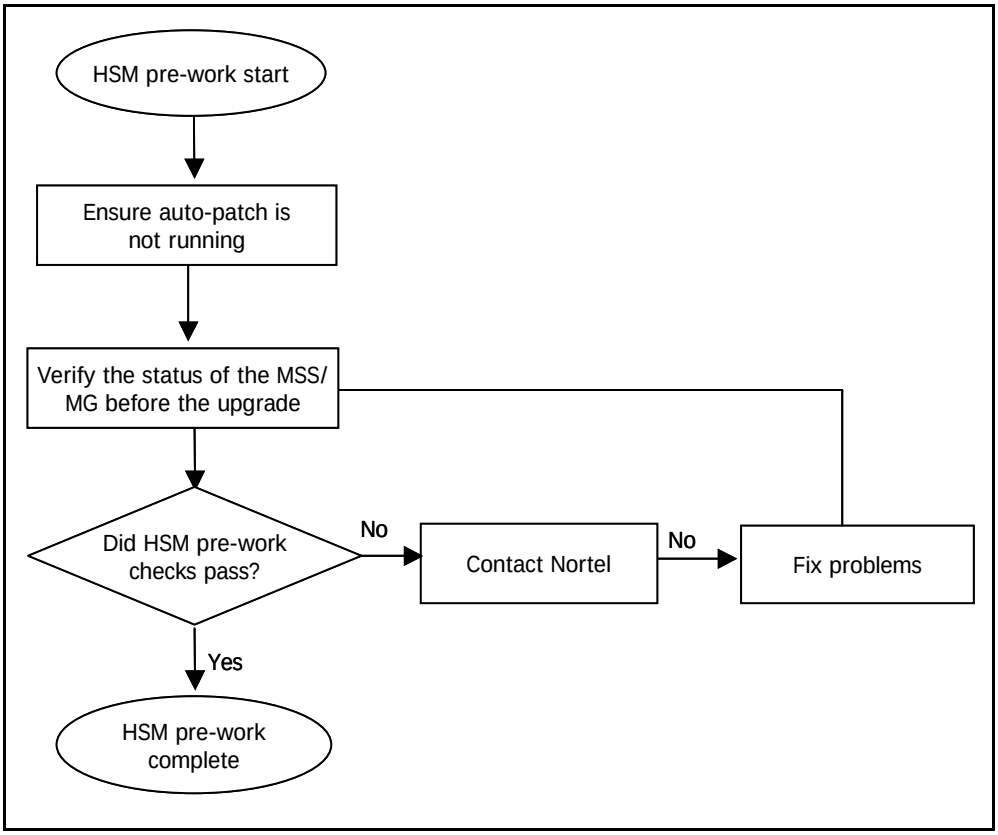
Note 2: On an MDM that manages nodes in more than one Carrier Voice over IPoffice, a running script may not necessarily include the node to be upgraded (refer to the -nodes parameter value for the ppautopatch script). If you are sure that none of the running scripts pertain to the node being upgraded, proceed with the HSM.

Note 3: The noppautopatchrun file should be deleted on both MDM servers after the HSM is completed. If performing HSM on a series of nodes from the same MDM, do not remove the file until after all the HSM's have been performed.

HSM task flow

The task flow shows the sequence of tasks 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 MSS 15000/MG15000/20000 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 do not cover ASPEN signalling and/or electrical TDM cards and 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 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 MDM server session:

display prov provisioningSession

Note: To find the value of the 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 l: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 standby control processor should have a value of either *hot*, indicating hot standby or *cold*, indicating cold standby, depending on how the node is configured.

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 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
```

15 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
```

16 If the node is connected with GigE to a ERS 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
```

17 Verify that all the *Sonet* or *SDH* ports configured on the system are enabled, unlocked, and free of alarms:

display Lp/* Sonet/* osistate

display Lp/* Sdh/* osistate

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *SONET* or *SDH* 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
```

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 and enabled.

Acceptable values for the operational attribute *NearEndRequest* (*neReq*) are `NoRequ` (noRequest) and `doNot`R (doNotRevert).

The following shows a sample output for this command:

```
display Laps/*
--------------------------------------------------------------------------------
 Laps  |osiAd|osiO|osiUs|neRxLi|neReq  |neReqC|feReq  |feReqC|sdOnLin|switchovers
       | min | per | age |  ne  |       | han  |       | han  |  es   |
--------------------------------------------------------------------------------
   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* and *vc4* components have a value of *off*.

display Laps/* Sts/0

display Laps/* vc4/* osiState

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* and *E3* components have been configured, verify that the components are enabled, unlocked, and free of alarms:

display lp/* ds3/* osistate

display Lp/* e3/* osiState

The osiAdmin column should contain only *unlck* values. The osiAvail column should be empty. All of the *DS3* or *E3* 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 GE ports on 2pGeMmSrVsp3 FP cards are being used, ensure that they are in the proper state to carry traffic.

display lp/* vsp Gige/* osiAdmin, osiOper, negAlarm, remFaultAlarm

The ports should be unlocked, enabled, off and off.

34 If the MSS 15000/MG15000/20000 node is connected with GigE to a ERS 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 |
```

35 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|
```

36 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
```

37 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|
```

38 If the MSS 15000/MG15000/20000 node is connected with GigE to an ERS 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|
```

39 If the MSS 15000/MG15000/20000 is connected with GigE to an ERS 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
```

40 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 cardboard (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
```

41 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
```

42 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|
```

43 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|
```

44 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|
```

45 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 |
```

46 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
```

47 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|
```

48 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|
```

49 Verify that all *SpvcAp* components are unlocked, enabled and active:

display Nsta/* Vgs Ctrl/* SpvcAp svcStatus

display Nsta/* Vgs IpMConn SpvcAp svcStatus

display Nsta/* Vgs AtmTConn/* SpvcAp svcStatus

The svcStatus should be *connected*.

50 If VrAP was provisioned in your solution, find and verify the VrAP status. (Otherwise, go to step 52.)

First enter the following command to verify the VrAP provisioning.

display Nsta/* Vgs Ctrl/* vrap

```
> display Nsta/* vgs Ctrl/* vrap

Nsta/* Vgs Ctrl/* Vrap
-------------------------------------------------------------------
|Nsta |Ctrl|Response|
-------------------------------------------------------------------
|   6|mg  |Component has no operational data
```

Then enter the following command to verify the logical interface address connection.

display Nsta/6 Vgs Ctrl/mg vrap sub

```
> display Nsta/6 vgs Ctrl/mg vrap sub

Nsta/6 vgs Ctrl/mediaGateway vrap
   subnetAccessName = Vr/1 Pp/PVG IpPort Logicalallf/172.16.200.1
```

51 To verify the full connectivity, ping the logical interface from the interconnected router.

ping 172.16.200.1

```
8600-0:5# ping 172.16.200.1
172.16.200.1 is alive
```

Note: This sample output is from an Ethernet Routing Switch 8600 where the MG15000 is interconnected.

52 Verify that all *vt1dot5* and *vc12* components are unlocked and enabled:

display Laps/* Sts/* vt1dot5/* osistate

display Laps/* vc4/* vc12/* 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
```

53 Verify that all *vt1dot5, DS1* and *E1* components are unlocked and enabled:

display Laps/* Sts/* vt1dot5/* ds1/* osistate

display Laps/* vc4/* vc12/* e1/* 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
```

54 Verify that all *vt1dot5, DS1 Chan* and *E1 Chan* components are unlocked and enabled:

display Laps/* Sts/* vt1dot5/* ds1/* chan/* osistate

display Laps/* vc4/* vc12/* e1/* 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
```

55 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|
```

56 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|
```

57 Verify that all *Q921* components are unlocked, enabled and active. For VSP3-0 FPs, use the following command:

display Nsta/* vgs q921/* osistate

For VSP2 and VSP3 FPs, use the following command:

display Nsta/* vgs brags/* Q921

The following shows sample output for the first command:

```
> display Nsta/* vgs q921/* osistate

Nsta/* Vgs Q921/*
-------------------------------------------------------------------
|Nsta |Q921|osiAd|osiO|osiUs|Response
|     |    | min |per | age |
-------------------------------------------------------------------
|   12|  22|unlck|ena |activ|
```

58 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.

59 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
```

60 Optionally, display, ping, and record information about the IP accessibility of the node to verify the accessibility 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
```

61 Verify and record information about the IP accessibility of the first 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)
```

62 Verify and record information about the IP accessibility of the second MDM server from the node:

ping -trace -ip(<MDM2 IP>) Vr/0 Ip Icmp

In conjunction with step 61, ensure that both 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.

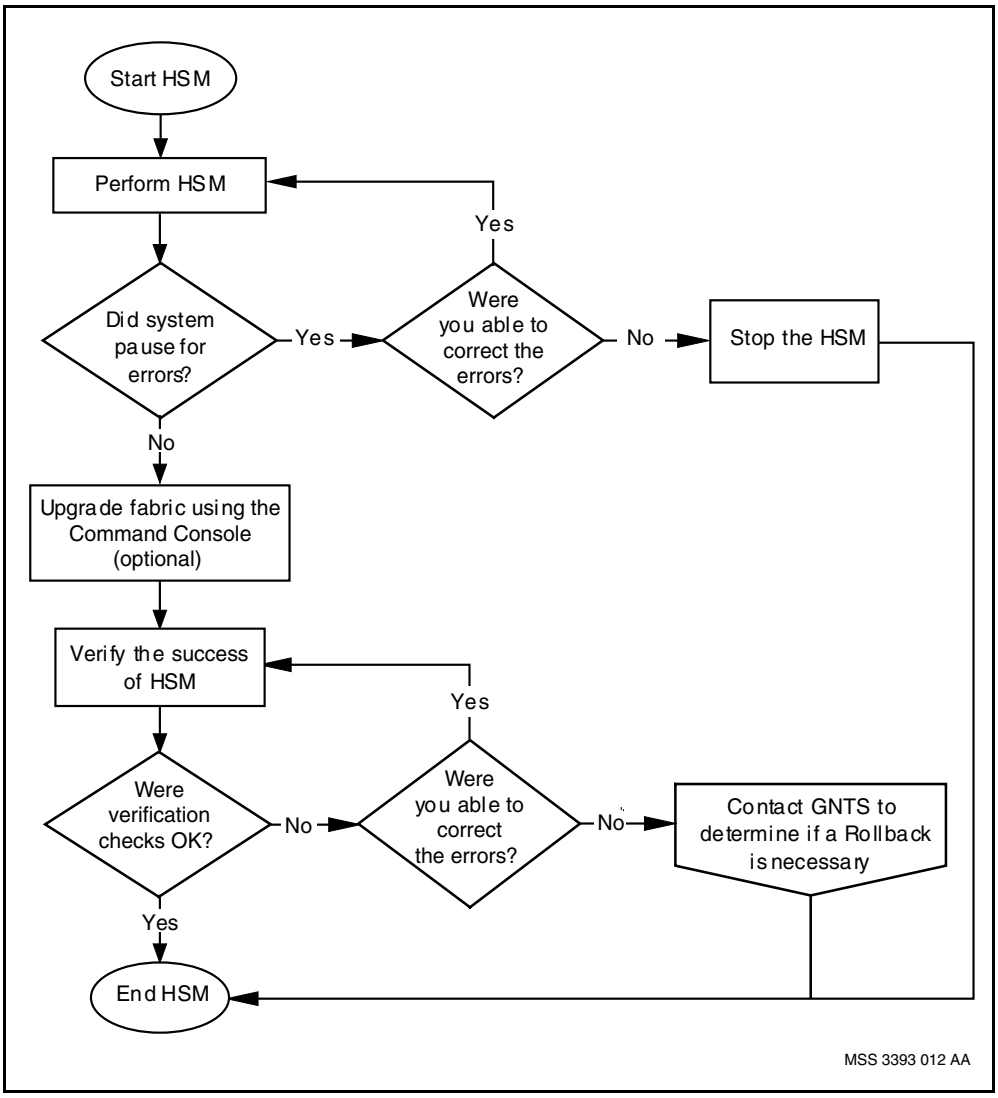
Prerequisites

- Complete the HSM pre-work. See HSM (Command Console) pre-work on page 975 for more information.
- Upgrade the MSS 15000/MG 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 Software upgrade checklist on page 946.

HSM task flow

The task flow shows the sequence of tasks you need to perform the HSM. To link to any procedure, go to the Work flow navigation on page 1005.

HSM task flow



Work flow navigation

- Perform HSM using Command Console on page 1006
- Upgrade the fabric firmware on page 1021
- Verify the success of HSM on page 1029
- Stop the HSM using Command Console on page 1037

Perform HSM using Command Console

Upgrade MSS 15000/MG15000/20000 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 firmware on page 1021 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 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 *Nortel Multiservice Data Manager Workstation Utilities*.
- The MSS 15000/MG15000/20000 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 Carrier Voice over IP portfolio architecture.
- Activate the same software applications in SN08 that are present in the current software release (SN07) to allow hitless software migration. These applications may include: base, networking, atmNetworking, and ip. If patches have been applied, you will also have the patch application. The application version list must not contain any additional applications.

  Note: wanDte, ethernet, pvg, and aal1Ces are not mandatory for all configurations. Download and activate these in SN08 only if they were present in the pre-SN08 release. For an SN08 to SN08 upgrade, the ipsec application may also be present.

- Refer to the software downloads area of the Nortel Web site (*www.nortel.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 Log in 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 referred 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 to SN08 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 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, and ip. If patches have been applied, you will also have the patch application. wanDte, ethernet, pvg, and aal1Ces are not mandatory for all configurations. Download and activate these in SN08 only if they were present in the pre-SN08 release. For an SN08 to SN08 upgrade, the ipsec application may also be present. 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 firmware on page 1021 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>

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 SN07 applications are base, networking, ip, pvg, aal1Ces, atmNetworking, wanDte patch and ipsec, then the SN08 applications must be the same).

Nodes with 4pGe FP cards that are being upgraded from a release prior to SN07 require 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.

set Software avList ethernet_CF01SLB

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 to SN08 in a PT-IP, PT-AAL2, IAC or IAW solution networks, go to step 9.

Note 2: If you are 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 Multiservice Switch Release Notes for this release* to determine the software patches required and apply the patches if needed for SN08 to the patchlist.

set Software patchlist ! <patches>

Attention: If you are migrating directly from a pre-SN06 release to SN08 FCS with patches, you must apply a patch to your current release before downloading the SN08 FCS software.

Switches must be running baseFT420A_XXXX.

Once this patch is applied, download the SN08 FCS software, including patch_CF01xxx. Then migrate to SN08 FCS with patches as described in this procedure.

Contact Nortel 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 1029.

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_CF0XXXX_UNIQUE_IDENTIFIER

"UAIP" identifies the Carrier Voice over IP Solution. "CF0XXXX" identifies the MSS 15000/MG15000/20000 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 1037.

Apply the changes:

activate -pause prov

Always use the **activate -pause prov** command. The software migration activation pauses before migration switchover occurs and displays a message. The sample shows an example of a successful output for this command.

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 1037.

CAUTION
Exercise caution when using the continue -force prov command
Contact Nortel 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 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 MSS 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 1037. You can choose to continue the migration by typing **continue -force prov.**

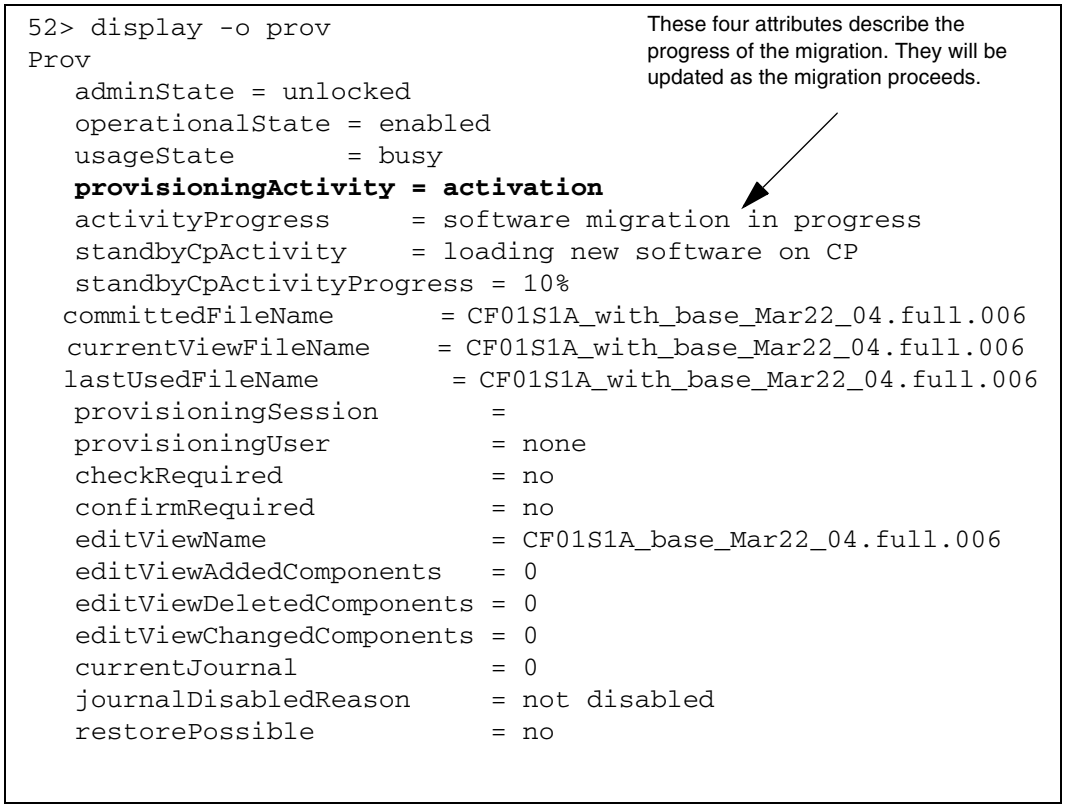
15 To monitor the progress of the migration, enter the following command:

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 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
```

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

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 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 Carrier Voice over IP UA-IP are base, networking, atmNetworking, and ip. If patches have been applied, you will also have the patch application. The application version list must not contain any additional applications. *Note*: wanDte, ethernet, pvg, and aal1Ces are not mandatory for all configurations. Download and activate these in SN08 only if they were present in the pre-SN08 release. For an SN08 to SN08 upgrade, the ipsec application may also be present.
<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 website.

Upgrade the fabric firmware

You can upgrade the fabric firmware installed on MSS/MG fabric cards to take advantage of enhancements and new functionality contained in later firmware releases. All software running on MSS 15000/MG15000/20000 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.

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 Multiservice Switch Release Notes*.
- The new fabric card firmware must be downloaded from an MDM server acting as the software distribution site (SDS). For more information on how to download from the SDS, see NN10600-272 *Nortel 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 Display the attributes of the fabric card banks:

display Shelf FabricCard/<n> banks

The following shows sample output for this command in a SN06 to SN08 upgrade:

```
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
```

The following shows sample output for this command in a SN07 to SN08 upgrade. If the output is:

"recommendedVersionToInstall = Fabric software version is up to date".

a fabric upgrade is not required.

2 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 MDM server on page 963.

3 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    |       |
```

4 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
```

5 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
```

6 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
```

7 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
```

8 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
```

9 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 Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* to interpret the test results.

10

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.

11 Repeat step 3 through step 10 for the other fabric card.

12 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 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 step 7.

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 SN07 to SN08 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 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 977
- Perform HSM using Command Console on page 1006

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 977:

   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 977:

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 977:

display Shelf Card/* SparedServices

If VRs are provisioned, ensure that the CPs OSI sparing availability state is not degraded.

8 Compare the status of the shelf hardware with the status recorded in step 14 of the procedure Verify the status of the node before the upgrade on page 977

display sh hardware

9 Compare the status of the logical processors using the dual L sparing model with the status recorded in step 15 of the procedure Verify the status of the node before the upgrade on page 977:

display Dlep/* osistate

10 Compare the status of the Ethernet ports with the status recorded in step 16 of the procedure Verify the status of the node before the upgrade on page 977:

display Lp/* Ethernet/* osistate

11 Compare the status of the SONET ports with the status recorded in step 17 of the procedure Verify the status of the node before the upgrade on page 977:

display Lp/* Sonet/* osistate

12 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 977:

display Laps/* Sts/0

13 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 977:

display Laps/* osistate

14 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 977:

display lp/* ds3/* osistate

15 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 977:

display lp/* ds3/* ds1/* osistate

16 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 977:

display lp/* ds3/* ds1/* chan/* osistate

17 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 977:

display lp/* ds3/* ima/* osistate

18 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 977.

display lp/* ds3/* ima/* lk/* osistate

19 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 977:

display Atmlf/* osistate

20 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 977:

display atmif/* uni sig/(operatingMode = normal) osistate

21 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 977:

display atmif/* uni ilmi/(operatingMode = addressRegEnabled) osistate

22 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 977.

display Atmlf/* Pnni Sig osistate

23 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 977:

display Atmmpe/* osistate

24 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 977.

display Atmmpe/* Ac/* osistate

25 If the MSS 15000/MG15000/20000 node is connected with GigE to an ERS 8600 node, compare the status of the *LanApplications* components with the status recorded in step 34 of the procedure Verify the status of the node before the upgrade on page 977.

display La/* osistate

26 Compare the status of the *VirtualRouter* components with the status recorded in step 35 of the procedure Verify the status of the node before the upgrade on page 977.

display Vr/* osistate

27 Compare the status of the *ProtocolPorts* components with the status recorded in step 36 of the procedure Verify the status of the node before the upgrade on page 977.

display Vr/* Pp/* osistate

28 Compare the status of the *Ip* components with the status recorded in step 37 of the procedure Verify the status of the node before the upgrade on page 977.

display Vr/* Ip osistate

29 If the MSS 15000/MG15000/20000/Media Gateway 15000/20000 node is connected with GigE to an ERS 8600 node, compare the status of the *Ospf* components with the status recorded in step 38 of the procedure Verify the status of the node before the upgrade on page 977.

display Vr/* Ip Ospf osistate

30 If the MSS 15000/MG15000/20000 node is connected with GigE to a ERS 8600 node, compare the status of the *Ospf neighbor* components with the status recorded in step 39 of the procedure Verify the status of the node before the upgrade on page 977.

display Vr/* Ip Ospf Nbr/* state

31 Compare the status of the static routes with the status recorded in step 40 of the procedure Verify the status of the node before the upgrade on page 977.

display Vr/* Ip static routeEntry/* operationalState, protectionLevel

32 Compare the status of the *nextHop* components under static routes with the status recorded in step 41 of the procedure Verify the status of the node before the upgrade on page 977. The components must have an operational status of enabled.

display Vr/VoIP Ip static route/* nexthop/* operationalState

33 Compare the status of the *Vsp* components with the status recorded in step 42 of the procedure Verify the status of the node before the upgrade on page 977.

display Lp/* Vsp osiState (for VSP3 - NTHW84xx)
and
display Dlep/* Vsp osiState (for VSP3-0 - NTHW77xx)

34 Compare the status of the *ProcessingModule* components with the status recorded in step 43 of the procedure Verify the status of the node before the upgrade on page 977.

display Lp/* Vsp Pm/* osiState (for VSP3 - NTHW84xx)
and
display Dlep/* Vsp Pm/* osiState (for VSP3-0 - NTHW77xx)

35 Compare the status of the *Nsta* components with the status recorded in step 44 of the procedure Verify the status of the node before the upgrade on page 977.

display Nsta/* osiState

36 Compare the status of the *TDMAccessGroup* components with the status recorded in step 45 of the procedure Verify the status of the node before the upgrade on page 977.

display Nsta/* vgs tag/* osiState

37 Compare the status of the *Aal1Ces* components with the status recorded in step 46 of the procedure Verify the status of the node before the upgrade on page 977.

display Aal1Ces/* osiState

38 Compare the status of the *IpMConn* components with the status recorded in step 47 of the procedure Verify the status of the node before the upgrade on page 977.

display Nsta/* vgs IpMConn osiState

39 Compare the status of the *ControlConnection* components with the status recorded in step 48 of the procedure Verify the status of the node before the upgrade on page 977.

display Nsta/* vgs Ctrl/* osiState

40 Compare the status of all SpvcAp components with the status recorded in step 49 of the procedure Verify the status of the node before the upgrade on page 977.

display Nsta/* vgs Ctrl/* SpvcAp svcStatus

display Nsta/* vgs IpMConn SpvcAp svcStatus

display Nsta/* vgs AtmTConn/* SpvcAp svcStatus

41 If VrAP was provisioned, compare the status of the VrAP and the logical interface address connection with the status recorded in step 50 of the procedure Verify the status of the node before the upgrade on page 977. Also compare the ping results recorded in step 51.

display Nsta/* vgs Ctrl/* vrap

display Nsta/* vgs Ctrl/mg vrap sub

42 Compare the status of the *vt1dot5* and *vc12* components with the status recorded in step 54 of the procedure Verify the status of the node before the upgrade on page 977.

display Laps/* sts/* vt1dot5/* osistate

display Laps/* vc4/* vc12/* osistate

43 Compare the status of the *vt1dot5 DS1* and *E1* components with the status recorded in step 53 of the procedure Verify the status of the node before the upgrade on page 977.

display Laps/* sts/* vt1dot5/* ds1/* osistate

display Laps/* sts/* vc4/* vc12/* ei/*osistate

44 Compare the status of the *vt1dot5, DS1 Chan* and *E1 Chan* components with the status recorded in step 54 of the procedure Verify the status of the node before the upgrade on page 977.

display Laps/* sts/* vt1dot5/* ds1/* chan/* osistate

display Laps/* vc4/* vc12/* e1/* chan/* osiState

45 Compare the status of the *CasDefn* components with the status recorded in step 55 of the procedure Verify the status of the node before the upgrade on page 977.

display Nsta/* vgs casdefn/* osistate

46 Compare the status of the *IsdnUserAdaption* components with the status recorded in step 56 of the procedure Verify the status of the node before the upgrade on page 977.

display Nsta/* vgs iua/* osistate

47 Compare the status of the *Q921* components with the status recorded in step 57 of the procedure Verify the status of the node before the upgrade on page 977.

display Nsta/* vgs q921/* osistate

48 Compare the status of the *Q921* components provisioned under the *brags* components for VSP3s and VSP2s recorded in step 57 of the procedure Verify the status of the node before the upgrade on page 977.

display nsta/* vgs brags/*

49 If the node being migrated relies on OAM Ethernet connectivity, compare the status of the active control processor with the status recorded in step 58 of the procedure Verify the status of the node before the upgrade on page 977. For VSP3-0 FPs use the command:

display Lp/0 Oamenet/0 activeStatus

50 If the node being migrated relies on OAM Ethernet connectivity, compare the status of the standby control processor with the status recorded in step 59 of the procedure Verify the status of the node before the upgrade on page 977.

display Lp/0 Oamenet/0 standbyStatus

51 Compare the information about the IP accessibility of the first MDM server from the Multiservice Switch 15000/Media Gateway 15000 node with the information recorded in step 60 of the procedure Verify the status of the node before the upgrade on page 977.

list ac ipaccess/*

52 Compare the information about the IP accessibility of the first MDM server from the Multiservice Switch 15000/Media Gateway 15000 node with the information recorded in step 61 of the procedure Verify the status of the node before the upgrade on page 977.

ping -trace -ip(<MDM1 IP>) Vr/0 Ip Icmp

53 Compare the information about the IP accessibility of the second MDM server from the Multiservice Switch 15000/Media Gateway 15000 node with the information recorded in step 62 of the procedure Verify the status of the node before the upgrade on page 977.

ping -trace -ip(<MDM2 IP>) Vr/0 Ip Icmp

If you have inhibited the ppautopatch file from running, remove the noppautopatchrun file on all MDM servers configured for auto-patching on the MSS/MG15000 node as follows:

Login as root.

Remove the file.

```
rm
/opt/MagellanNMS/cfg/private/noppautopatchrun
```

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 Perform HSM using Command Console on page 1006.

HSM (MDM SISM tool) activation

Perform the HSM by setting the application version list, setting the patchlist, and activating the provisioning changes. When the activation completes, the node will be running the new software.

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.

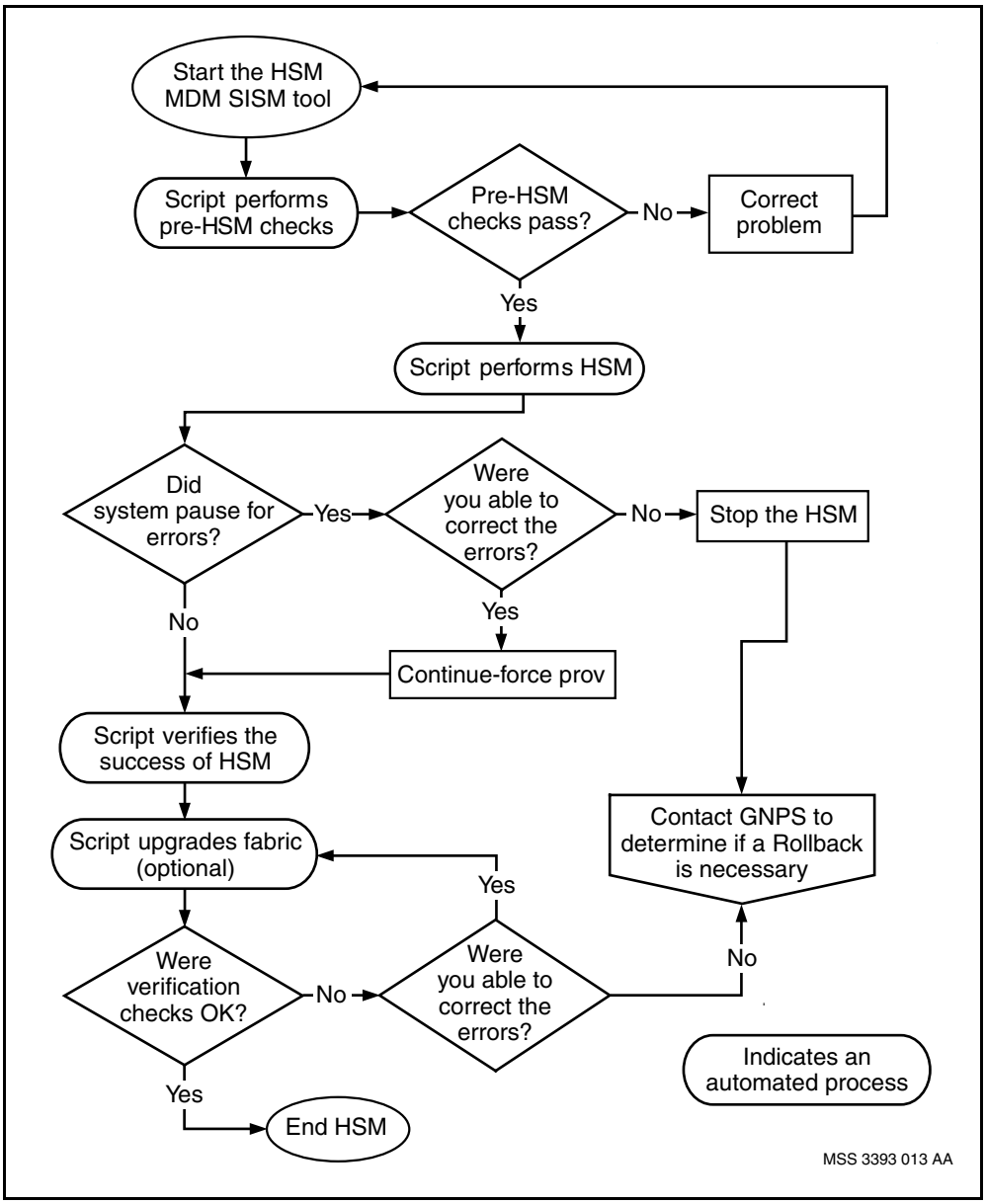
Prerequisites

- Refer to Prerequisites section in the HSM (Command Console) pre-work on page 975.
- For in-band OAM topologies, upgrade all MSS 15000/MG15000/20000 nodes in the network in the following sequence:
  - upgrade all the remote nodes first
  - upgrade the non-preferred Gateway node next
  - upgrade the preferred Gateway node last

HSM task flow

The task flow shows you the sequence of tasks you need to perform to execute the HSM.

HSM task flow



Work flow navigation

The following aspects of the HSM are automated by the SISM script:

- Start HSM using SISM on page 1042
- Pre-HSM verification checks on page 1049
- HSM activation on page 1049
- Post-HSM verification and Fabric upgrade on page 1052
- HSM script completion and final steps on page 1053

The final portion of the HSM is manually controlled by the operator:

- Stop the HSM using MDM SISM tool on page 1055

Performing HSM using MDM SISM

Perform HSM using a Nortel MDM GUI tool called Succession IP Software Migration (SISM), to upgrade the Nortel Multiservice Switch node.

Prerequisites

- Have the correct software load and patches downloaded to the MDM server.

Start HSM using SISM

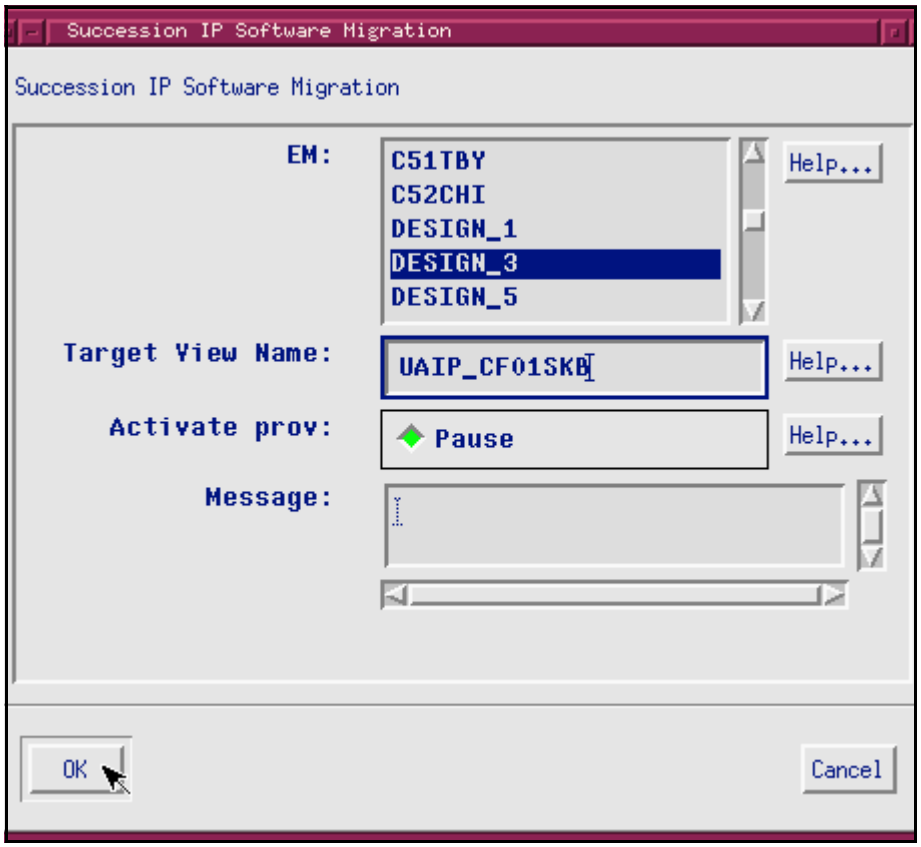
From the MDM window

1 Choose Configuration > MSS > Administration > Succession IP Software Migration.

Alternatively, from the MDM Command Console, type:

$ /opt/MagellanNMS/bin/succession_ipsw_migr

The Succession IP Software Migration window opens.



2 In the EM field, select the name of the node you want to upgrade.

3 In the Target View Name field, enter the new target view name without the view type or version in the name (for example, CF01S1B_April_24).

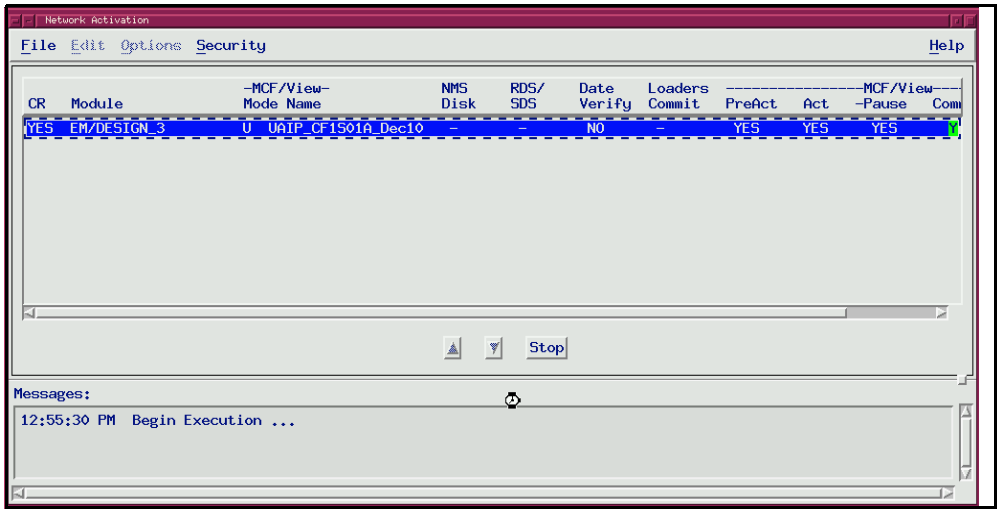
The target view name must be 22 characters or less and be composed of numbers, letters and underscore. Use a consistent naming convention because this name is used when saving the current view and to create the view that will be activated for the software migration.

Pause is the default setting for Activate Prov.

4 Click **OK**.

The Component Information Viewer (CIV) opens.

The Network Activation window opens.



The Network Activation tool launches automatically in Hitless Software Migration mode with the network activation file already loaded. The network activation file contains one network activation record defined specifically for Carrier Voice over IP software migration activation. The record is already selected.

5 From the MDM window, choose Fault > Alarm Display: Log.

The Alarm Display window opens.

6 Ensure the appropriate filters are turned on, including the filter for the target node, and that Format is set to full, then click **Filter**. For more information on how to filter alarms, see “Filtering alarms” in 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

7 From the MDM window, choose Fault > Alarm Display: Active.

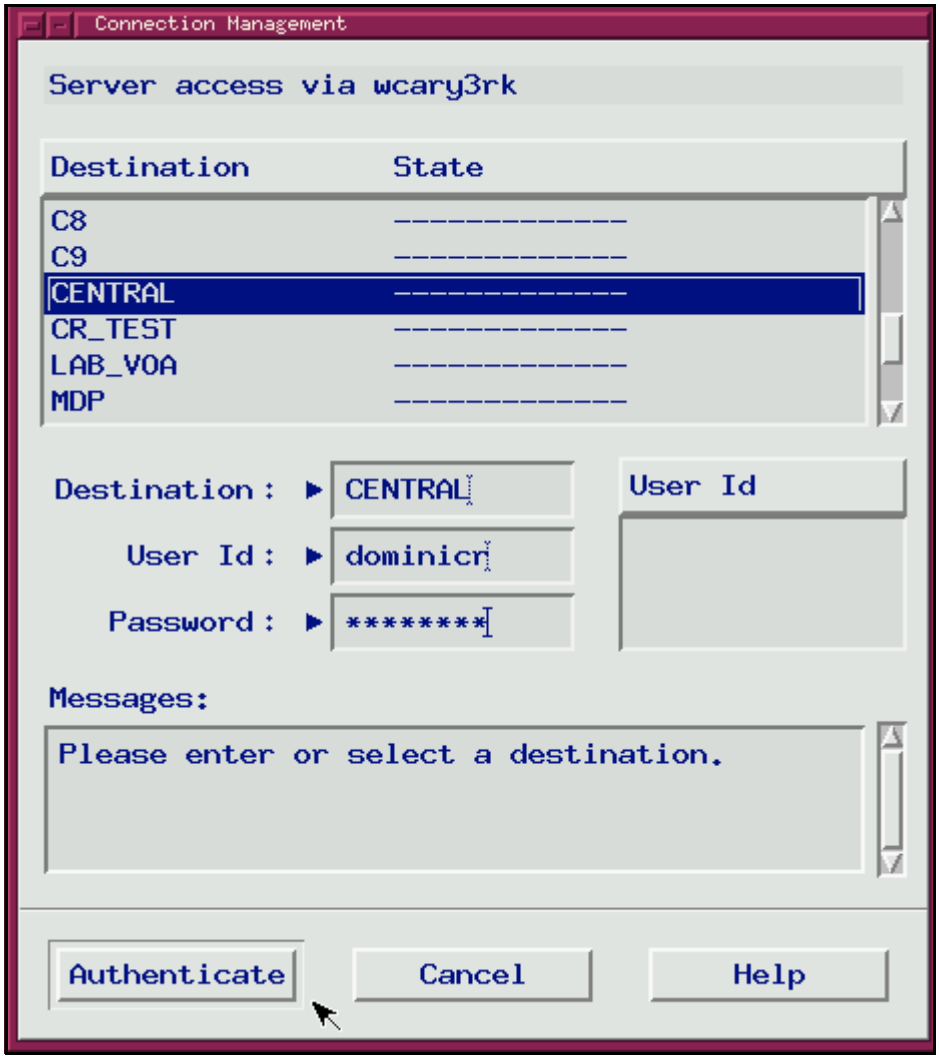
The Alarm Display window opens.

8 Ensure the appropriate filters are turned on, including the filter for the target node, and that Format is set to full, then click **Filter**. For more information on how to filter alarms, see “Filtering alarms” in 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

Note: You should monitor any alarms against the *prov* component (specifically 7000 0033, 7000 0034, and 7000 0035) and the *prov migration* component. You should also monitor 7012 0204 against the *Lp* component. This alarm indicates that the LP cannot achieve its expected migration switchover behaviour.

9 From the Network Activation tool, select **Group Authenticate** from the Security menu.

The Connection Management Dialog opens.



10 Enter or select the node's group name, and enter a valid user ID and password for the group. (Your user ID must have a minimum impact of System Admin and minimum scope of network.)

11 Click **Authenticate**.

Authentication takes place. If authentication is successful, the dialog closes.

Note: If your user ID does not have sufficient permissions to perform the upgrade, you must exit and restart the SISM tool using an ID that has a minimum impact of System Admin and minimum scope of network.

After you authenticate with the group that contains the node to be migrated, you can use the Component Information Viewer to display the attributes of the provisioned components and later

after the migration starts, monitor the progress of the migration. See 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

12 In the Network Activation tool window, ensure the activation record is selected and click **Execute**.

A confirmation dialog opens.

13 Click **OK** to proceed with the activation.

On the Network Activation tool, **Execute** is replaced by a Stop button (grey) which is not available for selection.

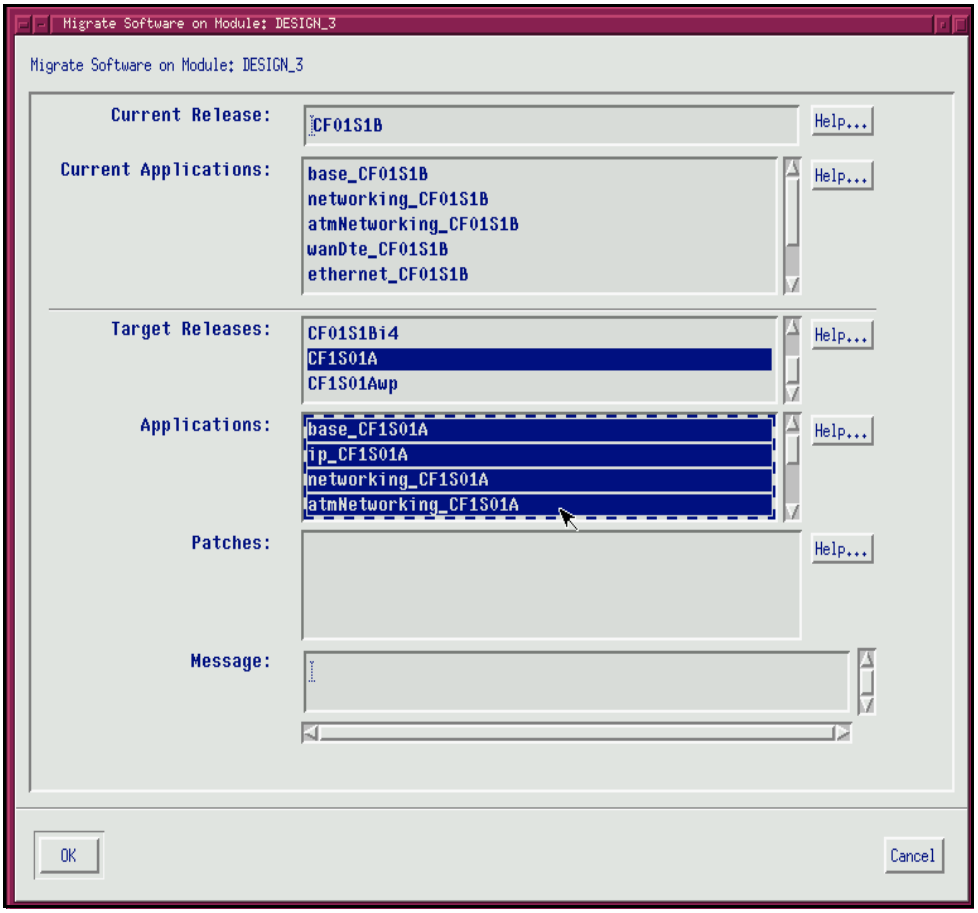
The activation begins.

A pre-check terminal window and a Migrate Software on Module window opens.

Information about the activation is written into the log file: `/opt/MagellanNMS/data/log/nat/nat_<nodename>_<timestamp>.log`.

As each process is performed, the corresponding field in the record turns green. If the action completes successfully, the field turns from green to blue and the next field turns green. If an action fails, the entire record turns red or yellow according to the severity of the error. During this process, **Execute** is replaced by **Stop** that can be used to halt execution.

A window opens displaying the results of the pre-check and post-check commands. If a fault is found, the operator can stop the script (for example, if there is a fault on a component and the the operator wants to fix it), fix the problem and repeat the process until all problems are corrected.


Migrate Software on Module: DESIGN_3
Migrate Software on Module: DESIGN_3
Current Release:
CF01S1B
Help...
Current Applications:
base_CF01S1B
networking_CF01S1B
atmNetworking_CF01S1B
wanDte_CF01S1B
ethernet_CF01S1B
Help...
Target Releases:
CF01S1Bi4
CF1S01A
CF1S01Awp
Help...
Applications:
base_CF1S01A
ip_CF1S01A
networking_CF1S01A
atmNetworking_CF1S01A
Help...
Patches:
Help...
Message:
OK
Cancel

14 In the Migrate on Software on window, select the target release.

The Migrate on Software Module window opens.

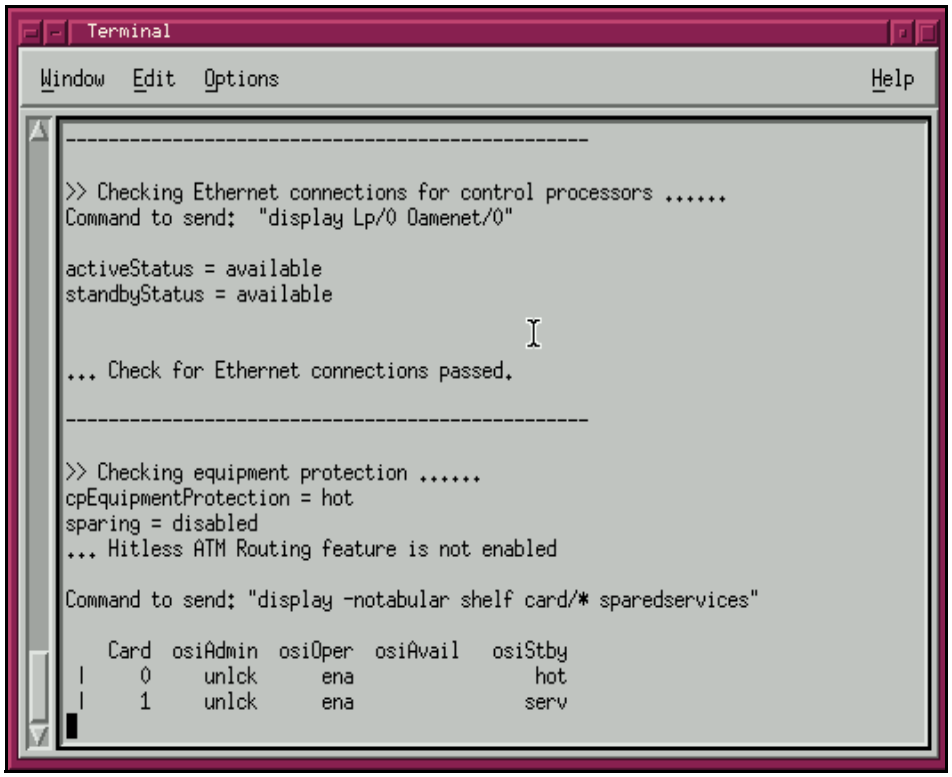
15 In the Migrate on Software Module window, select the destination software version from Target Releases and select applications matching the Current Release applications.

16 Select the required patches from the patch list.

Note: Refer to step 8 in procedure Perform HSM using Command Console on page 1006 for more details on how to apply patches in SN08.

17 If you would like to proceed with the migration, click **OK**.

18 The script progresses to the pre-activation stage and executes pre-HSM verification checks.



Pre-HSM verification checks

1 Monitor the pre-HSM verification.

While the record is executing the pre-HSM portion of the script, information is displayed and you may be prompted to continue with the software migration or to abort the software migration.

Note 1: You should monitor the *prov* component using the Component Information Viewer. While the activation is in progress, you should monitor for alarms from the node using the MDM alarm display. The migration should be stopped if unexpected warnings or alarms appear.

Note 2: The Command Console CLI response format is different from the SISM tool GUI command response format because the SISM format is optimized for automated processing. The information presented is the same.

Error messages can occur for various reasons, for example: if another operator is also provisioning or if there are warnings or errors from the check prov and so forth.

For information on how to handle these error messages, see "Impact of an error condition on a HSM using the SISM tool" in *Upgrading MSS 15000 and MG 15000/20000 in IP Solutions*, NN10419-461.

HSM activation

1 At the completion of the pre-activation portion of the script, you are asked if you want to continue with the software migration. If you would like to proceed, press **Enter**.

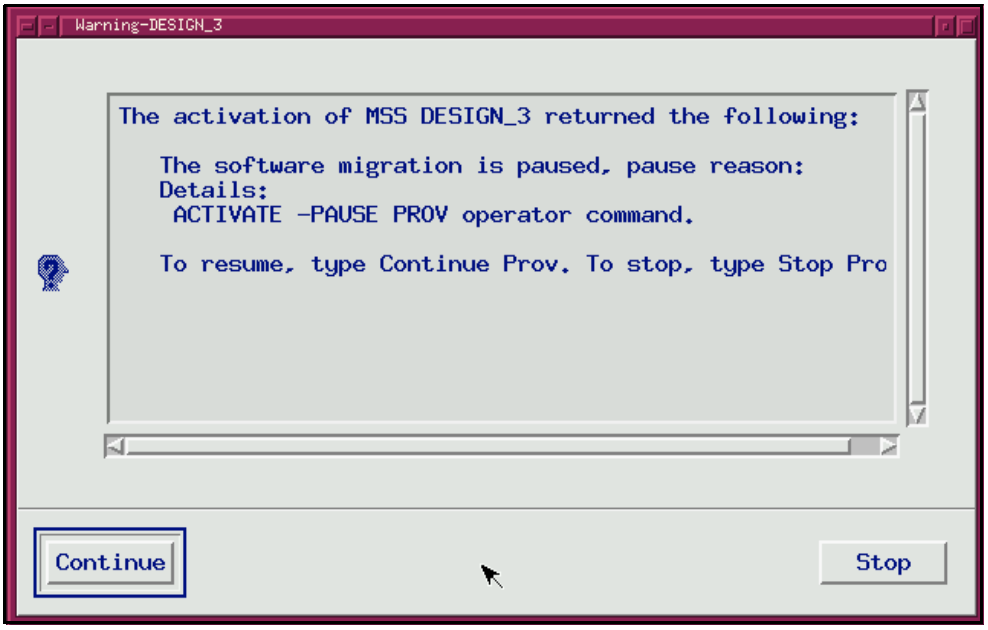
The migration takes place. The number of calls and components that have been provisioned on the node determine how long the activation takes.

Monitor the status of the node and the status of the migration. To monitor the progress of the migration, use the Component Information Viewer to display the attributes of the provisioning component. You can continue to do this until you lose connectivity to the node, which is when the originally active CP begins to load the new software. The MDM server automatically reconnects to the node when possible.

While the activation is in progress, monitor the alarms from the node using the MDM Alarm Display. If unexpected warnings or alarms appear, stop the migration. Refer to What happens to the node during a hitless software migration on page 970 for more information.

2 When the software migration pauses, you are prompted to either stop the migration or continue the migration.

The software migration will pause because the **-pause** option has been chosen or, there is something wrong with the application during the software migration (Phases 1 to 3).



Note: Review the Migration Visible Alarms to determine whether or not you should continue the migration. Click **Continue** or **Stop**.

CAUTION
Contact GNTS before continuing during a migration pause
Contact Nortel Global Networks Technical Support (GNTS) for advice or assistance before continuing if the software migration pauses due to a Migration Visible Alarm.

Note: When you have used the **-pause** option and the system has paused prior to the switchover, and you select **Continue** to continue HSM, the HSM will not pause again to allow you to make the checks outlined above (unless the system finds a fault).

Post-HSM verification and Fabric upgrade

After the HSM activation phase and commit phase are complete, the Network Activation tool starts the post-HSM verification portion script. After the record has executed the post-HSM verification, a fabric card firmware upgrade is performed on each fabric card if required.

Information on the result of the fabric card firmware upgrade and fabric card test is written to the log file. If the first fabric card firmware upgrade does not complete successfully, the second fabric card firmware upgrade is not attempted.

HSM script completion and final steps

When all actions in the record have completed successfully, the entire record turns blue.

1 Double-click on the executed record in the record list to display and review the logged information. Alternatively, you can choose Show Status from the record list pop-up menu.

2 Select **Exit** from the File menu to close the Network Activation Tool.

3 Select **Exit** from the File menu to close the Component Information Viewer tool.

4 If you have configured in-band OAM, use step 49 and step 50 inclusive in Verify the success of HSM on page 1029 to compare the status of the *Atmmpe* components with the information you gathered in steps 31 and step 32 of the procedure Verify the success of HSM on page 1029.

5 If **display -o prov** shows a different version number for the `editViewName` from the `committedFileName`, execute the following comments through the `commandConsole`:.

```
PROV 3> st pr
Prov
ok              2004-06-01 10:36:06.01

PROV 4> load -file(<committedFileName>) pr
Prov
   Loaded or applied file <committedFileName>.
ok              2004-06-04 10:20:47.36

PROV 5> end pr
Prov
ok              2004-06-01 10:36:09.45
```

The following output shows an example of misaligned `editViewName` and `committedFileName`.

```
Prov
   adminState = unlocked
   operationalState = enabled
   usageState       = idle
   provisioningActivity = none
   activityProgress     = n/a
   standbyCpActivity    = none
   standbyCpActivityProgress = n/a
   committedFileName         = CF0124F_April_27.full.001
   currentViewFileName       = CF0124F_April_27.full.001
   lastUsedFileName          = CF0124F_April_27.full.001
   provisioningSession       =
   provisioningUser          =
   checkRequired             = no
   confirmRequired           = no
   editViewName              = CF0124F_April_27.full.001
   editViewAddedComponents   = 0
   editViewDeletedComponents = 0
   editViewChangedComponents = 0
   currentJournal            = 0
   journalDisabledReason     = not disabled
   restorePossible           = no
```

Stop the HSM using MDM SISM tool

At any decision point during the software migration before the activation phase has begun, you can select **Abort** or **Cancel** and the migration will stop. The Network Activation and MDM Component Information Viewer windows can be closed by selecting **File** and then **Exit**.

During the pre-script phase, you can stop the process by entering **<Ctrl> -C** in the pre-script window.

After the software activation has started and before the migration switchover phase starts, you can abort the software migration hitlessly by clicking **STOP** in the Network Activation tool's main window. The Network Activation tool sends a **stop prov** command to the node and all the tool's processes stop. The success of the stop depends on timing. If the node enters the migration switchover phase before processing the **stop prov** command then it is too late to stop the hitless software migration.

If the system detects a problem during the software migration (phases 1-3), the hitless software migration automatically pauses before migration switchover occurs to allow you to review the migration visible alarms before continuing or stopping the migration.

To stop the process after the Migration switchover phase has started, click **Stop** in the Network Activation Tool main window. Further processing stops on the HSM SISM tool (but not on the node).

Close the SISM tool after stopping an HSM.

- Select **Exit** from the File menu to close the NAT.
- Select **Exit** from the File menu to close the Component Information Viewer window.

Issue **start prov; copy prov; end prov** from the Command Console before restarting SISM.

To back out after the migration switchover, follow the steps in "Rollback" (page 131).

CAUTION
Non-hitless process
Stopping the process after the HSM switchover is not a hitless process.

Feature activation

The following MSS 15000/MG15000/20000 features for a UA-IP solution must be activated:

- Recurring fan alarm enhancement if you are upgrading from SN06 to SN08. If your current release is SN07 or SN08, this feature should already be enabled.
- Setting solution release name identification

If the node you are upgrading supports 2 wire Transmit Low Receive High (TLRH) Continuity operational test (COT) and is being upgraded from SN07 to SN08, you must also perform the procedure Activating 2 wire Continuity operational test (COT) on page 1062 because 2 wire TLRH COT was previously supported by a patch application.

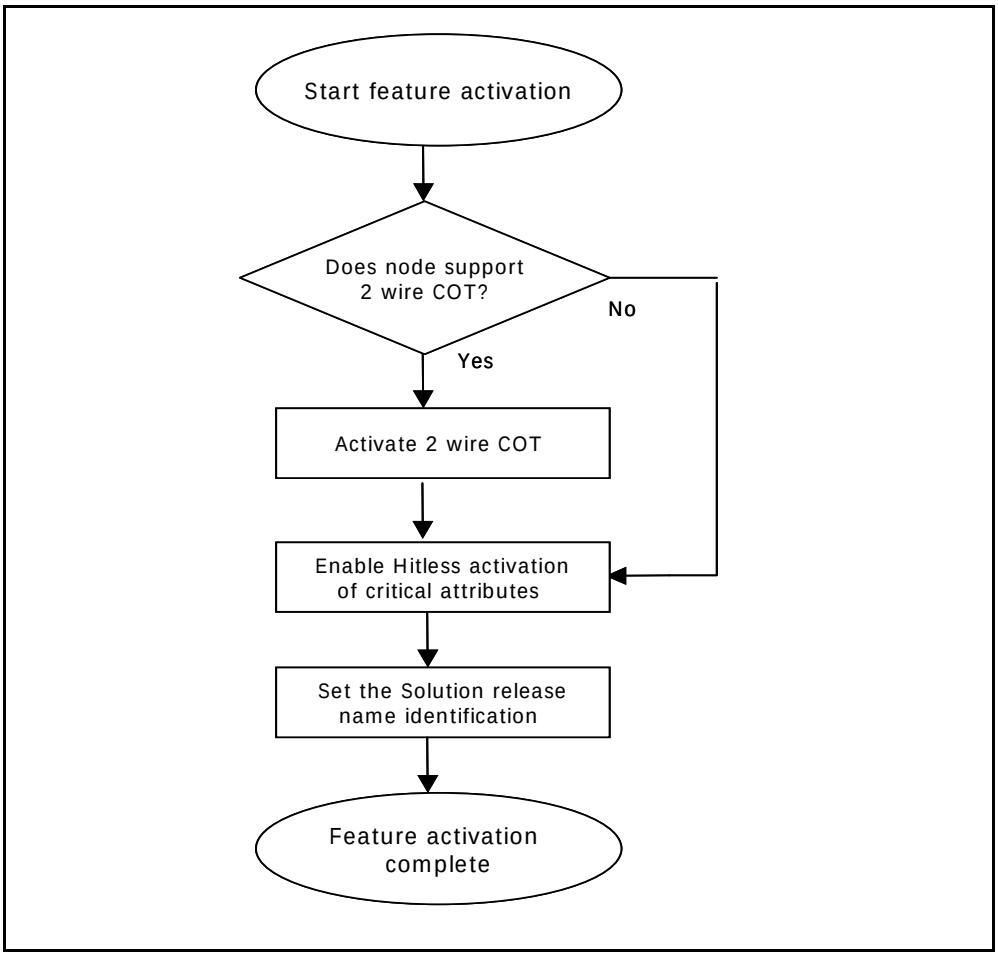
Prerequisites

- Complete the HSM. See HSM (Command Console) activation on page 1004.

Feature activation task flow

The task flow shows you the sequence of tasks you must perform to activate new features in an SN07 to SN08 UA-IP/PT-IP/PT-AAL2/IAC/IAW upgrade for a MSS 15000/MG15000/20000. To link to any procedure, go to the Work flow navigation on page 1057 that follows the flow chart.

Feature activation work flow



Work flow navigation

- Enabling the recurring fan failure alarm enhancement on page 1058
- Setting the solution release name identification on page 1059
- Activating 2 wire Continuity operational test (COT) on page 1062

Enabling the recurring fan failure alarm enhancement

In a Carrier Voice over IP solution, Nortel recommends configuring the recurring fan failure alarm on MSS 15000/MG15000/20000 nodes. If a fan fails, the alarm 7012 0051 is always raised. If the recurring alarm is configured, the alarm is 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.

Prerequisites

- SN08 software must be running on the node.

From the node

1 Login with 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 the section “Troubleshooting a software upgrade” in *Upgrading Multiservice Switch 15000/Media Gateway 15000/20000 in Carrier Voice over IP Networks*, 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

Setting the solution release name identification

The commentText field of the MSS15000/MG 15000/20000 shelf component contains record release and load information that appears in the following order:

- solution release
- patchlevel of Nortel 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

Use the MDM toolset to set the solution (Carrier Voice over IP) release name on the MDM tool launcher and to modify the commentText field of the shelf component. An alternate way to modify the solution release name is to use the **Set Shelf Commenttext** command.

Perform either:

- Setting solution release name using the Set Shelf CommentText command on page 1059 or Setting solution release name using SISM on page 1061

Prerequisites

- upgrade to SN08

Setting solution 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 “SN08” leaving the remainder of the text unchanged. For example:

set Shelf CommentText “SN08, MDM 142-09, IM9095 1.01, IM1662 1.35, IM1661 1.04, Spec 2.0"

Setting solution release name using SISM

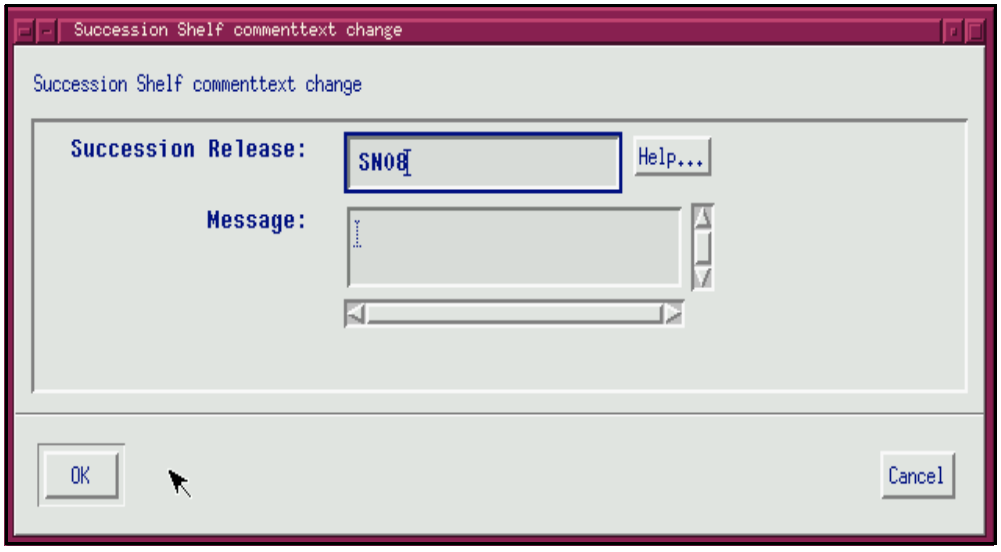
Prerequisites

- The MSS15000 hitless software migration must have been performed using the MDM SISM tool.

Setting solution release name for MSS15000 using SISM

From the MDM server

1 The SISM tool post-activation script prompts you for the new solution (Carrier Voice over IP) release name to display in the MSS15000 Shelf CommentText. Use the format: SNxx.y.



If you click **Cancel**, the update is cancelled before execution and the MSS15000 Shelf *CommentText* remains unchanged.

2 Click **OK**.

A NAT record is created and the NAT window is displayed for a second time since the start of SISM.

This time it activates the service data (the only change is the S*helf CommentText*) with no pre- and post checks.

The *Shelf CommentTex*t attribute on the target node is updated with the solution (Carrier Voice over IP) release name being displayed before the rest of the information in the *Shelf CommentText* field.

Activating 2 wire Continuity operational test (COT)

Activating 2 wire COT

1 Using either the CLI or the MDM Nodal Provisioning tool, set the *continuityTestType* attribute of all the *TProf/15* components on the node to *2WireAnnexB3TLRH*:

start prov

2 Get a list of *nsta* components needing 2 wire COT:

list nsta/* vgs TProf/15

3 Repeat the following for all instances of *nsta* listed:

set nsta/<n> vgs TProf/15 COTtype 2WireAnnexB3TLRH

4 Perform a semantic check:

check prov

5 Activate, confirm, save and commit the change:

activate prov

confirm prov

save prov

commit prov

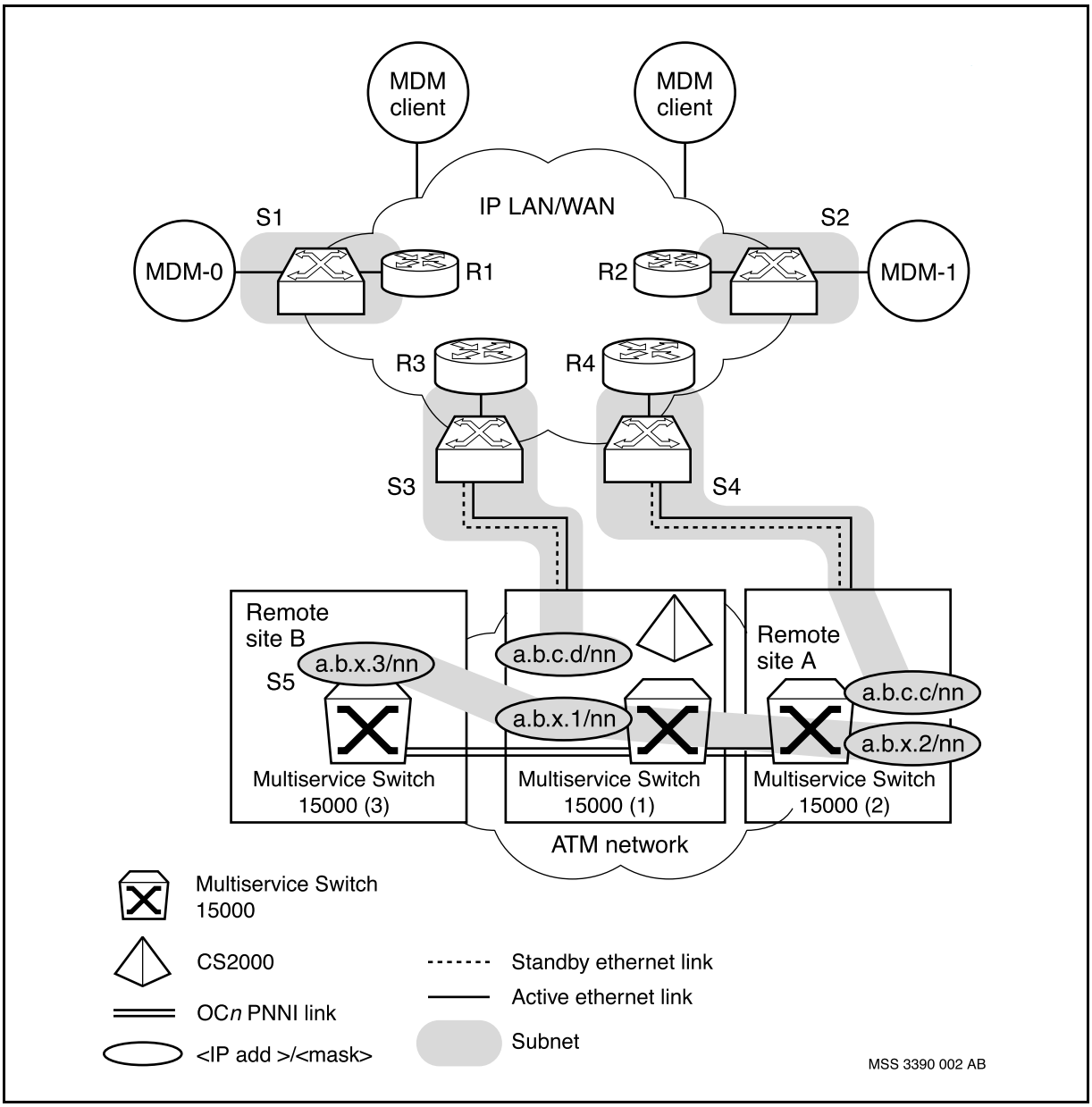
end prov

In-band OAM quick reference

Key relationships

The figure Sample in-band connectivity topology on page 1063 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 Multiservice Data Manager (MDM) servers manage Nortel Multiservice Switch network.

The chosen server is the server that the operator uses as a launching point for MDM applications, such as Command Console.

The alternate server is another MDM server that could be used to perform the same set of tasks, but wasn't chosen.

Multiservice Switch -1

This MSS 15000/MG15000/20000 node is in the Carrier Voice over IP Office and is a Gateway node using out-of-band connectivity.

From the perspective of MDM-0, S3 represents subnet to the preferred MSS 15000/MG15000/20000 node.

Multiservice Switch-2

This MSS 15000/MG15000/20000 node is in a remote office and is a Gateway node using out-of-band connectivity.

From the perspective of MDM-0, S4 represents the subnet to the alternate MSS 15000/MG15000/20000 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 MSS 15000/MG15000/20000 nodes are Remote nodes using in-band connectivity with Multiservice Switch-1.

Peripheral Modules

Before upgrading Peripheral Modules

Perform the required prerequisite upgrade as follows:

Network	Peripheral Modules apply to:	Previous Upgrade
ATM	PT-AAL1 and UA-AAL1	Multiservice Switch (MSS) 15000/20000 on page 820
IP	UA-IP - North America and PT-IP[1]	Multiservice Switch (MSS) 15000/20000 on page 820
	IAC - North America	CS 2000 Management Tools and Clients (CMT) on page 523
Tri-Modal	all applications	Multiservice Switch (MSS) 15000/20000 on page 820

1.Includes IP International: PT-IP

After upgrading Peripheral Modules

Perform the next required upgrade as follows:

Network	Peripheral Modules apply to:	Next Upgrade
ATM	UA-AAL1	Media Gateway (MG) 9000 Manager on page 1103
	PT-AAL1	Enhanced Network and Message Switch on page 1636
IP	UA-IP - North America	Media Gateway (MG) 9000 Manager on page 1103
	PT-IP[1]	Session Server on page 1158
	IAC - North America	SAM21 Shelf Controller on page 1280
Tri-Modal	all applications	one of above based on configuration

1.Includes IP International: PT-IP

About Peripheral modules

Peripheral module upgrades use the PANTHER automated upgrade tool and can consist of the following components:

- Legacy Peripheral Modules:
  - LCM
  - XPM
  - XPMs hosted by MG 9000 ABI cards
  - DMS SPM (PT-AAL1)
  - LPP/FLPP
- IW SPM IP (IAC and PT-IP *plus International PT-AAL2*)
- IW SPM ATM (PT-AAL1 and UA-AAL1)
- MG 4000 (PT-AAL1 and UA-AAL1)
- DPT SPM (PT-AAL1 and UA-AAL1)

CAUTION

For DMS SPM and IW SPM nodes only, the Sync Resource Module (SRM) does not provide sparing therefore offices that use SRM in those nodes must manually upgrade those SRMs prior to using the PANTHER tool. Those SRMs can be located in the SYNCLK table.

Software Delivery methods

The following software delivery methods are available:

- DAT Tape Delivery - XA-Core tape drives
- CD-ROM - Call Agent CD drives
- Electronic Software Delivery

SPM-based node upgrade overview

The upgrade process requires upgrading the node circuit pack software. A separate load exists for each type of circuit pack. Software upgrades require the following sequence:

- SRM
- OC3 (MG 4000 and DMS SPM - North America)
- STM-1 (DMS SPM - International)
- IED or SUP (MG 4000 only - see note)

- DSP or VSP
- DLC (MG 4000 and DMS SPM)
- ATM (MG 4000, IW SPM ATM, and DPT SPM)
- CEM
- GEM (IW SPM IP only)

Note: "IED" is the load name for the Low Speed Access (LSA) circuit pack complex and "SUP" is the load name for the Synchronous Transport Level 1 (STS-1) circuit pack complex.

Circuit packs are grouped into protection groups. An upgrade consists of the following phases:

- Check alarms before starting the upgrade
- Verify the carrier status 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 SPM-based node upgrade consists of two different upgrade methods:

- Automated upgrades
- Manual upgrades

The automated method upgrades several circuit pack types at once. The manual method upgrades circuit pack types individually. This book, "Upgrading a Carrier Voice over IP Network", NN10440-450, describes the automated upgrade procedure. Refer to the corresponding component level document for manual upgrade procedures.

For SPMs and IW SPMs, the Sync Resource Module (SRM) does not provide sparing therefore TDM offices that use SRMs 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 TDM office has two SRMs which can be located in the SYNCLK table.

SRMs configured in MG 4000 nodes use contain sparing and may be upgraded using the Automated Upgrade process.

Upgrade Preparation

Before performing an SPM-based node (referred to as SPM throughout the remainder of this section) 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

Upgrade strategies

Nortel Networks strongly recommends completely loading entire SPMs with a single maintenance release or milestone upgrade. Failure to load all RMs and CEMs in an SPM can result in inadvertently running unsupported mixed load 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 SPMs in one session, plan to upgrade a limited number of SPMs in multiple sessions.

During the upgrade process 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 SPM at the same time.

To upgrade multiple at the same time on the same SPM, open a MAPCI session for each RM type.

To concurrently upgrade multiple SPMs, Nortel Networks recommends upgrading up to two SPMs at the same time. Open a MAPCI session for each RM type on each 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.

Automated Upgrades

An automated upgrade procedure, known as 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.

IPANTHER can concurrently mate load up to 64 RMs across 8 SPMs in the current upgrade set. The calculation for determing 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.

Peripheral Module CD-ROM based installation

For CS 2000 - Compact/Call Agent applications, use this procedure to install SPM and IW SPM IP software that is delivered on CD-ROM.

SITE — At the CS 2000 Management Tools server

1 Insert the disk into the drive.

SITE — At the CS 2000 Management Tools terminal

2 Log into the Core Manager or CBM by typing

`telnet <cbm_ip_address>`

Choose the username of Core0usr or Core1usr and enter the appropriate password.

3 Change the directory to the PMLOADS volume by typing:

`cd /3PC/<sd0x>/<pmloads_volume>`

Example

`[mtc@hostname mtc]$ cd /3PC/sd01/pmloads`

4 Open an FTP session to the CS 2000 Management Tools (CMT) server by typing:

`ftp <cmt_ip_address>`

Log in using *maint* for the hostname and password.

Example

```
[mtc@10.40.44.67 pmloads]$ ftp <cmt_ip_address>
Connected to <cmt_ip_address>.
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 (cd), list (ls) the file size, change the mode to binary (bin), turn the prompt off (prompt), get the files (mget), and end the ftp session by typing the commands as indicated in teh following example:

Example

```
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
byt
226 Transfer complete.
150 Opening data connection for
ENX20CE.img1020 (binary mode) (3913740
byt
226 Transfer complete.
.......
.......
ftp> bye
```

6 At the core0 prompt, type exit to return to the CBM session.

Example

[mtc@hostname mtc]$ exit

7 At the CBM prompt, telnet to the CM session by typing.

telnet cm

When prompted type in the appropriate username and password.

8 Enter the DISKUT level by typing:

DISKUT

9 Import the PMLOADS file by typing

IMPORT sd01 <pmloads_volume>

Example

```
DISKUT:
>IMPORT SD01PMLOADS
Attempting to import 24 files selected on SD01PMLOADS.

Imported ERS20CE.img1020 as ERS20CE.IMAGE1020.
Imported ENX20CE.img1020 as ENX20CE.IMAGE1020.
...
Imported MPF20CE.bin128 as MPF20CE BIN128.
Imported QLI20BT.img1020 as QLI20BTIMAGE 1020

Imported 24 files successfully of 24 attempts on SD01PMLOADS.
```

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.

10 Once the IMPORT has completed quit and logout using the following commands:

quit all
logout

This returns you to the CBM prompt.

11 From the CBM prompt, log into the CMT by typing :

telnet <cmt_ip_address>

Log in using *maint* for the hostname and password.

12 Eject the disk from the drive by typing:

eject cdrom

Software on the CS 2000 Management Tools server unmounts the disk and opens the drive tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session has ended and no users have changed the directory into /cdrom/... directory. Re-enter the eject command.

SITE — At the CS 2000 Management Tools server

13 Remove the disk from the drive.

14 This procedure is complete.

Manually upgrading an SRM

CAUTION

Use this procedure before performing an automated upgrade only if the network contains **DMS SPM**s or **IW SPM**s that require a Sync Resource Module (SRM) software upgrade.

Both nodes with SRMs configured must be upgraded prior to performing an automated upgrade for the remaining nodes. 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
DSP 2  1 A Insv  CEM 1  8 I Insv  --- -  1 - ----  --- -  8 - ----
DSP 4  2 A Insv  ATM 0  9 A Insv  --- -  2 - ----  --- -  9 - ----
DSP 1  3 I Insv  ATM 1 10 I Insv  --- -  3 - ----  --- - 10 - ----
DSP 3  4 A Insv  VSP 2 11 A Insv  --- -  4 - ----  --- - 11 - ----
--- -  5 - ----  VSP 4 12 A Insv  --- -  5 - ----  --- - 12 - ----
SRM 0  6 A ISTb  VSP 1 13 I Insv  --- -  6 - ----  --- - 13 - ----
CEM 0  7 A Insv  VSP 0 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

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 SRM17BU N SPM 23 SRM 0
DEF10S13       20020915 23:33 GEN A SRM17BU N SPM 23 SRM 0
GHI45S13       20020915 23:36 GEN A SRM17BU N SPM 23 SRM 0
TAB51S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
CTC51S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
BUZ80S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
DXH63S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
DXH62S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
JXM65S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
KAA01S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
KRI62S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
LLH11S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
SBF80S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
SBF90S0P      20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
TAV54S0P      20020915 23:10 GEN A SRM17BU 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 is completed.

Prepare Peripheral Modules for an Automated Upgrade

This procedure prepares all of the peripheral modules in an office for an automated upgrade.

Each destination volume must have sufficient free space for the new peripheral module 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
dist_vol	the name of the new Load File Distribution volume
ip_address	the remote FTP volume server IP address for electronic software delivery (ESD)
pm_path	the location of the PM loads files on the FTP server
patch_vol	the name of the Patch Distribution volume
patch_path	the location of the patch files on the FTP server
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.

Before begnning the automated upgrade, ensure that spares are configured for all RMs requiring an upgrade.

Prepare peripheral modules for 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 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 6

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 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
```

7 Access the PMUPGRADE utility by typing

>PMUPGRADE

8 Set confirmation to ON by typing

>SET CONFIRMATION ON

9 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 peripheral module loads for the office. The default carryover setting is OFF.

If the office	Do
requires all peripheral module loads for the office be copied	step 10
does not require all peripheral module loads for the office to be copied	step 11

10 Set carryover to ON by typing

>SET CARRYOVER ON

11 Confirm the Load File Distribution setting is correct. If necessary, change the setting by typing

If using	Do
tape	**>SET LOADDISTRIB dist_vol** *Example* **>SET LOADDISTRIB F02UTAPE**
ESD	**>SET LOADDISTRIB ip_address pm_path** *Example* **>SET LOADDISTRIB 123.123.123.123 /PMLOADS/**

12 Confirm the Load File Destination setting is correct. If necessary, change the setting by typing

>SET LOADDEST dist_vol

Example

>SET LOADDEST F02LPMLOADS

13 Confirm the Patch File Distribution setting is correct. If necessary, change the setting by typing

If using	Do
tape	**>SET PATCHDISTRIB patch_vol** *Example* **>SET PATCHDISTRIB F02LPMLOADS**

If using	Do
ESD	**>SET PATCHDISTRIB ip_address patch_path** *Example* **>SET PATCHDISTRIB 123.123.123.123 /PATCHLOADS/**

14 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 6. 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
```

15 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 7 of this procedure

16 Generate a node report for the office by typing

```
>DISPLAY NODES
```

Result

The PMUPGRADE Node Report is compiled from SPM inventory tables. The nodename information for the MNCKTPAK table is obtained from the MNNODE table.

17 Display the firmware information by typing

```
>DISPLAY FWINFO
```

18 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 17.

19 Start the filecopy 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 peripheral module loads and PRSU files.

20 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 peripheral module load files.

21 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 22
the replacement loadname cannot be found	step 23
Multiple replacements found for EXT file on the distribution volume or multiple replacement loadnames are found Possible one old replacement found on load distribution volume	step 24

If the response indicates	Do
or ready to continue	step 25

22 Stop the automated upgrade by typing

>Q

Contact the next level of support to update the SPMLDVAL table.

23 A response similar to the following example appears if PMUPGRADE cannot locate the replacement loadname.

```
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 loadname. Ensure the loadname is typed accurately Go to step 25
The load is manufacture discontinued	Enter "S" Go to step 25
The load is a filler RM load name, indicating an RM that does not have a load	Enter "S" Go to step 25

24 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 load name appears before the underscore in the load file name. For example, DLC16DE is the load name for the load file DLC16DE_010082A3.

25 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 26
the report is complete and no loads need to be added or removed	step 31

26 Stop the file copy process by typing

```
>N
```

If	Do
one or more loads need to be removed from the report	step 27
one or more loads need to be added to the report	step 28

27 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 28
the report is complete and no loads need to be added or removed	step 29

28 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 27
the report is complete and no loads need to be added or removed	step 29

29 Repeat the file selection phase of the utility by typing

```
>START FILECOPY
```

30 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 26
shows the excluded and/or included load names	step 31

31 Accept the Load Selection Report by typing

```
>Y
```

32 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.

33 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 peripheral module loads and PRSU files.

34

ATTENTION

Perform this step only if any offline peripheral modules 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 peripheral modules

35 Generate a PMUPGRADE load report for the office by typing

```
>DISPLAY LOADS
```

Confirm the selected new loads have been added to the report.

36 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.

37 Display the PM upgrade plan by typing

```
>DISPLAY PLAN
```

The PMUPGRADE Plan Report organizes the peripheral module upgrade by tasks and layers. A task is a set of peripheral modules of the same type at the same site with the same load requirements. A layer is a grouping of tasks.

38 Review the PMUPGRADE report.

- Confirm all peripheral modules 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 peripheral modules 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 upgrade to change the order of tasks.

- Confirm offline peripheral modules that are being installed or commissioned in the office are not included in the plan report. If an offline peripheral module is included in the plan
  - — quit the PMUPGRADE process
  - — update the appropriate peripheral module inventory table. Change the loadname field for that peripheral module to the new loadname from the loadfile selection report.
  - — start this procedure again from step 6

39 Exit the PMUPGRADE utility by typing

```
>QUIT
```

40 Stop the terminal responses from printing by typing

```
>RECORD STOP ONTO printer_name
```

41 Remove the peripheral module load tape from the tape drive.

Check office policy concerning additional copies of peripheral module load and PRSU files. Some offices require additional copies of peripheral module load and PRSU files on a parallel device.

At your desk

42 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 43
does not have the required hardware	Contact your next level of support for more information.

43 You have completed this procedure.

Perform an automated upgrade for peripheral modules

This procedure upgrades all of the peripheral modules in an office.

Use at least two devices with this procedure. Use one device to perform the automated peripheral module upgrade. Use the second device as a trace device to monitor the progress of the automated peripheral module upgrade.

Some offices use a third device during the automated upgrade. Use the third device as a MAP terminal. Post the peripheral modules and monitor peripheral module loading, patching, and service status.

Send the output of each device to a printer for record keeping.

SWUPGRADE PM disables 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 enabled. No action is required when this log is generated.

Variable Abbreviations

Abbreviation	Definition
printer	the printer name
max_no	the UNLIMITED or the maximum number of peripheral modules the system upgrades concurrently
dev_name	the name of the new Patch Distribution volume
spm_no	the ID (number) of the peripheral module
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.

Perform an automated upgrade for peripheral modules

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 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 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 upgrade shift by typing

```
>SET SHIFT STARTED
```

If unspared SRMs	Do
included in the plan	step 6
not included in the plan	step 8

6 A list of SPMs with unspared SRMs appears with the option to stop or continue PMUPGRADE.

Either stop PMUPGRADE and manually upgrade the SRMs before resuming PMUPGRADE or continue PMUPGRADE and upgrade all components in the plan except for the non-spared SRMs.

Note: The recommended choice is to stop PMUPGRADE, manually upgrade the SRMs and then resume the PMUPGRADE plan.

If choosing to	Do
stop PMUPGRADE	Press **Y** go to step 7

If choosing to	Do
continue PMUPGRADE	Press **N** go to step 8

7 PMUPGRADE has stopped. Manually upgrade the SRMs and return to step 5.

8 SWUPGRADE PM checks for the availability of a $XREF patch cross-reference file and processes patch cross-reference information.

9 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.

10 Display HELP for the CONCURRENCY variable by typing

```
>HELP VAR CONCURRENCY
```

11 Determine the maximum number of peripheral modules to upgrade concurrently. Note that a concurrency value set to UNLIMITED can exceed the maintenance window for the 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 12
does not need to be changed	step 14

12 Set the concurrency value by typing

```
>SET CONCURRENCY max_no
```

13 Display the environment variables and confirm the change by typing

```
>DISPLAY VAR ALL
```

14 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.

15 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
```

16 Display alarms on the RMs on the peripheral modules by typing

```
>QUERYPM FLT REASON
```

17 Display and note any alarms on the nodes by typing

```
>LISTALM
```

18 Display and note the carrier statuses on the nodes by typing

```
>MAPCI;MTC;TRKS;CARRIER;POST SPM spm_no  1
```

Example

```
>MAPCI;MTC;TRKS;CARRIER;POST SPM 23 1
```

19 Determine the impact of the current alarm status on the upgrade.

If there are	Do
alarms other than ISTB alarm	step 20
no alarms or all alarms are ISTB alarms	step 21

20 Perform the appropriate alarm clearing procedures. After completing the required procedures, go to step 21.

21 From the SWUPGRADE device, begin the automated upgrade by typing

```
>START
```

22 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 an SPM upgrade.

Steps proceed automatically, however the option exists to manually select a step.

23 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

24 Based on your office requirements, determine if you wish to upgrade or not upgrade (override) the step.

If	Do
not upgrading a step	step 25
upgrading a step	step 27

25 Override the step by typing

>OVERRIDE step_name

26 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** .

27 Ensure that the HELP STEP command has been performed for every step_name.

If all step_names have	Do
not been verified	step 23
been verified	step 28

28 Execute the upgrade process sequentially or out of sequence through one of the following commands:

If executing the upgrade	Do
sequentially	Type **>GO**
out of sequence	To run a step, type **>RUNSTEP step_name** **ATTENTION** Do not choose to RUNSTEP a step_name that was selected for override.

29 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 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.

30 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 upgrade shift	step 32
a node in the step failed	step 31
every node in the step passed and you want to finish the upgrade shift	step 33

Note: Use the QUERYPM FILES command from the MAP display to confirm each node is correctly loaded and in-service.

31 Possible reasons for a node failure are:

- The peripheral module status, or one of its units, changed due to a maintenance problem not related to the automated upgrade.
- The peripheral module 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 28
not determine why the node failed	Contact your next level of support. If the problem is resolved, go to step 28 To continue the upgrade shift, go to step 22 To end the upgrade shift, go to step 32

32 At the ALIGN_RMS prompt, choose to align the RMIDs and PWIDs of all resource RMs in the office by typing

```
>Y
```

If	Do
you want to continue the upgrade shift	step 22
you want to finish the SPM upgrade shift	step 33

33 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.

34 Display the step of the automated upgrade by typing

```
>DISPLAY STEPS
```

If all steps	Do
except UPGRADE_COMPLETE are complete or overridden	step 35
are not complete or overridden and you do not intend to continue[1]	step 38

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.

35 Execute the UPGRADE_COMPLETE step by typing

```
>GO
```

36 Obtain the final record of all completed steps by typing

```
>DISPLAY STEPS
```

37 Complete the UPGRADE_COMPLETE step by typing

```
>GO
```

38 Quit the SWUPGRADE PM utility by typing

```
>QUIT
```

39 Stop the terminal responses from printing by typing

```
>RECORD STOP ONTO printer
```

40 You have completed this procedure.

Post upgrade or downgrade process

Perform procedure Post upgrade or downgrade process on page 1101 after the entire office upgrade or downgrade is completed. The procedure consists of the following tasks:

- Dump an image to disk after completing maintenance shift upgrade or downgrade activities
- Delete the old file names from the PMLOADS table
- Delete the old load and patch files from disk volumes

The Variable Abbreviations table defines the variables used in this procedure.

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.

Media Gateway (MG) 9000 Manager

ATTENTION

Upgrade the SSPFS software before upgrading any application software on the server.

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. If required, refer to procedure "Verifying disk utilization on an SSPFS-based server" in *ATM/IP Security and Administration*, NN10402-600.

Before upgrading the MG 9000 Manager

Perform the required prerequisite upgrade as follows:

Network	MG 9000 Manager applies to:	Previous Upgrade
ATM	UA-AAL1	Peripheral Modules on page 1065
IP	UA-IP[1]	Multiservice Switch (MSS) 15000/20000
Tri-Modal	configuration specific	Peripheral Modules on page 1065

1.Includes IP International: UA-IP

After upgrading the MG 9000 Manager

Perform the next required upgrade as follows:

Network	MG 9000 Manager applies to:	Next Upgrade
ATM	UA-AAL1	SAM21 Shelf Controller on page 1280
IP	UA-IP[1]	SAM21 Shelf Controller on page 1280
Tri-Modal	configuration specific	SAM21 Shelf Controller on page 1280

1.Includes IP International: UA-IP

About the MG 9000 Manager

The MG 9000 Manager provides a network management system for the MG 9000. The MG 9000 Manager enables remote management of multiple MG 9000 network elements through a single graphical user interface (GUI).

Note: The MG 9000 element upgrade occurs after the MG 9000 Manager and Gateway Controller upgrades are completed.

The MG 9000 Manager runs on the SUN Microsystems servers which reside in the Cabinetized Operations Administration and Maintenance (COAM) cabinet. The Sun platform uses the Succession Server Platform foundation software (SSPFS) which is a high-performance, UNIX-based processing platform based on Sun Micro System's Netra line of NEBS compliant servers. The SSPFS platform is used as the platform for OAM&P services.

Upgrading the MG 9000 Manager

This document contains upgrade information and procedures for the MG 9000 Manager.

When to use this document

Use this document to upgrade the MG 9000 Manager from SN06.2 or SN07 to SN08.

When upgrading the MG 9000 Manager from SN06.2 to SN08 or SN07 to SN08, the following activities take place in the following order:

- remove SN06.2 or SN07 software packages
- upgrade the MG 9000 Manager master server and mid-tier software

For a high level MG 9000 Manager upgrade summary, refer to either the MG 9000 Manager SN06.2 or SN07 to SN08 upgrade checklist (one-server) on page 1112 or the MG 9000 Manager SN06.2 or SN07 to SN08 upgrade checklist (two-server) on page 1113, depending on the appropriate upgrade path. These checklists reference detailed procedures that are provided later in the document.

Refer to *Upgrading the MG 9000*, NN10048-461 for the following related procedures:

- downgrading the MG 9000 Manager software
- upgrading the MG 9000 Manager software to a maintenance release (MR)

Upgrade strategy

The following high-level strategy summarizes network upgrade procedures required when upgrading the MG 9000 Manager:

1. Upgrade the Communication Server 2000 (CS2000) Management Tools software to ensure node and line provisioning applications are updated (CS 2000 Management Tools and Clients (CMT) on page 523).
2. Remove the existing SN06.2 or SN07 software packages. Perform this activity just prior to upgrading the Succession Server Platform Foundation Software (SSPFS). SN06.2 or SN07 SSPFS software does not operate with SN08 SSPFS software.

3. Upgrade the SSPFS software (Upgrading SSPFS software on page 666). This includes the SSPFS on the MG 9000 Manager master and mid-tier servers.

   Note: The CS2000 Management Tools and the SSPFS platform software must be upgraded to SN08 before upgrading the MG 9000 Manager server and mid-tier software (step 4).

4. Upgrade the MG 9000 Manager software in the following order:
   - server
   - mid-tier

Service impacts

The following are the service impacts to consider when proceeding with the upgrade:

- After starting the SN08 MG 9000 Manager, the SN07 MG 9000 Manager reverts to a backed up instance if run against the same tablespace. The SN07 server shuts down if the SN07 MG 9000 Manager attempts to start up against a database schema that has been upgraded by the SN08 MG 9000 Manager. If this occurs, the following error message appears:

  ```
  The application is trying to start up against a
  database schema of a later release than the
  application. This is not supported. The database
  of the earlier release must be restored - or the
  application must be taken up to the later release.

  Application Version: >7.0< Database Schema
  Version: >8.0<
  ```

- When upgrading the MG 9000 Manager from an earlier release to SN08, earlier releases cannot run in tandem with the SN08 MG 9000 Manager. In addition, the SN08 MG 9000 Manager software is not compatible with earlier SSPFS platform versions. The software release versions of the MG 9000 Manager and the SSPFS platform cannot be mixed.
- Warnings for all components and services impacted during upgrade
  - — No data provisioning can be performed during upgrades. During the upgrade of a given network element (NE), the MG 9000 Manager blocks any attempt to change data for that NE. The MG

9000 Manager displays a minor warning indicating provisioning is halted and the database is unavailable for that NE.

— When the SN07 MG 9000 EM is upgraded to SN08, PM collection cannot be performed during the time between stopping the pre-SN08 OM Collector and when the MG 9000 Manager server starts.

When the SN06.2 MG 9000 EM is upgraded to SN08, PM collection cannot be performed during the time between stopping the pre-SN08 OM Collector and when OM collection is enabled for the NE on the SN08 EM.

— Call processing should not be impacted during the MG 9000 Manager upgrade.

— 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.

- Recommendations for limiting service impact: none

Tools and utilities

The MG 9000 Manager software supports software upgrades and downgrades. For MG 9000 Manager software downgrade procedures, refer to *Upgrading the MG 9000*, NN10048-461.

The MG 9000 Manager supports patching through the network patch manager (NPM). Patching procedures and information are located in Carrier Voice over IP Network patching on page 1850.

MG 9000 Manager client system requirements

The following table provides recommended minimum configurations for the MG 9000 Manager client.

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 • Pentium III 1 GHz or higher • display resolution of 1280 x 1024 with 256 colors • 256 MB RAM • 200 MB hard drive space • 10BaseT/100BaseT Ethernet network connection • Java Web Start (JWS) 1.4.2_05 and higher If the Windows PC supports more network client applications than just the MG 9000 Manager client application, the following minimum configuration is required: • Windows 2000 (SP2 or later), or Windows XP • Pentium III 2.5 GHz or higher • display resolution of 1280 x 1024 with 256 colors • 1 Ghz RAM • 30 Gb hard drive space • 10BaseT/100BaseT Ethernet network connection • Java Runtime Environment (JRE) 1.4.2_05 and higher • 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) 1.4.2_05 • Ultra 5 400 MHz or higher • display resolution of 1280 x 1024 with 256 colors • 256 MB RAM • 200 MB hard drive space • 10BaseT/100BaseT Ethernet network connection

MG 9000 Manager client minimum configurations

Client platform	Configuration
Windows or Solaris client	Third party software • Netscape 6.0 and higher or Internet Explorer 5.5, 6.0 and higher • Java Web Start (JWS) 1.4.2_05 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). Some operating systems contain SSH clients. Any missing SSH clients must be obtained separately. Sources for SSH clients include, but are not limited to, the following: • PUTTY - freeware • OpenSSH - freeware • SSH Inc. - commercial • Secure CRT - commercial • WinSCP - freeware Nortel does not supply or recommend a particular supplier.	

Pre-upgrade requirements

Ensure the CS 2000 Manager has been upgraded to SN08 before upgrading any MG 9000 NEs to SN08.

The MG 9000 Manager must be upgraded to SN08 before upgrading MG 9000 NE cards to SN08. This means the MG 9000 Manager is capable of managing an MG 9000 NE operating at SN06.2, SN07 or, SN08.

Note: All alarms on the MG 9000 Manager and MG 9000 NE must be cleared prior to proceeding with the SN06.2 or SN07 to SN08 upgrade process.

Do not provision any new data to the NEs during upgrade activities.

Entry criteria

The following information and tools are required during the software upgrade:

- 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 Manager software must be at SN06.2 or SN07 with all patches applied and enabled
- tools required: database browser (optional)

Upgrade interdependencies

The following interdependencies are required during the upgrade process:

- SSPFS on MG 9000 Manager master and mid-tier servers must be upgraded to SN08 (Upgrading SSPFS software on page 666).
- CS 2000 Management Tools must be upgraded to SN08 prior to upgrading the MG 9000 Manager to SN08.
- 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 points to the CS 2000 Management Tools machine where NPM is running. If it is not configured correctly, reconfigure accordingly. Refer to Upgrading SSPFS software on page 666 for more information.

- if this is an SN06.2 or SN07 to SN08 Sun Netra cluster (two-server) upgrade, run a getpatch to retrieve all SN08 patches before the upgrade starts. Refer to Transferring patches delivered on CD to the NPM database on page 1884 for more information.

Exit criteria

The following are the criteria for exiting from the SN06.2 or SN07 to SN08 upgrade process:

- The upgrade was successful after the MG 9000 Manager mid-tier server and server applications are running in SN08
- Additional exit criteria is determined later in the upgrade process, after upgrading the MG 9000 network element. Refer to MG 9000 NE Exit criteria on page 1446.

Applying software fixes

When it is necessary to apply software fixes, the following methods are available:

- Maintenance Release upgrade process: refer to procedure “Upgrading the MG 9000 Manager software to a maintenance release” in *Upgrading the MG 9000*, NN10048-461.
- Patching

— refer to Carrier Voice over IP Network patching on page 1850 for more information.

MG 9000 Manager upgrade checklists

SN06.2 or SN07 to SN08 t1400/N240 one-server (simplex) upgrade checklist

Use the following table as a checklist for upgrading the MG 9000 Manager from SN06.2 or SN07 to SN08 in a t1400/N240 single-server (simplex) configuration. Enter a check mark (√) in the √column as each step or procedure is completed.

MG 9000 Manager SN06.2 or SN07 to SN08 upgrade checklist (one-server)

	Activity	Procedure	√
1	Upgrade the MG 9000 Manager to SN08.	1. The following steps are part of the procedure Upgrading MG 9000 Manager software from SN06.2 or SN07 to SN08 on page 1123. Refer to that procedure and those referenced in the following steps to complete the MG 9000 Manager upgrade.	
	Note: This is a safe stopping point		
2	Update the version of the software registered in IEMS for the MG 9000 Manager.	Edit the object properties in the IEMS for the MG 9000 Manager you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the Device Version field: • Editing and viewing object properties using Java Web Client on page 1841 • Editing and viewing object properties using Web Client on page 1846	
3	Before proceeding, ensure the GWC has been upgraded.	Refer to "*Upgrading the GWC*, NN10196-461", then return to step 4 of this checklist.	
4	Enable OM collection for NEs in SN08.	As each NE is upgraded, OM collection for that NE must be enabled. To enable OM collection, use the following procedure: Enabling OM collection for NEs when upgrading from SN06.2 to SN08 on page 1152, then return to this checklist. ***Note:*** If you do not wish to collect OMs, you can omit this procedure.	
5	This procedure is complete.		

SN06.2 or SN07 to SN08 N240 two-server (cluster) upgrade checklist

Use the following table as a checklist for upgrading the MG 9000 Manager from SN06.2 or SN07 to SN08 in a two-server (cluster) configuration. Enter a check mark (√) in the √ column as each step or procedure is completed.

MG 9000 Manager SN06.2 or SN07 to SN08 upgrade checklist (two-server)

	Activity	Procedure	√
On the Inactive node			
1	Upgrade the MG 9000 Manager to SN08.	1. Perform the following steps to complete the MG 9000 Manager upgrade. a. Telnet to the inactive node of the specific machine to be upgraded by typing **`> telnet <server ip address>`** b. Login as root c. To verify you are on the inactive node, type **`> bash`** d. To verify all applications have stopped, type **`> servquery -status all`** e. To verify if the node in the cluster is active or standby unit, type **`> ubmstat`** If the system response is ClusterIndicatorSTBY, proceed to the next step. If the response is other than ClusterIndicatorSTBY, refer to Verifying the state of a cluster on page 629. f. To verify the unit is in standby and is in a normal state **`> udstat`** If the system response is STANDBY normal UP clean, proceed to the next step. If the response contains “nodaemon”, “offline”, “down’, or “not mounted”, refer to Verifying the state of a cluster on page 629. g. Perform procedure Upgrading MG 9000 Manager software from SN06.2 or SN07 to SN08 on page 1123.	
	Note: This is a safe stopping point		

MG 9000 Manager SN06.2 or SN07 to SN08 upgrade checklist (two-server)

	Activity	Procedure	√
2	Update the version of the software registered in IEMS for the MG 9000 Manager.	Edit the object properties in the IEMS for the MG 9000 Manager you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the Device Version field: • Editing and viewing object properties using Java Web Client on page 1841 • Editing and viewing object properties using Web Client on page 1846	
3	Before proceeding, ensure the GWC has been upgraded.	Refer to "*Upgrading the GWC*, NN10196-461", then return to this procedure.	
4	Enable OM collection for NEs in SN08.	As each NE is upgraded, OM collection for that NE must be enabled. To enable OM collection, use the following procedure: Enabling OM collection for NEs when upgrading from SN06.2 to SN08 on page 1152, then return to this checklist. ***Note:*** If you do not wish to collect OMs, you can omit this procedure.	
5	This procedure is complete.		

Retrieving MG 9000 Manager software using Electronic Software Delivery

Purpose of this procedure

These procedures describe how to transfer MG 9000 Manager software loads from Nortel Networks to a customer drop box using the Electronic Software Delivery (ESD) method, and how to make the transferred loads available for installation on the MG 9000 Manager.

When to use this procedure

Use this procedure after receiving electronic notification for MG 9000 Manager software loads.

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

Retrieving MG 9000 Manager software using Electronic Software Delivery

At the MG 9000 Manager server requiring software loads

1 Become the root user by typing

Note: If this is an N240 cluster (two-server) configuration, perform the following step in the inactive node.

```
# su - root
```

2 Make a temporary directory to store the ESD software by typing

```
# mkdir /data/iso_esd
```

and pressing the Enter key.

3 Change directory by typing

```
# cd /data/iso_esd
```

and pressing the Enter key.

4 Get the MG 9000 Manager ISO image file into the newly created directory of the MG 9000 Manager server by performing the following steps

a Use FTP to get the ISO file by typing

```
# ftp x.x.x.x
```

where
x.x.x.x is the IP address of the MG 9000 Manager master server

b Change directory to the iso files location.

c Select the file transfer protocol type by typing

```
# binary
```

d Get the MG 9000 Manager iso image file by typing

```
# get mg9kem_8_<version_number>.iso
```

where
version_number is the version number of the iso file, such as 501

e Quit the FTP activity by typing

```
# quit
```

5 Verify that the file exists on the MG 9000 Manager server in the newly created directory by performing the following

a Change to the iso_esd directory by typing

```
# cd /data/iso_esd
```

b List the contents of the directory containing files with .iso extension by typing

```
# ls -l *.iso
```

An example system response

```
-rw-r--r-- 1 root other 47945728 Jan 11 15:39
mg9kem_8_501.iso
```

6 Mount the image by performing the following

a Enter the command line interface by typing

```
# cli
```

The system responds with the following

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

select -
```

b Select option 3.

The system responds with the following

```
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 Select option 4

The system responds with the following

```
=== Executing "mount_image"
Enter Full Path To ISO Image:
```

d Enter the full path to the ISO image by typing

 # /mg9kem_8_<version_number>.iso

Example
/mg9kem_8_501.iso

The system responds with the following

```
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

=== "mount_image" completed successfully
```

A response is printed to the terminal. Use following table to determine if the command was successful.

cli 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 image by entering **ls -l /*.iso**
`ISO Image Already Mounted`	Perform step 8 to unmount the image.

cli command responses

Response	Meaning and action
`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/.`

e To exit each menu level, type

 # x

7 Access the MG 9000 Manager packages and copy them to a permanent location.

a List the contents of the tmpmnt directory by typing

 # ls -l /tmpmnt

The system responds with the following

```
total 93520
-r--r--r-- 1 root root 25888256 Dec 9 12:42
NTMG9KM_8_501_0.PKG
-r--r--r-- 1 root root 21303808 Dec 9 12:42
NTMG9KS_8_501_0.PKG
-r--r--r-- 1 root root 690176 Dec 9 12:42
NTOMCLTR_8_501_0.PKG
```

b Copy the packages in tmpmnt directory to a permanent location by typing

 # cp /tmpmnt/*.PKG /opt/nortel/

c Verify the package files are on directory /opt/nortel by typing

 # cd /opt/nortel

List the contents of all files with .PKG suffix by typing

 # ls -l *PKG

8 Unmount the MG 9000 Manager ISO image by performing the following

a Enter the command line interface by typing

```
# cli
```

The system responds with the following

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

select -
```

b Select option 3.

The system responds with the following

```
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 Select option 5.

The system responds with the following

```
=== Executing "umount_image"
=== "umount_image" completed successfully
```

d To exit each menu level, type

```
# x
```

e Verify the MG 9000 Manager packages no longer exist in the tmpmnt directory by changing to the /tmpmnt directory and listing the contents

```
# cd /tmpmnt
# ls -l
```

The system responds with the following

```
total 0
```

f Change to the root directory by typing

```
# cd /
```

g List the contents of the directory containing files with a .iso extension by typing

```
# ls -l *.iso
```

h Remove the EM ISO file by typing

```
# rm /mg9kem_8_<version_number>.iso
```

Example
rm /mg9kem_8_501.iso

9 This procedure is complete.

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 SN06.2 or SN07 to SN08 on page 1123.

The following procedures are included in this section:

- Upgrading MG 9000 Manager software from SN06.2 or SN07 to SN08
- Enabling OM collection for NEs
- 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

If software is delivered to the customer using Electronic Software Delivery (ESD), ensure the MG 9000 Manager loads are available by performing procedure Retrieving MG 9000 Manager software using Electronic Software Delivery on page 1115.

Action

Upgrading MG 9000 Manager software from SN06.2 or SN07 to SN08

At the MG 9000 Manager

1 Collect current configuration data for the SN06.2 or SN07 master server by performing the following steps:

Note: If this is an N240 cluster (two-server) configuration, perform the following steps in the Active node.

a Login as root.

b To determine the RELEASE_NUMBER used in the next step, change directory by typing

```
cd /opt/nortel/
```

and list the contents by typing

```
ls -l
```

c To display current configuration data, type

```
> /opt/nortel/mg9ksrv_0<RELEASE_NUMBER>/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 CS2M 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 Imaging Server settings
8) Change EM Factory Sleep
9) Display current settings
10) Exit from Main Menu
```

d Enter 8 for SN06.2 or 9 for SN07 to display current settings.

The system responds with the following example output:

```
 CURRENT SETTINGS
Package Name                        :NTmg9ks07
Version                           :NTMG9KS_7_31_0
Server Mode                         :MASTER
Master Server IP Address            :47.142.89.69
CS2M IP Address                     :47.142.89.70
Oracle IP Address                   :47.142.89.70
Security Authentication Host        :47.142.89.69
Image Server                      :172.17.40.250
Image Server User ID                :root
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
ESA data download time              :1:30 AM
ESA data device name                :/SFDEV
ESA data file name             :ESA_SYSTEM_SD$XML
```

e Record the configuration data manually using pencil and paper or copy the information to a file for access later using a text editor.

f Exit the tool by entering 9 for SN06.2 or 10 for SN07.

g Copy the hidden SN06.2 or SN07 configuration data file to the persistdata directory as an SN08 file by typing

`> cp /data/mg9kem/persistdata/.NTmg9ksxx.cfg /data/mg9kem/persistdata/.NTmg9ks08.cfg`

where

xx in.NTmg9ksxx.cfg is 62 for SN06.2 or 07 for SN07

Note: If this is an N240 cluster (two-server) configuration, the copy will be done on the Active node. The copy cannot be performed on the Inactive node.

h Change directory by typing

`cd /data/mg9kem/persistdata/`

i Check the files to ensure they copied correctly by typing

`ls -al`

2 Collect the current configuration data for the SN06.2 or SN07 mid-tier server by performing the following step:

Note: If this is an N240 cluster (two-server) configuration, perform the following steps in the Active node.

a Login as root.

b To determine the RELEASE_NUMBER used in the next step, change directory by typing

`cd /opt/nortel/`

and list the contents by typing

`ls -l`

c To display current configuration data, type

`# /opt/nortel/mg9kmtr_0<RELEASE_NUMBER>/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) Change Debug Level for logs
3) Display current settings
4) Exit from Main Menu
```

d Select 4 for SN06.2 or 3 for SN07 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
Security Type              :PAM Security
Authentication Host          :106.40.34.135
```

e Record the configuration data manually using pencil and paper or copy the information to a file for access later using a text editor.

f Exit the tool by entering 5 for SN06.2 or 4 for SN07.

g Copy the hidden SN06.2 or SN07 configuration data file to the persistdata directory as an SN08 file by typing

```
> cp /data/mg9kem/persistdata/.NTmg9kmxx.cfg
/data/mg9kem/persistdata/.NTmg9km08.cfg
```

where

xx in.NTmg9kmxx.cfg is 62 for SN06.2 or 07 for SN07

Note: If this is an N240 cluster (two-server) configuration, the copy will be done on the Active node. The copy cannot be performed on the Inactive node.

h Change directory by typing

```
cd /data/mg9kem/persistdata/
```

i Check the files to ensure they copied correctly by typing

```
ls -al
```

3 Use the information in the following table to determine the next step.

If the MG 9000 Manager is being upgraded from	Do
SN06.2	step 4
SN07	step 5

4 Record the current configuration data for the SN06.2 or SN07 mid-tier server by performing the following step:

Note: If this is an N240 cluster (two-server) configuration, perform the following steps in the Active node.

a Login as root.

b To display current configuration data, type

```
> /opt/nortel/omcltr_06/bin/OMCollector
config
```

The system responds with the following output:

```
Starting OM Configuration Tool ...

*****************************************
*     Welcome to the Nortel Networks    *
*                                       *
*     OM Collection Configuration Tool  *
*                                       *
*****************************************

Please pick one of the following options:
```

```
[C]reate a new device collection list
[A]dd device(s) to the collection list
[R]emove device(s) from the collection list
[D]isplay the existing collection list
[S]how this menu again
[P]assword configuration
[H]elp menu
e[X]it
```

c Select option D.

The system responds with the following output:

```
// ***** Device list for OM collection *****
// FILE CREATION TIME = Thu May 22 10:12:15
EDT 2003
// IPAddress <mandatory>, DeviceName
<mandatory>, Status <optional>
*****************************************
 47.142.107.33,CO19,inband
 47.142.80.80,CO9,outOfBand
*** end of file:
/data/OMCollector/config/gwlist.cfg ***
```

d Record the configuration data manually using pencil and paper or copy the information to a text editor file for access later in this procedure.

5 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 7
a t1400/N240 simplex (one-server) configuration	step 6

6 Stop the SN06.2 or SN07 MG 9000 client applications since an earlier version cannot operate with an SN08 MG 9000 Manager.

To stop the client application on a PC or UNIX workstation, close the SN06.2 or SN07 Subnet View.

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	step 8
a t1400/N240 simplex (one-server) configuration	step 10

8 To remove a server from a cluster, perform procedure Removing a server from a cluster on page 684.

9 On the inactive node, run the pkgrm script to uninstall the SN06.2 or SN07 server and mid-tier application packages.

Note: Once the packages have been removed, it will not be possible to downgrade without re-importing a saved data image.

Perform the following steps:

a Login as root.

b To verify the MG 9000 mid-tier and server applications are stopped, type

```
> servquery -status all
```

c To remove the master server SN06.2 or SN07 software, type

```
> pkgrm NTmg9ks<release_number>
```

where
release_number is 62 for SN06.2, or 07 for SN07

To continue, respond to the two prompts with Y for SN06.2, or Yes for SN07.

d To remove the mid-tier server SN06.2 or SN07 software, type

```
> pkgrm NTmg9km<release_number>
```

where
release_number is 62 for SN06.2, or 07 for SN07

To continue, respond to the two prompts with Y for SN06.2, or Yes for SN07.

e To remove the OM collector SN06.2 or SN07 software, type

```
> pkgrm NTomclt<release_number>
```

where
release_number is 62 for SN06.2, or 07 for SN07

To continue, respond to the two prompts with Y for SN06.2, or Yes for SN07.

Go to step 16.

10 Login as root.

11 Stop the SN06.2 or SN07 mid-tier server application by typing

```
> servstop MG9KMIDTIER_0<release_number>
```

where
release_number is 6_2 for SN06.2, or 7 for SN07

12 Stop the OM Collector by typing

```
> servstop MG9KOMC_0<release_number>
```

where
release_number is 6_2 for SN06.2, or 7 for SN07

13 Stop the SN06.2 or SN07 server application

```
> servstop MG9KSERVER_0<release_number>
```

where
release_number is 6_2 for SN06.2, or 7 for SN07

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.

14 To verify the MG 9000 mid-tier and server applications have stopped, type

```
> servquery -status all
```

15 Run the pkgrm script on each server (master server and mid-tier server) to stop the SN06.2 or SN07 server application and uninstall the server application. The OM Collector software is located on the mid-tier server.

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.

Perform the following steps:

a To remove the master server SN06.2 or SN07 software, type

```
> pkgrm NTmg9ks<release_number>
```

where
release_number is 62 for SN06.2, or 07 for SN07

To continue, respond to the two prompts with Y for SN06.2, or type Yes and respond to the prompt with Y for SN07.

b To remove the mid-tier server SN06.2 or SN07 software, type

```
> pkgrm NTmg9km<release_number>
```

where
release_number is 62 for SN06.2, or 07 for SN07

To continue, respond to the prompt with Y for SN06.2, or type Yes and respond to the prompt with Y for SN07.

c To remove the OM collector SN06.2 or SN07 software from the mid-tier server, type

```
> pkgrm NTomclt<release_number>
```

where
release_number is 62 for SN06.2, or 07 for SN07

To continue, respond to the two prompts with Y for SN06.2, or type Yes and respond to the prompt with Y for SN07.

16 Upgrade both the mid-tier server and the master server to the SN08 SSPFS platform.

Note 1: If this is an N240 cluster configuration, upgrade the SSPFS on the inactive side.

Note 2: Ensure the master server is restarted before mid-tier server.

Note 3: 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 on page 666

17 Install any patches for SSPFS using the NPM by performing procedure Applying patches using the NPM on page 1895.

Note: If this is an N240 cluster configuration, install the patches using the NPM on the inactive side.

Upgrading the master server software

18 Install the SN08 master server application by performing the following steps:

a Login as root (superuser).

Note: If this is an N240 cluster (two-server) configuration, perform this step on the inactive node.

b Use the following table to determine the next step.

If installing the master server software from	Do
CD-ROM	step c
electronic software delivery (ESD)	step f

c 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.

d 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_8_31_0.PKG
NTMG9KM_8_31_0.PKG
```

e At the prompt (#), use pkgadd to install the server portion (NTmg9ks08.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_8_31_0.PKG

The system responds with the following:

```
The following packages are available:
```

```
 1 NTmg9ks08  Succession MG 9000 Manager
Server
        (sparc) 8.44

Select package (s) you wish to process (or
'all' to process all packages). (default:
all) [?,??,q]:
```

Go to step g.

f At the prompt (#), use pkgadd to install the server portion (NTmg9ks08.pkg) of the software from ESD by typing

Note 1: If this is an N240 cluster configuration, install the software on the inactive side.

Note 2: For information on retrieving software from ESD, refer to procedure Retrieving MG 9000 Manager software using Electronic Software Delivery on page 1115.

`# pkgadd -d /opt/nortel/<mgemserver_package>.pkg`

where <mgemserver package> is the MG 9000 Manager server package name, for example NTMG9KS_8_31_0.PKG

```
The following packages are available:
1 NTmg9ks08 Succession MG 9000 Manager Server
            (sparc) NTMG9KS_08_44_0
Select package(s) you wish to process (or
'all' to process all packages).
(default: all) [?,??,q]:1
```

g Enter "1" and press return to begin the server installation process.

The system responds with the following:

```
Processing package instance <NTmg9ks08> from
</NTmg9ks08.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 <NTmg9ks08> [y,n,?]
```

h To continue, respond to the two prompts with Y.

Note: Verify that the “Installation of <NTmg9ks08> was successful.” If there are any errors please contact your next level of support.

i If applicable, eject the CD-ROM by typing

```
# eject cdrom0
```

j Obtain the IP address or hostname of the current master server by typing

```
# hostname
```

k The steps for installing software in the master server is complete.

Configuring the master server software

19 Configure the MG 9000 Manager master server by performing the following steps:

a To configure the master server, type

Note: If this is an N240 cluster (two-server) configuration, perform this step on the inactive node.

```
> /opt/nortel/mg9ksrv_08/bin/mg9kconfig.sh
```

The system responds with the following:

```
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.220
Image Server : 47.xxx.xx.8
Image Server User ID : maint
SuperCore Gige Image Directory : /swd/mg9k
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
OM Collector CSV Directory : /swd/mg9k
*****************************************
Is the above information correct?Press the
enter key to accept the default (y/n)?Default
: [n] => n
```

b 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.

c 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>

d 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
Midtier server for authentication?
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.

e 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.

f 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 overwrite privileges. Communication to the server is verified.

g Enter the User ID and password to the Image server. This must have overwrite 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
```

h 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:
SCG: Press the enter key to accept the default
?
Default: [/swd/mg9k] =>
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] =>
ITX: 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] =>
Enter the directory where CSV files will be
generated:
OMC DownloadDir: Press the enter key to
accept the default ?
Default: [/data/oms/1] =>
```

i 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.220
Image Server : 47.xxx.xx.8
Image Server User ID : maint
SuperCore Gige Image Directory : /swd/mg9k
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
OM Collector CSV Directory : /swd/mg9k
*****************************************
Is the above information correct?
Press the enter key to accept the default
(y/n)?
Default : [n] => y
```

j Verify that the DB Host IP address is correct. Perform the following steps:

i Change the directory by typing

cd /opt/nortel/mg9ksrv_08/bin

ii Enter the following command:

./mg9kserver config

The system responds with

```
Main Configuration Menu

1) Change Distribution Policy
2) Change CS2M 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 Imaging Server settings
8) Change EM Factory Sleep
9) Change OMC settings
10) Display current settings
```

```
11) Exit from Main Menu
Please make a selection =>
```

iii Enter 10 to display current setting.

The system responds with the following:

```
        CURRENT SETTINGS
Package Name             :NTmg9ks08
Version                  :NTMG9KS_8_031_0
Server Mode              :MASTER
Master Server IP Address :47.142.92.98
CS2M IP Address          :47.142.92.66
Oracle IP Address        :47.142.92.66
Security Authentication Host :47.142.92.98
Image Server             :47.142.92.26
Image Server User ID     :root
SuperCore Gige Image Directory :/swd/mg9k
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
OM Collector CSV Directory :/data/oms/1
ESA data download time   :1:30 AM
ESA data device name     :/SFDEV
ESA data file name
       :ESA_SYSTEM_SD$XML
```

iv Enter 11 to exit from the Configuration menu.

v Log out by typing

exit

vi Login as root.

vii Verify that the Oracle IP address is correct.

viii 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, and also matches the CS 2000 Management Tools IP address.

k The next step is determined by the information in the following table.

If the DB Host IP address is	Do
correct	Step n
not correct	Step l

l To change the DB Host IP address, perform the following steps:

i 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=>
```

ii 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":
```

iii To change the Oracle server, type

```
> Yes
```

iv 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.
```

m The MG 9000 mid-tier GUI banner now displays the CM_CLLI. This needs to be configured by performing the following steps while logged into the MG 9000 master server. Once this is complete, log into the MG 9000 mid-tier and perform the same steps. If the MG 9000 master server and mid-tier reside on the same IP, you only need to perform this once.

i Log in as root by typing

```
$ su - root
```

The system responds with the following:

```
Password:
<enter the root password>
```

ii Access the command line interface by typing

```
# cli
```

The system responds with the following:

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

 X - exit
```

iii Enter 2 to access the Configuration menu.

The system responds with the following:

```
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
```

iv Enter 4 to access the OAMP Application Configuration menu.

The system responds with the following:

```
OAMP Application Configuration
 1 - sdm_conf (Configure SDM IP Address)
 2 - sdm_unconf (Unconfigure SDM IP
Address)
 3 - sdmuser_conf (Configure SDM User)
 4 - sdmuser_unconf (Unconfigure SDM User)
 5 - cmClli_rediscovery  (Re-discovery the
CM CLLI by SDM IP )
 6 - cmClli_conf (Configure CM_CLLI
Address)
 7 - cmClli_unconf (Unconfigure CM_CLLI IP
Address)
 8 - cm_conf (Configure CM IP Address)
 9 - cm_unconf (Unconfigure CM IP Address)

 X - exit
```

v Enter 6 to configure the CM CLLI address.

The system responds with the following:

```
=== Executing "cmClli_conf"
Enter CM_CLLI:  <site CM_CLLI>
CM CLLI :          <site CM_CLLI>
```

vi Enter "ok" to accept current settings.

ok

```
Processing values....

CM_CLLI Configured
Please perform a logout and login so your
shell will reflect CLLI environment
settings

=== "cmClli_conf" completed successfully
```

vii Quit this shell and login again to inherit the new settings.

n For additional help on available options, execute the following command.

 # /opt/nortel/mg9ksrv_08/bin/mg9kserver help

20 Use the information in the following table to determine the next step.

If the MG 9000 Manager is being upgraded from	Do
SN06.2	step 22
SN07	step 21

21 If the MG 9000 Manager is being upgraded from SN07, make a backup of the SN07 tablespace by typing

```
> opt/nortel/mg9ksrv_08/bin/mgems_ora_ts_backup.sh <ip_address>
```

where

ip_address is the IP address of the database machine

Note: The tablespace data will be written to /data/mg9kem/persistdata/tsBackup.

22 Use the following table to determine the next step.

If the server being upgraded is	Do
an N240 cluster configuration	step 24
an N240 one-server or t1400 configuration	step 23

23 Start the SN08 master server application by typing

```
> servstart MG9KSERVER_08
```

Note: Messages may appear indicating that a "<file_name>_patch failed to stay up." These messages can be ignored.

Upgrading the mid-tier server software

24 Install the SN08 mid-tier server application by performing the following steps:

a Login as root (superuser).

Note: If this is an N240 cluster (two-server) configuration, perform this step on the inactive node.

b Use the following table to determine the next step.

If installing the mid-tier server software from	Do
CD-ROM	step c
electronic software delivery (ESD)	step e

c 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.

d 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_8_xx_0.pkg
```

where

xx is the build number.

The system responds with the following information.

```
The following packages are available:
1 NTmg9km08 Succession MG 9000 Manager
Midtier Server
                    (sparc) 8.44
Select package(s) you wish to process (or
'all' to process all packages). (default:
all) [?,??,q]:
```

Go to step f.

e At the prompt (#) use pkgadd to install the mid-tier portion (NTmg9km08.pkg) of the software from ESD by typing

Note 1: If this is an N240 cluster configuration, install the software on the inactive side.

Note 2: For information on retrieving software from ESD, refer to procedure Retrieving MG 9000 Manager software using Electronic Software Delivery on page 1115.

```
# pkgadd -d /opt/nortel/NTMGKM_8_xx_0.pkg

The following packages are available:
1 NTmg9km08 Succession MG 9000 Manager
            Midtier Server
            (sparc) NTMG9KM_8_44_0
Select package(s) you wish to process (or
'all' to process all packages).
(default: all) [?,??,q]:1
```

f 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 <NTmg9km08> [y,n,?]
```

 # Y

Note: Verify that “Installation of <NTMG9KM_8_xx_0> was successful.” If there are any errors please contact your next level of support.

g The installation continues automatically and installs all the mid-tier server files in /opt/nortel/mg9kmtr_08 subdirectory as noted in the system response.

```
Installing Succession MG 9000 Manager Midtier
Server as <NTmg9km08>

## Installing part 1 of 1.
.
.
.
Configuring system, please wait ...

Installation of <NTmg9km08> was successful.
```

After the installation is compete, a message appears reporting that the installation was successful.

Configuring the mid-tier server software

25 Configure the MG 9000 Manager mid-tier server by performing the following steps:

a To configure the mid-tier server, type

Note: If this is an N240 cluster (two-server) configuration, perform this step on the inactive node.

```
# /opt/nortel/mg9kmtr_08/bin/mg9kconfig.sh
```

b Enter the IP address or hostname of the master server obtained in step j of step 18.

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.

c 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] =>
```

d Enter Y and continue.

```
Configuring system, please wait ...
Set JNLP softlinks for NTmg9km08...

Configuration complete ...
```

26 Use the following table to determine the next step.

If the server being upgraded is	Do
an N240 cluster configuration	step 28
an N240 one-server or t1400 configuration	step 27

27 Start the SN08 mid-tier server application by typing

```
> servstart MG9KMIDTIER_08
```

Note: Messages may appear indicating that a "<file_name>_patch failed to stay up." These messages can be ignored.

28 Apply any MG 9000 Manager software patches.

29 Use the following table to determine the next step.

If the server being upgraded is	Do
an N240 cluster configuration	step 30
an N240 one-server or t1400 configuration	step 33

30 Patch the inactive node of the cluster by performing the procedure Patching the inactive node of a cluster during an upgrade on page 737

31 Stop the SN06.2 or SN07 MG 9000 client applications since earlier version cannot operate with an SN08 MG 9000 Manager.

To stop the client application on a PC, close the SN06.2 or SN07 Subnet View.

To stop the client application on a workstation, kill the Unix process for the MG 9000 Manager. Refer to "Killing a UNIX process on the MG 9000 Manager" in *MG 9000 Fault Management*, NN10074-911 for more information.

32 Telnet to the cluster IP address, login to the active unit and perform a failover of the system by performing the following steps to stop a cluster:

a Log in to the active node through the console (port A) using the root user ID and password

b To return a server to the cluster, perform procedure Returning a server to a cluster on page 744.

c To stop the cluster perform procedure Stopping a cluster on page 749.

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 server to Active state.

33 Install the SN08 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 1155 or Installing the MG 9000 Manager Windows PC client software on page 1153 procedure.

34 Use the information in the following table to determine the next step.

If a userid with appropriate permissions	Do
needs to be provisioned	step 35
does not need to be provisioned	step 37

35 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 Security and Administration,* NN10162-611 for details.

36 To enter the password for this userid, type

```
>passwd [userid]
```

Note: The password must be entered twice.

37 Verify the health of the master and mid-tier servers by typing

```
> servquery -status all
```

38 Start any SN08 3rd party application(s), especially those using the OSS alarm interface.

39 Launch SN08 GUI client software, which for an N240 cluster configuration is from the active node.

During the upgrade process, when the user clicks on the SN08 link in the Application Launch Point, the SN08 application launches. At that point, the user must login. This allows the user into the SN08 application.

40 Use the information in the following table to determine the next step.

If the MG 9000 Manager is being upgraded from	Do
SN06.2	step 41
SN07	step 44

41 Verify all NEs are in the Subnet. Use the information in the following table to determine the next step.

If	Do
an NE is missing	step 43
an NE is not discovered	steps 42 and 43
all NEs are discovered	step 44

Note: After upgrades from SN06 to SN06.2 or SN06.2 to SN07, NEs previously included in the Audit Schedule no longer appear. Manual intervention is needed to add the NEs back into the audit schedule, if they were included prior to the upgrade. Note the status of the Audit Schedule for each of the NEs prior to the upgrade, and set each accordingly after the upgrade. The settings for each of the NEs can be noted by going to the Configuration pull down menu at the Subnet view, then selecting Audit NE. Select the Add button in the Audit window. In the next window, select each of the NEs and note the Audit Properties. These settings will be used to add each NE into the Audit Schedule after the upgrade. The NEs audit settings are ported over to the new load starting in SN08, and no manual action is required. For additional info, refer to *Auditing MG 9000 Provisioning Data,* NN10096-511.

42 Delete the NE from the MG 9000 Manager Subnet View.

43 From the server command line, type

```
/opt/nortel/mg9ksrv_08/bin/bin/mg9kimpl
dataconv62 NE:<number>
```

44 Use the following table to determine the next step.

If the server being upgraded is	Do
an N240 cluster configuration	step 45
an N240 one-server or t1400 configuration	step 49

45 Perform the following steps to confirm the upgrade on a cluster:

At the active node console

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

b Use the following table to determine your next step:

If	Do
you choose to accept the upgraded environment	step c only
you choose to rollback to the state prior to the upgrade	step d

c Accept the upgraded environment by typing

```
# /SSPFS_Upgrade.accept
```

and pressing the Enter key.

d Rollback to the state prior to the upgrade by typing

```
# /SSPFS_Upgrade.fallback
```

and pressing the Enter key.

The node is now restored as it was before the upgrade.

46 To verify the node is the active unit, type

```
> ubmstat
```

47 To check the health of the unit, type

```
> servquery -status all
```

48 Perform the procedure Cloning the image of one node in a cluster to the other node on page 766.

49 This procedure is complete.

If this is a simplex upgrade, return to step 3 on page 1112 of the MG 9000 Manager SN06.2 or SN07 to SN08 upgrade checklist (one-server) and continue with the SN06.2 or SN07 to SN08 upgrade process.

If this is a two-server upgrade, return to step 3 on page 1114 of the MG 9000 Manager SN06.2 or SN07 to SN08 upgrade checklist (two-server) and continue with the SN06.2 or SN07 to SN08 upgrade process.

Enabling OM collection for NEs

Use the following procedure to enable OM collection for NEs when upgrading the MG 9000 EM from SN06.2 to SN08.

Beginning in SN08, OMs are collected in the base server, not the mid-tier server. Depending on your network configuration, you may need to reconfigure the (nothbound) interfaces which read the CSV file generated by the MG 9000 EM OM collector.

Note 1: If you do not wish to collect OMs, you can omit this procedure.

Note 2: This procedure in not required when upgrading from SN07 to SN08.

For general information about OM collection, refer to *MG 9000 Performance Management*, NN10140-711.

Enabling OM collection for NEs when upgrading from SN06.2 to SN08

At the Windows PC client

1 Refer to Step 4 on page 1126 in “Upgrading MG 9000 Manager software from SN06.2 or SN07 to SN08”. Use the information you recorded to perform the following steps for each of the NEs.

2 From the menu bar of the Subnet View select Configuration->View/Modify NE Properties->MG 9000 Provisioning View.

3 in the MG 9000 Provisioning View, manually enable OM Collection for the NE by clicking the OMCollection checkbox.

4 This procedure is complete.

If this is a simplex upgrade, return to Step 4 on page 1112 of the MG 9000 Manager SN06.2 or SN07 to SN08 upgrade checklist (one-server) and continue with the SN06.2 or SN07 to SN08 upgrade process.

If this is a two-server upgrade, return to step 4 on page 1114 of the MG 9000 Manager SN06.2 or SN07 to SN08 upgrade checklist (two-server) and continue with the SN06.2 or SN07 to SN08 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://<SN08 MG9KEM Midtier Server IP or hostname>. Click on Application Launcher.

The Application Launch Point window appears. Click on the" MG9000 Element Manager [SN08]" 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 To verify the version of Java Web Start being executed, perform the following steps:

a Access the Java Web Start Application Manager by selecting Start->Programs->Java Web Start. The Java Web Start Application Manager appears.

b From the JWS Application Manager, select Help->About Java Web Start.

c If the version is not 1.4.2_05, reinstall from the Client Software Installation page as noted in the following step.

3 Use the following figure and the information in the following table to determine the next step.

If Java Web Start (JWS) version 1.4.2_05 software	Do
is already installed in the client machine	step 9
is not installed in the client machine, as evidenced by the preceding message	step 4

4 Select the link “Java™ Web Start Install Guide” to visit “Client Software Installation” page.

5 Visit “Java 2 Runtime Environment Install Guide” under “Microsoft Windows” section for online documentation.

6 Visit “Java 2 Runtime Environment Software Download” under “Microsoft Windows” section to download Java Runtime Environment.

7 Save j2re-1_4_2_05-windows-i586-i.exe and execute the JRE software.

8 Follow the instructions in JRE software to install JRE 1.4.2_05

9 The PC client is setup to launch MG 9000 Manager SN08 client applications.

10 Remove JWS cache by performing procedure Removing an MG 9000 Manager JWS application from cache on page 1157.

11 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://<SN08 MG9KEM Midtier Server IP or hostname>. Click on Application Launcher

The Application Launch Point window appears with a link for SN08. Click on the “MG9000 Element Manager [SN08]” link. Enter the username and password in the login when prompted.

2 To verify the version of Java Web Start being executed, perform the following steps:

a To change directory to where the Java Web Start application is installed, type

```
> cd <path/javaws>
```

b To launch the Java WebStart application manager, type

```
> javaws &
```

c From the JWS Application Manager, select Help->About Java Web Start. The application version is displayed.

d If the version is not 1.4.2_05, reinstall from the Client Software Installation page as noted in the following step.

3 Use the following figure and the information in the following table to determine the next step.

If Java Web Start (JWS) version 1.4.2_05 software	Do
is already installed in the client machine	step 15
is not installed in the client machine, as evidenced by the preceding message	step 4

4 Select the link “Java™ Web Start Install Guide” to visit “Client Software Installation” page.

5 Visit “Java 2 Runtime Environment Install Guide” under “Sun Solaris” section for online documentation.

6 Visit “Java 2 Runtime Environment Software Download” under “Sun Solaris” section to download Java Runtime Environment.

7 Save j2re-1_4_2_05-solaris-sparc.sh to your home directory.

8 Change execute permissions

```
$ chmod +x j2re-1_4_2_05-solaris-sparc.sh
```

9 Execute JRE, this will create a JRE subdirectory called j2re1.4.2_05 in your home directory. Remember the path of this directory as you will need this path later when configuring JWS.

```
$ ./ j2re-1_4_2_05-solaris-sparc.sh
```

10 Follow the instructions in JRE software to install JRE 1.4.2_05

11 In your j2re1.4.2_05 subdirectory there is a zip file called javaws-1_4_2_05-solaris-sparc-i.zip. Copy this zip file to your home directory.

12 Install JWS by unzipping the zip file and executing “install.sh”.

```
$ unzip ./javaws-1_4_2_05-solaris-sparc-i.zip
```

```
$ ./install.sh
```

13 Accept the license agreement and enter the path to JRE from step 9.

14 Follow the remaining online directions.

15 The Sun Solaris client is now setup to launch MG9KEM SN08 client applications.

16 Remove JWS cache by performing procedure Accessing JWS application on a Sun workstation on page 1157.

17 Exit the browser and launch the browser again for settings to take effect.

18 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.

Session Server

Before upgrading the Session Server

Perform the required prerequisite upgrade as follows:

Network	Session Server applies to:	Previous Upgrade
ATM	not applicable	not applicable
IP	PT-IP[1]	Peripheral Modules on page 1065
Tri-Modal	configuration specific	Peripheral Modules on page 1065

1.Includes IP International: PT-IP.

After upgrading the Session Server

Perform the next required upgrade as follows:

Network	Session Server applies to:	Next Upgrade
ATM	not applicable	not applicable
IP	PT-IP[1]	SAM21 Shelf Controller on page 1280
Tri-Modal	configuration specific	SAM21 Shelf Controller on page 1280

1.Includes IP International: PT-IP.

About the Session Server

The Session Server is a call media and signaling interoperability component deployed as two redundant hardware units housed in the SAM-F frame only and used in PT-IP solutions. The primary application introduced on the Session Server platform is the SIP Gateway application which facilitates interoperability between the CS 2000 network and 3rd party SIP-based Call Servers and Media Application Servers.

Upgrading from a previous major release - SN07 to SN08

This section describes how to perform an in-service major release upgrade of the Session Server units. It also describes how to perform a rollback of a partial or complete major release upgrade in cases where a major release fails or causes problems with the system.

Major release upgrade strategy

A major release upgrade impacts both the Session Server NCGL platform and the SIP Gateway application.

- A Session Server NCGL platform software release consists of release notes, CS 2000 NCGL Platform Manager software, NCGL software and optional CS 2000 NCGL Platform Manager patches.

  Using the CS 2000 NCGL Platform Manager GUI you can select an image to upgrade to. You can upgrade the Session Server load from the local DVD-ROM drive, from an ISO image located on a remote system, or from a local file on the Session Server disk drive. Space is available on the local hard drive to maintain approximately 2 loads in case fallback to a previous load is necessary. Partial and complete rollbacks of a failed upgrade can be performed.

- A Session Server SIP Gateway application software release consists of release notes, CS 2000 NCGL Platform Manager software, and SIP Gateway application software.

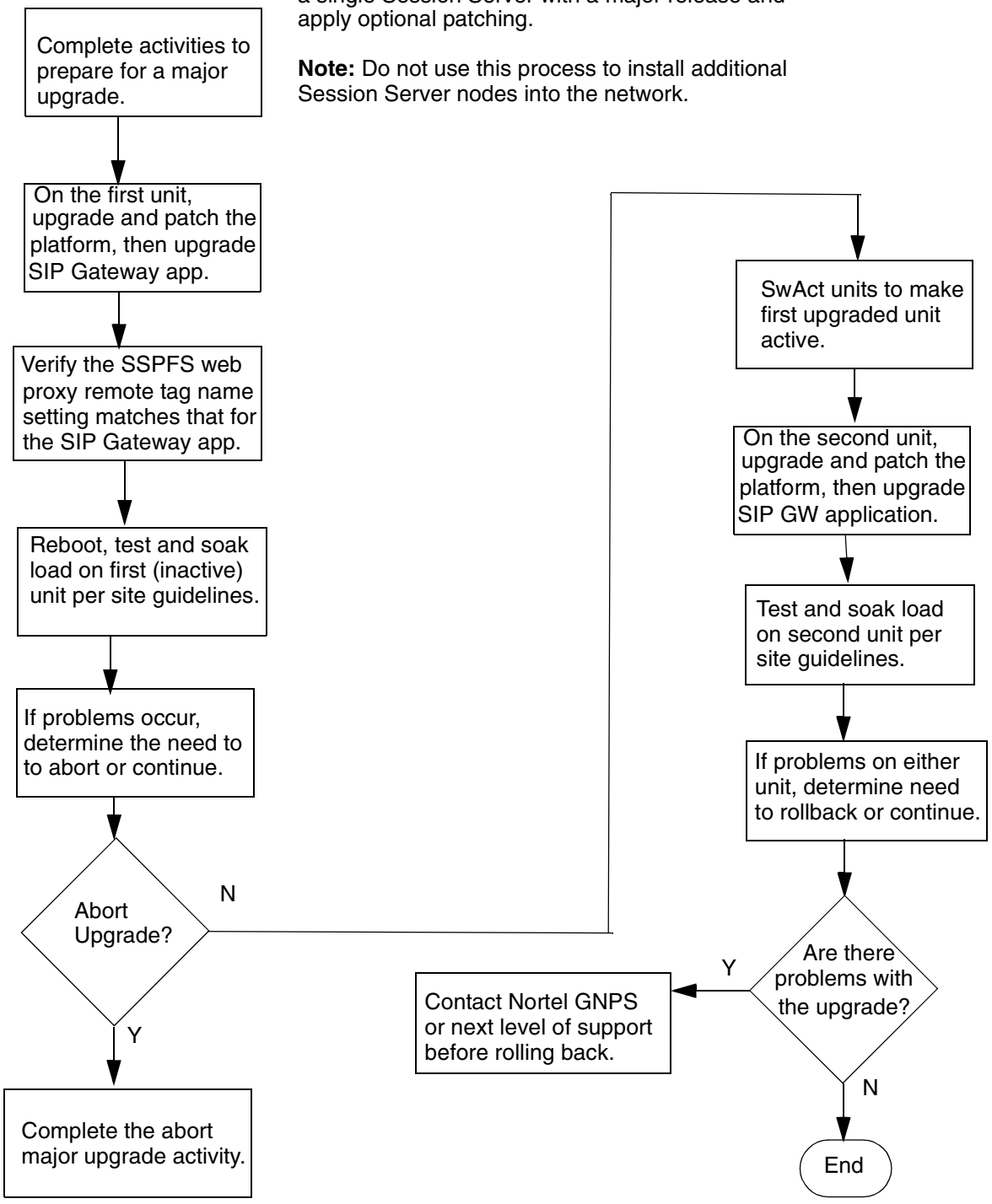
  Using both the CS 2000 NCGL Platform Manager GUI and the Session Server command line interface (CLI), you can upgrade the SIP Gateway application.

Refer to the following activity diagram for a high-level view of the upgrade process for the Session Server units.

Major release upgrade of Session Server with patching

Use the following high-level process to upgrade a single Session Server with a major release and apply optional patching.

Note: Do not use this process to install additional Session Server nodes into the network.



Network upgrade order for Session Server-SIP Gateway application

For all applicable solutions, Session Server with SIP Gateway application should be upgraded before the DPT-GWCs. Verify the upgrade order by referring to the Carrier Voice over IP Network Upgrade Overview NTP, NN10440-450.

Time required for a major upgrade

The approximate time to complete a major upgrade for a Session Server node running the SIP Gateway application is 2-1/2 hours.

Major release upgrade limitations and restrictions

The following general limitations apply to performing a major release upgrade or rollback of a major release upgrade.

- While a major upgrade is a full in-service activity, performing a full rollback of a major upgrade is an out-of-service activity. All call processing and billing information generation is terminated for part of the rollback activity.
- Patches can only be applied using the CLI (command line interface).

Software delivery methods for major releases

Major release software is delivered on a data CD/DVD disk or using Electronic Software Delivery (ESD,) where a compressed ISO image is delivered to an electronic drop-box on the customer network from Nortel Networks.

Major release upgrades using ESD delivery require that the upgrade package be transferred onto both Session Server units and put in the /opt/swd directory using a secure file transfer program such as scp. After the Major release upgrade of the NCGL platform, the bootload file is stored in the /boot directory.

In order to receive Major release software from Nortel using ESD, the operating company must have an ESD agreement with Nortel. When the agreement is established, the operating company furnishes Nortel with the location of an electronic dropbox, an email address for notification and a username and password pair for delivering software loads. When Nortel delivers a software load to the dropbox, an electronic mail notification is sent to the e-mail address specified by the operating company.

Software installation methods for major releases

You can upgrade the Session Server NCGL load from the local DVD-ROM drive, or from an ISO image located on a remote system, or

copied to a local directory. The following upgrade protocols (methods) are selectable from the CS 2000 NCGL Platform Manager GUI:

- Local CDROM - the local DVD-ROM drive (labeled in the software as the local CD-ROM).
- Local file - an iso image, or load.tgz file copied from the local DVD-ROM drive to the hard drive using the secure copy program, **scp**, to transfer the data.
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in cleartext format across the network. This is not a recommended method.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service. This is not a recommended method.

You can upgrade the Session Server SIP Gateway application from the local DVD-ROM drive, or from an ISO image copied to a local directory. Most of the time the software load for the SIP Gateway application is on the same CD/DVD disk or copied ISO image as the NCGL platform load; however, some customers may receive a separate software load for the SIP Gateway application. Consult your release notes for details.

Managing security certificates in SN08

For upgrades from SN07, read and understand the following considerations since action is required during the software upgrade:

- Are you using self-signed certificates or CA-signed certificates?

  The determination of whether the installation is using self-signed certificates or CA-signed certificates is based on the Service Provider's Security Policies. Check with your Security Policy or contact the individual responsible for establishing the security Policies. If after checking the Policies it is unclear if CA-signed certificates are mandated, then self-signed certificates may be used.
- If you are using the original, temporary certificates supplied during an initial SN07 installation, you will need to use the certificate management tool to create new self-signed certificates. During the upgrade, the following questions will need to be answered. For more

information and the values used during the upgrade, refer to Generate self-signed security certificates on page 1218.

— Do you accept the security disclaimer?

— What is the RSA modulus size?

— What is the Expiry days value?

— What is the Country Name?

— What is the State/Province Name?

— What is the Locality Name?

— What is the Organizational Name?

— What is the Organizational Unit Name?

— What is the Common Name

— What is the E-mail address, if applicable?

- If you have previously upgraded the initial SN07 installation according to the Service Provider's Security Policies with certificate authority (CA)-signed certificates for either Apache or Tomcat, then preparation is required and identified in steps 3 and 4 on page 1164. During the upgrade, step 7 on page 1166 will also be necessary to import these certificates.

Prepare for a major release upgrade

Complete the steps for following activity, to prepare for a major release upgrade:

Major release upgrade preparation activity

Step	Procedure or activity
1	Verify the component network order in which the Session Server node will be upgraded for the end-to-end upgrade strategy.
2 (new)	Refer to section Managing security certificates in SN08 on page 1162 and determine the kind of certificates you currently have (customer self-signed or purchased from a certificate authority). You will need this information during the upgrade and after the upgrade is complete.

Major release upgrade preparation activity

Step	Procedure or activity
3	If you have purchased security certificates from a Certificate Authority or created self-signed certificates, use procedure Back up security certificates on page 1173 to ensure that you have made a backup copy of the security certificate files on both Session Server units and to make a backup to a secure remote server location.
4	If you have purchased security certificates from a Certificate Authority, you must prepare to validate your existing certificate chain using procedure Prepare to validate a certificate chain on page 1177.
5	Back up the SIP Gateway application database on the **active** unit using procedure Perform a manual backup of the Session Server database on page 1183.
6	Acquire the appropriate major release software from Nortel either using ESD delivery to a customer dropbox/repository server or from a major release CD/DVD disk.
7	If you are performing a major release upgrade using an ISO image acquired using ESD, complete procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 1185 to copy the ISO files to hard drive of each unit.
8	Use procedure View release notes for a maintenance release on page 1188 to check release notes for upgrade issues.
9	Locate and have available the original Session Server software CD/DVD disk along with a copy of the existing version of the SIP Gateway application installed on your system. The existing version may be from the last maintenance release image installed from a CD/DVD disk or an ESD downloaded image file.
10	Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
11	You have completed this high-level activity.

Perform a major release upgrade

Complete the steps in the order listed, to perform an in-service major release upgrade and optional patching of the NCGL platform.

Major release upgrade activity

Step	Procedure or activity
Upgrade the NCGL platform load on first unit (inactive)	
1	Ensure that you have completed section Prepare for a major release upgrade on page 1163 before continuing.
2	Determine what version of the NCGL platform load is currently installed on your Session Server node by going to the **System Information** page of the CS 2000 NCGL Platform manager and using procedure Determine the current version of the NCGL platform software load on page 1190, to determine if any maintenance releases must be applied before performing a major upgrade. Determine what version of the SIP Gateway application software (listed as Session Server load info) is currently installed on your Session Server node using procedure Determine the current version of software loads on page 1193, to determine if any maintenance releases must be applied before performing a major upgrade.
3	If applying a major upgrade using a CD/DVD disk, insert the disk into the disk drive of the **inactive** unit.
4	At the **active** unit, use procedure Inhibit a system SwAct (Jam) on page 1197 to jam the units.
5	At the NCGL Platform Manager for the physical unit which is **inactive**, upgrade the NCGL platform software using procedure Upgrade Session Server NCGL platform software on page 1201. Ensure that you set the new NCGL load as the default boot load. For instance, if unit 0 is the **active** unit, log into the NCGL Platform Manager GUI for unit 1.
6	From the **active** unit, use procedure Reboot a Session Server unit on page 1208 to perform a **RebootMate** of the **inactive** unit. Monitor the reboot progress from **active** unit CS 2000 NCGL Platform Manager.

Major release upgrade activity

Step	Procedure or activity
7	If your site uses certificates signed by a Certificate Authority, at the **inactive** unit complete procedure Validate a certificate chain on page 1214. If your site uses self-signed certificates, at the **inactive** unit complete procedure Generate self-signed security certificates on page 1218. **Note:** You cannot migrate from self-signed to CA-signed certificates during this upgrade.
8	On the **inactive** unit make a backup copy of your new security certificates using procedure Back up security certificates on page 1173.
9	Log into the **inactive** unit NCGL Platform Manager and go to the **System Information** page. Use procedure View the operational status of a Session Server NCGL platform on page 1228 for assistance with this task. If you can access the NCGL Platform Manager GUI, then the security certificates are properly installed. **Note:** If you cannot access the NCGL Platform Manager, then there is a problem with your security certificates. Contact your next level of support, Nortel GNPS or Nortel's emergency response team.
Apply and commit NCGL patches to the first unit	
10	Use procedure View release notes for a maintenance release on page 1188 to identify the required NCGL platform patches (if any) for the new release.
11	Log onto the **active** unit and use procedure Inhibit a system SwAct (Jam) on page 1197 to verify that the units are jammed. If they are not, then jam the units.
12	Use procedure Acquire patch files on page 1247 to copy all required patches from the CD/DVD disk or the ESD delivered ISO image file to the patching holding directory on the unit.
13	Use procedure Apply and commit an NCGL patch on page 1250 to apply and commit NCGL patches to the **inactive** unit.

Major release upgrade activity

Step	Procedure or activity
Upgrade the SIP Gateway application on the first unit	
14	If an NCGL upgrade was not necessary and the **inactive** unit was not jammed as described in the step 11 on page 1164, follow procedure Inhibit a system SwAct (Jam) on page 1197 before proceeding.
15	On the **inactive** unit, upgrade the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 1258.
16	If necessary, use procedure View web proxy settings in SSPFS for Session Server on page 1253 to determine the tag name you are using for this Session Server node.
17	From the **active** unit, use procedure Reboot a Session Server unit on page 1208 to perform a **RebootMate** of the **inactive** unit. Monitor the reboot progress from **active** unit CS 2000 NCGL Platform Manager.
18	After the **inactive** unit completes rebooting, log into the **inactive** unit's CLI and verify that the current version of the SIP Gateway application matches the expected SN08 version by executing the following command: **cat /opt/apps/webint/version_info.txt.** Refer to procedure Determine the current version of software loads on page 1193 for assistance with this task.
Activate and soak the new load on the first unit	
19	From the **active** unit, verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 1265.
20	Use procedure Enable a system SwAct (Unjam) on page 1267 to unjam the units.

Major release upgrade activity

Step	Procedure or activity
21	As applicable to your site, check the new software on upgraded unit, still **inactive**. • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
22	From the **active** unit, perform a SwAct using procedure Invoke a maintenance SwAct of the Session Server platform on page 1270. All calls will continue to be processed on the (non-upgraded) **active** unit up to the time that the **active** IP address is switched to the **inactive** (upgraded) unit.
23	From the **active** unit, re-verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 1265.
24	As applicable to your site, test new software on upgraded unit, now **active**. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
25	If all software tests are successful, continue with the next step in this procedure to upgrade the second (mate) unit (now **inactive**). Otherwise, if the **active** unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure and complete activity *Abort a major release upgrade* in the Session Server Upgrades NTP, NN10349-461, and contact your next level of support or Nortel GNPS.

Major release upgrade activity

Step	Procedure or activity
Upgrade the NCGL platform load on second unit (now inactive)	
26	Verify that all applicable activities in Section Prepare for a major release upgrade on page 1163 have been completed for the second unit.
27	If applying a major upgrade using a CD/DVD disk, insert the disk into the disk drive of the **inactive** unit.
28	At the **active** unit use procedure Inhibit a system SwAct (Jam) on page 1197 to jam the units.
29	On the NCGL Platform Manager for the physical unit which is **inactive**, upgrade the NCGL platform software using procedure Upgrade Session Server NCGL platform software on page 1201. Ensure that you set the new NCGL load to be the default boot load. For instance, if unit 0 is the **active** unit, log into the NCGL Platform Manager GUI for unit 1.
30	On the **active** unit, copy the new certificates to the mate (**inactive**) unit using procedure Copy security certificates to the mate unit on page 1275.
31	On the **inactive** unit make a backup copy of the new security certificates using procedure Back up security certificates on page 1173.
32	From the **active** unit, use procedure Reboot a Session Server unit on page 1208 to perform a **RebootMate** of the **inactive** unit. Monitor the reboot progress from **active** unit CS 2000 NCGL Platform Manager.
Apply and commit NCGL patches to the second unit	
33	Use procedure View release notes for a maintenance release on page 1188 to identify the required NCGL platform patches for the new release.
34	Log onto the **active** unit and use procedure Inhibit a system SwAct (Jam) on page 1197 to verify that the units are jammed. If they are not, then jam the units.

Major release upgrade activity

Step	Procedure or activity
35	Use procedure Acquire patch files on page 1247 to copy all required patches from the CD/DVD disk or the ESD delivered ISO image file to the patching holding directory on the unit.
36	Use procedure Apply and commit an NCGL patch on page 1250 to apply and commit NCGL patches to the **inactive** unit.
Upgrade the SIP Gateway application software on the second unit	
37	At the **inactive** unit, upgrade the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 1258. **Note:** As indicated in the procedure, when entering the remote tag name, use the same tag name as the one entered for the first unit. Both units in the node must use the same remote tag name.
38	From the **active** unit, use procedure Reboot a Session Server unit on page 1208 to perform a **RebootMate** of the **inactive** unit. Monitor the reboot progress from **active** unit CS 2000 NCGL Platform Manager.
39	After the **inactive** unit completes rebooting, log into the **inactive** unit's CLI and verify that the current version of the SIP Gateway application matches the expected new version by executing the following command: **cat /opt/apps/webint/version_info.txt.**
Activate and soak the new load on the second unit	
40	From the **active** unit, verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 1265.
41	Use procedure Enable a system SwAct (Unjam) on page 1267 to unjam the units.

Major release upgrade activity

Step	Procedure or activity
42	As applicable to your site, check the new software on the upgraded unit, still **inactive**. • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
43	From the **active** unit perform a SwAct of the units using procedure Invoke a maintenance SwAct of the Session Server platform on page 1270.
44	As applicable to your site, test new software on the upgraded unit, now **active**. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
45	If all software tests are successful, continue with the next step in this activity to upgrade. Otherwise, if the **active** unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure. Go to and complete procedure *Perform a major release rollback activity* in the Session Server Upgrades NTP, NN10349-461, and contact your next level of support, Nortel GNPS or Nortel's emergency response team.
46	From the **active** unit, verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 1265.

Major release upgrade activity

Step	Procedure or activity
47	Monitor the system for an appropriate period per your site guidelines before declaring this major upgrade complete. In SN08, multiple Session Server nodes can be installed in your network. However, ensure that all upgrade related issues are resolved for this Session Server node before installing any additional nodes in your network. Once additional nodes are installed in your network, you cannot roll back to SN07.
48	Edit the object properties in the IEMS for the Session Server you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the Device Version field. • Editing and viewing object properties using Java Web Client on page 1841 • Editing and viewing object properties using Web Client on page 1846
49	You have completed the major release upgrade activity.

Back up security certificates

Purpose of this procedure

Use the following procedure to create backup copies of security certificates to a folder on the Session Server unit and make copies to a remote server location, chosen by the customer.

Use this procedure anytime new security certificates are created or when the system is changed from using self-signed certificates to CA-signed certificates. This procedure is also used as part of a major release upgrade activity.

Limitations and Restrictions

There are no limitations on performing this procedure.

Prerequisites

There are no prerequisites for this procedure.

Action

Perform the following steps to complete this procedure.

At the Session Server CLI or Integrated EMS client

1 Log on to the Session Server unit that has the security certificates you need to back up, and change to the root user.

If you are performing this procedure outside of a high-level task, back up the security certificates on both units. Otherwise, back up the security certificates on the unit indicated in the high-level task that directed you to this procedure.

2 Change directories to the /opt/base/share/ssl directory. Type

```
# cd /opt/base/share/ssl
```

and press the Enter key.

3 Create a new directory to store backup copies of the certificate files

```
$ mkdir <SNxx_ddmmyyyy>
```

and pressing the Enter key.

where

SNxx_ddmmyyyy
is the name of the new directory based on the currently installed release of the system software (for example SN08) and the current date in the format ddmmyyyy

4 Copy the certificates to the newly created backup directory by typing

```
# cp * <SNxx_ddmmyyyy>
```

and press the Enter key.

where

SNxx_ddmmyyyy
is the name of the new backup directory

ATTENTION

Completing this step ensures that you have valid backup copies of the security certificates for restoring in case of an upgrade abort or rollback or for disaster recovery purposes.

5 Use the following table to determine your next step:

If	Do
you want to make backup copies of the security certificates to a remote server	Ensure that the remote host that will store the security related files is secure, that the host is unavailable to general users, and offers restricted access to personnel with security related responsibilities. Proceed to step 6
you do not want to make backup copies of the security certificates to a remote server	This procedure is complete.

6 Secure copy the server.key file to the remote server by typing

```
$ scp server.key <user>@<remote_server>:</path>
```

and pressing the Enter key.

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The server.key file is copied to the remote server.

7 Secure copy the certificate.keystore file to the remote server by typing

```
$ scp certificate.keystore
<user>@<remote_server>:</path>
```

and pressing the Enter key.

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The certificate.keystore file is copied to the remote server.

8 Secure copy the server.crt file to the remote server by typing

```
$ scp server.crt <user>@<remote_server>:</path>
```

and pressing the Enter key.

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The server.crt file is copied to the remote server.

9 If you have a CA-signed certificate, secure copy the trusted.crt file to the remote server by typing

```
$ scp trusted.crt
<user>@<remote_server>:/<path>
```

and pressing the Enter key.

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The trusted.crt file is copied to the remote server.

10 You have completed this procedure.

Prepare to validate a certificate chain

Purpose of this procedure

Use the following procedure to migrate certificate authority (CA)-signed security certificates during an upgrade from SN07. If not upgrading from SN07, do not use this procedure.

This procedure cannot be performed on self-signed certificates. Migrating self-signed certificates is not supported. If your site uses self-signed certificates, you must create new ones during the upgrade activity.

Limitations and Restrictions

The following restrictions apply to migrating CA-signed certificates:

- Only PEM formatted, CA-signed certificates are supported on Session Server.
- A CA-chain is required in PEM format in a trusted.crt file, top down, with the root CA at the top. Refer to section Additional information about trusted certificates on page 1178 for more information.

Prerequisites

Existing CA-signed security certificates must be prepared per section Additional information about trusted certificates on page 1178.

Action

Perform the following steps to complete this procedure.

At the Session Server CLI or Integrated EMS client

1. Log onto the inactive Session Server unit and change to the root user.
2. Ensure that the local server CA-signed certificate that was obtained from the certificate authority is in the file /opt/base/share/ssl/server.crt.
3. Ensure that the private key corresponding to the local server CA-signed certificate is in the file /opt/base/share/ssl/server.key.

ATTENTION

There can only be one certificate in the server.crt file and that certificate must be in PEM format.

Note: Refer to section Additional information about trusted certificates on page 1178 for assistance with this task.

4 From the certificate authority, obtain the CA certificate chain, with the root CA-certificate, in top down format, in the file /opt/base/share/ssl/trusted.crt file. This chain can be obtained from the certificate authority directly.

ATTENTION
The trusted.crt certificate must be in PEM format.

5 Verify successful preparation of the certificate files by typing

```
openssl verify /opt/base/share/ssl/trusted.crt
/opt/base/share/ssl/server.crt
```

and press the Enter key.

6 If the result from step 5 is “OK”, you are ready to proceed with the upgrade preparation. If the result from step 5 is not “OK”, then there was problem with the security certificates and you must contact Nortel GNPS.

7 The procedure is complete.

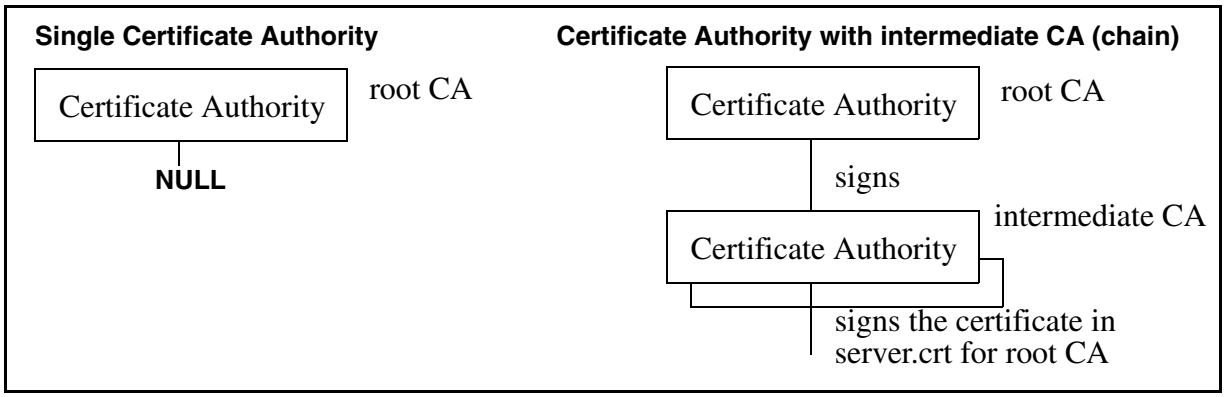
Additional information about trusted certificates

The following section provides additional information about trusted certificates and root CAs.

Root CAs that do not correspond to the local server certificate are not placed in the trusted.crt file. They are added using the CS 2000 Session Server Manger GUI using procedure *Manage Trusted Certificates*, found in the Session Server Security and Administration NTP, NN10346-611. Only the Root CA corresponding to the local certificate is placed in the trusted. crt file, followed by the CA chain. For example, if the local certificate is signed by one of the global public root certificate authorities, then that root CA certificate is placed in this file.

The following figure shows an example of the structure of a trusted.crt file. The trusted.crt on the left shows a single CA signing the root certificate. The trusted.crt on the right shows the certificate of the Certificate Authority (CA), followed by each intermediate chain CA, followed by the CA which ultimately signed the local certificate.

Structure of a trusted.crt file



The following is an example of a CA-signed trusted.crt file. In this case, it is a chain composed of a root CA, followed by 3 (three) intermediate chain CAs. At the top of the file is certificate of the root Certificate Authority (CA), followed by each intermediate chain CA, followed by that last CA which ultimately signed the local certificate.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks,
OU=Certificate Authority
        Validity
            Not Before: Oct  8 01:14:48 2004 GMT
            Not After : Oct  8 01:14:48 2005 GMT
        Subject: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks,
OU=Certificate Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                00:bc:53:2a:bd:bf:36:87:36:5b:12:93:a7:55:84:
                 1d:3b:75:0f:d9:de:d6:34:d3:51:8d:96:c6:41:c6:
                       80:b3:08:18:e7:b1:e5:af:0a:00:1d:65:82:77:0a:
                ca:7d:74:00:79:85:d6:80:07:79:8d:ec:b0:e3:6e:
                8c:d0:a7:20:6f:c7:3b:df:09:83:93:36:9f:eb:67:
                  c1:e2:ab:a5:ed:ab:3a:d8:97:ad:83:bf:8c:11:02:
                     12:3b:dc:a9:82:0d:f3:45:d7:8a:ae:96:eb:17:26:
                  3c:de:7a:cd:91:71:b9:56:c7:e7:0c:7a:5e:57:62:
                9c:d7:3e:41:82:c9:f3:34:1d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:

90:20:BC:77:DD:64:50:D7:50:56:5D:C7:3F:EC:7A:32:21:0F:AE:F4
            X509v3 Authority Key Identifier:

keyid:90:20:BC:77:DD:64:50:D7:50:56:5D:C7:3F:EC:7A:32:21:0F:AE:F4
                DirName:/C=CA/ST=Ontario/L=Timbuktu/O=Nortel
Networks/OU=Certificate Authority
                serial:00

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
```

```
        33:65:6c:d0:0d:b8:7f:58:1c:33:1c:d2:4e:e3:19:2d:36:c3:
        15:7f:b3:80:cb:22:2a:dc:eb:ba:84:50:24:7c:cc:07:49:62:
        f5:2c:f9:bc:47:04:56:ea:bd:78:de:44:43:22:e2:1c:5f:fc:
        17:91:80:70:f3:29:e2:74:46:8d:3d:ac:fa:63:f2:b4:ba:79:
        d2:22:76:6c:2e:fb:e6:55:16:6f:db:27:5f:e3:ff:32:84:5a:
        b7:a3:9c:c4:73:f9:72:c2:8b:6e:8d:4f:bf:d2:3f:b1:51:48:
        b5:4e:27:b4:bb:80:4b:87:f9:e7:18:ba:63:20:ac:6d:25:c2:
        74:1b

-----BEGIN CERTIFICATE-----
MIIDGDCCAoGgAwIBAgIBADANBgkqhkiG9w0BAQQFADBsMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzERMA8GA1UEBxMIVGltYnVrdHUxGDAWBgNVBAoTD05v
cnRlbCBOZXR3b3JrczEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTA0MTAwODAxMTQ0OFoXDTA1MTAwODAxMTQ0OFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xETAPBgNVBAcTCFRpbWJ1a3R1MRgwFgYDVQQKEw9Ob3J0
ZWwgTmV0d29ya3MxHjAcBgNVBAsTFUNlcnRpZmljYXRlIEF1dGhvcml0eTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvFMqvb82hzZbEpOnVYQdO3UP2d7WNNNR
jZbGQcaAswgY57HlrwoAHWWCdwrKfXQAeYXWgAd5jeyw426M0Kcgb8c73wmDkzaf
62fB4qul7as62Jetg7+MEQISO9ypgg3zRdeKrpbrFyY83nrNkXG5VsfnDHpeV2Kc
1z5BgsnzNB0CAwEAAaOByTCBxjAdBgNVHQ4EFgQUkCC8d91kUNdQVl3HP+x6MiEP
rvQwgZYGA1UdIwSBjjCBi4AUkCC8d91kUNdQVl3HP+x6MiEPrvShcKRuMGwxCzAJ
BgNVBAYTAkNBMRAwDgYDVQQIEwdPbnRhcmlvMREwDwYDVQQHEwhUaW1idWt0dTEY
MBYGA1UEChMPTm9ydGVsIE5ldHdvcmtzMR4wHAYDVQQLExVDZXJ0aWZpY2F0ZSBB
dXRob3JpdHmCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQAzZWzQ
Dbh/WBwzHNJO4xktNsMVf7OAyyIq3Ou6hFAkfMwHSWL1LPm8RwRW6r143kRDIuIc
X/wXkYBw8ynidEaNPaz6Y/K0unnSInZsLvvmVRZv2ydf4/8yhFq3o5zEc/lywotu
jU+/0j+xUUi1Tie0u4BLh/nnGLpjIKxtJcJ0Gw==
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks,
OU=Certificate Authority
        Validity
            Not Before: Oct  8 01:19:20 2004 GMT
            Not After : Oct  8 01:19:20 2005 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain1, CN=Chain1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c5:d9:e9:4d:aa:87:56:ce:b0:ba:17:fb:fd:78:
                    89:85:54:21:5b:2e:e8:71:e8:14:64:00:dd:b5:2e:
                    0b:2a:e5:75:71:c2:42:17:29:e7:44:79:b0:2a:82:
                    05:5b:92:c1:f3:5a:72:90:72:ee:ec:b1:77:39:cf:
                    3c:c3:92:6a:6d:49:41:43:96:4c:e9:f6:3f:c3:3a:
                    d9:79:11:ff:aa:74:ba:31:71:b3:0e:f0:f8:20:21:
                    3c:76:5b:ad:6b:b6:27:2a:27:86:99:06:3a:1c:81:
                    a5:ca:7c:68:36:cd:45:bd:2f:48:b0:5e:03:75:6e:
                    35:95:42:60:3e:6e:f5:bc:35
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        99:56:1b:2f:2f:b0:5f:4f:a5:7b:70:ce:6c:41:d3:36:20:2c:
        31:fb:61:df:81:58:81:4c:7f:30:a8:e1:d8:c7:97:0b:ad:19:
        21:19:79:ba:90:9f:3d:38:a0:66:6d:0a:6e:47:16:7f:4c:5b:
        7d:5b:bd:21:23:bc:15:27:e9:e5:f5:ec:6b:38:67:69:4e:86:
        82:a9:c0:f5:8a:c4:39:f7:98:89:ac:45:3f:a1:c9:47:26:9b:
        54:d2:d4:9d:d2:dd:c8:4f:58:cf:7c:57:d8:10:6d:d4:3e:3e:
        0a:12:1f:54:d7:f5:38:43:3d:f7:09:8e:33:b5:a1:80:00:14:
        50:f0

-----BEGIN CERTIFICATE-----
```

```
MIICXjCCAcegAwIBAgIBATANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzERMA8GA1UEBxMIVGltYnVrdHUxGDAWBgNVBAoTD05v
cnRlbCBOZXR3b3JrczEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTA0MTAwODAxMTkyMFoXDTA1MTAwODAxMTkyMFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjExDzANBgNVBAMTBkNoYWluMTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxdnpTaqHVs6wuhf7/XiJhVQhWy7ocegU
ZADdtS4LKuV1ccJCFynnRHmwKoIFW5LB81pykHLu7LF3Oc88w5JqbUlBQ5ZM6fY/
wzrZeRH/qnS6MXGzDvD4ICE8dluta7YnKieGmQY6HIGlynxoNs1FvS9IsF4DdW41
lUJgPm71vDUCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
gQCZVhsvL7BfT6V7cM5sQdM2ICwx+2HfgViBTH8wqOHYx5cLrRkhGXm6kJ89OKBm
bQpuRxZ/TFt9W70hI7wVJ+nl9exrOGdpToaCqcD1isQ595iJrEU/oclHJptU0tSd
0t3IT1jPfFfYEG3UPj4KEh9U1/U4Qz33CY4ztaGAABRQ8A==
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain1, CN=Chain1
        Validity
            Not Before: Oct  8 01:22:23 2004 GMT
            Not After : Oct  8 01:22:23 2005 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain2, CN=Chain2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:bf:8a:b7:44:9c:92:b5:fd:f0:e7:d3:1c:9d:65:
                    c4:e3:8c:cb:d3:60:a0:9d:bc:d7:87:15:d1:f0:68:
                    3c:71:be:2e:8d:2f:d0:7e:f6:95:2f:f3:89:b4:9b:
                    b6:c9:bd:52:62:8d:05:e3:71:3e:d5:c1:50:27:67:
                    01:f4:8b:7e:c9:6d:4e:a5:24:ff:d7:80:37:86:09:
                    8c:0a:8d:79:cc:b2:e6:9e:d8:7d:71:db:12:e6:84:
                    7e:2f:90:17:ca:84:87:9b:63:72:4a:28:d7:75:91:
                    f1:4f:c2:6b:5e:a7:d2:2b:01:60:f7:5f:35:dd:8e:
                    92:d7:b7:f5:a4:66:f6:af:21
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        3c:0c:fa:58:1f:14:d3:3f:f1:cb:80:7b:8f:bb:f7:17:e5:18:
        21:bd:a2:77:3e:ce:5d:4c:80:a8:3e:7e:a1:9c:fe:c8:6a:d0:
        7d:67:45:b9:5a:a6:89:3a:2f:de:25:20:2f:ed:62:b5:06:8f:
        dd:a1:85:aa:a2:a3:8d:a3:6d:4c:5e:ed:e8:35:f3:50:98:26:
        99:38:1c:33:a3:99:0a:50:11:f8:0e:21:9d:fe:56:fb:ec:b9:
        55:ed:83:a7:b0:a4:26:82:7f:12:3b:35:9c:03:b9:40:02:3d:
        5c:d5:34:e2:ee:ff:91:58:9f:9d:cf:2e:91:35:9d:c8:5a:f1:
        19:59

-----BEGIN CERTIFICATE-----
MIICXjCCAcegAwIBAgIBAjANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzEPMA0GA1UEBxMGT3R0YXdhMRgwFgYDVQQKEw9Ob3J0
ZWwgTmV0d29ya3MxDzANBgNVBAsTBkNoYWluMTEPMA0GA1UEAxMGQ2hhaW4xMB4X
DTA0MTAwODAxMjIyM1oXDTA1MTAwODAxMjIyM1owbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjIxDzANBgNVBAMTBkNoYWluMjCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAv4q3RJyStf3w59McnWXE44zL02CgnbzX
hxXR8Gg8cb4ujS/QfvaVL/OJtJu2yb1SYo0F43E+1cFQJ2cB9It+yW1OpST/14A3
hgmMCo15zLLmnth9cdsS5oR+L5AXyoSHm2NySijXdZHxT8JrXqfSKwFg91813Y6S
17f1pGb2ryECAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
gQA8DPpYHxTTP/HLgHuPu/cX5RghvaJ3Ps5dTICoPn6hnP7IatB9Z0W5WqaJOi/e
JSAv7WK1Bo/doYWqoqONo21MXu3oNfNQmCaZOBwzo5kKUBH4DiGd/lb77LlV7YOn
sKQmgn8SOzWcA7lAAj1c1TTi7v+RWJ+dzy6RNZ3IWvEZWQ==
-----END CERTIFICATE-----
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain2, CN=Chain2
        Validity
            Not Before: Oct  8 01:24:40 2004 GMT
            Not After : Oct  8 01:24:40 2005 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain3, CN=Chain3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:9e:10:4a:52:3a:e3:27:cc:0f:bb:70:a0:dc:66:
                    df:27:47:17:54:4c:56:1e:f1:7c:6e:71:e6:b0:f1:
                    7e:2d:a3:32:e0:c1:a4:50:5e:3a:cf:eb:09:ac:f5:
                    00:f4:25:a5:ae:59:3d:b0:e5:02:af:ec:d8:b2:e5:
                    c3:31:35:d0:d0:14:35:7d:c9:85:ef:fc:b3:c4:05:
                    0b:06:b4:b9:67:53:4d:0b:e9:c8:f1:a0:44:ac:6f:
                    27:4c:71:6f:be:31:63:12:21:4d:4b:a8:58:97:67:
                    c0:e4:1f:bb:d2:fe:4d:d6:48:3c:19:c6:fb:db:2a:
                    4e:1d:bf:f4:b4:41:23:69:c5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        bd:1b:08:a2:9f:af:f4:3e:3e:b6:72:e4:ca:ec:89:c5:fe:e4:
        fd:99:b9:a4:31:b9:58:64:83:df:b5:8e:d3:97:89:c3:e8:0c:
        96:0b:9d:c2:cc:81:b1:cd:78:17:13:ad:28:e8:ae:4d:2b:0e:
        1b:b7:96:e2:74:65:23:02:5a:b1:e6:90:89:cf:9b:3c:c1:b5:
        44:6f:ac:05:0d:d7:86:cc:eb:ce:ea:36:12:5a:3b:44:ac:f9:
        0e:44:f5:c0:23:ff:55:1f:ef:1d:64:04:82:f2:7b:cc:22:25:
        49:e4:a5:74:8c:9a:1d:22:5c:a7:7e:04:12:90:c9:88:d6:f4:
        a2:b0
-----BEGIN CERTIFICATE-----
MIICXjCCAcegAwIBAgIBAzANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzEPMA0GA1UEBxMGT3R0YXdhMRgwFgYDVQQKEw9Ob3J0
ZWwgTmV0d29ya3MxDzANBgNVBAsTBkNoYWluMjEPMA0GA1UEAxMGQ2hhaW4yMB4X
DTA0MTAwODAxMjQ0MFoXDTA1MTAwODAxMjQ0MFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjMxDzANBgNVBAMTBkNoYWluMzCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAnhBKUjrjJ8wPu3Cg3GbfJ0cXVExWHvF8
bnHmsPF+LaMy4MGkUF46z+sJrPUA9CWlrlk9sOUCr+zYsuXDMTXQ0BQ1fcmF7/yz
xAULBrS5Z1NNC+nI8aBErG8nTHFvvjFjEiFNS6hYl2fA5B+70v5N1kg8Gcb72ypO
Hb/0tEEjacUCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
gQC9Gwiin6/0Pj62cuTK7InF/uT9mbmkMblYZIPftY7Tl4nD6AyWC53CzIGxzXgX
E60o6K5NKw4bt5bidGUjAlqx5pCJz5s8wbVEb6wFDdeGzOvO6jYSWjtErPkORPXA
I/9VH+8dZASC8nvMIiVJ5KV0jJodIlynfgQSkMmI1vSisA==
-----END CERTIFICATE-----
```

Perform a manual backup of the Session Server database

Purpose of this procedure

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

Limitations and Restrictions

ATTENTION

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

Prerequisites

ATTENTION

The SIP Gateway application database must be in sync with the CS 2000 to ensure an accurate copy of the active unit database is created. Verify this condition using procedure Verify synchronization status of Session Server units on page 1265.

Action

At the Session Server CLI or Integrated EMS client

1. Log onto the active Session Server unit and change to the root user.
2. Change directory to the database directory by typing

   ```
   # cd /opt/apps/database/solid/dbfiles
   ```

   and pressing the Enter key.
3. Put a copy of the database for the active unit in the backup directory by typing

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

and pressing the Enter key.

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

Example

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

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

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

5 You have completed this procedure.

Extract an ISO image from an Electronic Software Delivery (ESD)

Purpose of this procedure

Use this procedure to extract an ISO image, patch files and release notes for a major upgrade or maintenance release archive file retrieved from an electronic software delivery dropbox. This procedure can be used as a standalone task or as part of higher level activity.

Prerequisites

Ensure that the ESD software archive file has been transferred from the dropbox on the repository server. The repository server is the machine owned by the operating company that was selected to be the destination for the ESD software files.

To secure copy the ISO image from the dropbox into the target directory, type

```
scp <ISO_filename> mtc@<Session_Server_IP>:/opt/swd
```

This command assumes the customer has logged onto the dropbox and is in the target directory that contains the ISO file before the command is executed. The system prompts for a password before the file transfer can commence. If the transfer fails, delete any older ISO files in the /opt/swd directory to ensure enough space exists for the new ISO file.

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 Carrier Voice over IP Network Upgrade Overview NTP, NN10440-450 and the document Electronic Software Delivery Customer Implementation Guide, found on your solution CD.

Restrictions and Limitations

This procedure must be completed on both the active and inactive units.

Action

At the Session Server CLI or Integrated EMS client

1 Log onto either Session Server unit and change to root user.

2 Change directory to the location of the ESD software archive file by typing

$ cd /opt/swd

and pressing the Enter key.

3 Ensure that enough disk space is available for the extracted ISO image by typing

$ df -h /opt/swd

and pressing the Enter key.

Ensure that the value in field Avail is at least 350. This ensures that at least 350 Megabytes are available. In the example that follows, 1013 Megabytes are available.

```
[root@hostname swd]# df -h /opt/swd
Filesystem            Size  Used Avail Use% Mounted on
/dev/ntvg/_opt_swd   1014M  364k 1013M   1% /opt/swd
[root@hostname swd]#
```

4 Uncompress the ESD software load from the ESD archive file by typing

$ tar xvzf <ESD_ISOfilename>.tar.gz

and pressing the Enter key.

where

<ESD_ISOfilename>
is the file name of the ESD delivered upgrade file

Example
$ tar xvzf NGSS0080.80.P.NCL.NAP.VAULT.6.D.tar.gz

The ESD software load is unarchived, 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.

5 Change directory to the newly created directory by typing

$ cd <ESD_ISO_directory>

and pressing the Enter key.

where

<ESD_ISO_directory>
is the file name of the ESD delivered upgrade file

Example
$ cd NGSS0070.70.P.NCL.NAP.VAULT.6.D

6 Verify that the image file exists in the directory by typing

`$ ls -l`

and pressing the Enter key.

The system responds with a long listing of files in the directory including the ISO image file, any applicable patch files and the release notes file.

7 Mount the image file to mount point `/cdrom` by typing

`mount -t iso9660 -o loop <iso image> /cdrom`

Example
mount -t iso9660 -o loop NGSS08.x_NCL.iso.tape /cdrom

The command prompt returns upon success and the contents of the image are available from the /cdrom mount point.

8 List the contents of the ISO by typing

`cd /cdrom`
`ls -l`

The system responds with a list of files in the ISO image including any applicable patch files and the release notes file.

```
[root@hostname cdrom]# ls -l
total 19361
-r-xr-xr-x    1 208126   4848         5005 Mar 22 17:36 InstallApps
drwxrwxrwx    2 208126   4848         6144 Mar 22 17:36 Tools
-r-xr-xr-x    1 208126   4848           33 Feb 23 18:09 buildversion
drwxrwxrwx    2 208126   4848         2048 Feb 23 18:09 isolinux
-r-xr-xr-x    1 208126   4848     19810925 Feb 23 18:09 load.tgz
```

9 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

The NCGL software is available for install by selecting Local CDROM from the Software Upgrade area of the Services web page.

The SIP Gateway application software is available for install by logging in to the unit and running the InstallApps script from the `/cdrom` directory.

Note: Repeat this procedure on the second unit before beginning the software upgrade.

View release notes for a maintenance release

Purpose of this procedure

Use this procedure to view the release notes for a maintenance release or patching release. This procedure may be used as a standalone task or as part of a higher level activity.

Limitations and Restrictions

There are no restrictions for performing this procedure.

Prerequisites

If reading release notes from a DVD disk, ensure that the maintenance release DVD-ROM disk is inserted into the inactive unit DVD-ROM drive.

Action

At a Session Server CLI or Integrated EMS client

1 Log on to the inactive Session Server unit and change to root user

2 Use the following table to determine your first step.

If media is delivered by	Do
ESD	step 3
CD/DVD disk	step 4

3 Ensure the software archive file, which includes the release notes, has been extracted and put in the /opt/swd directory on the inactive unit, and that the image file has been mounted to mount point /cdrom. If required, refer to procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 1185

When complete, return to this procedure, and proceed to step 7.

4 Insert the CD/DVD-ROM disk into the DVD-ROM disk drive of the inactive unit.

5 At the prompt, type

```
$ cd /
```

and press Enter.

6 Mount the DVD-ROM drive by typing

```
$ mount /cdrom
```

and pressing the Enter key.

7 Change directories to the mounted filesystem by typing

```
$ cd /cdrom
```

and pressing the Enter key.

8 Locate the release notes file by typing

```
$ ls
```

and pressing the Enter key.

If release notes are available, they are listed as a .pdf file with the rest of the files.

9 Transfer the release notes file from the unit and then open the file with a viewer that reads .pdf format files.

Note: It may be necessary to transfer the release notes .pdf file (/cdrom/pdf) using FTP to an OAMP node in the network, and then transfer the pdf file to a PC with Adobe Acrobat Reader.

10 When you have finished reviewing the release notes file, change directories out of the mounted DVD-ROM filesystem by typing

```
$ cd /
```

and pressing the Enter key.

11 Unmount the DVD-ROM drive by typing

```
$ umount /cdrom
```

and pressing the Enter key.

12 You have completed this procedure. Return to the high level task or procedure that directed you to this procedure.

Determine the current version of the NCGL platform software load

Purpose of this procedure

Use this procedure to determine the version of the NCGL platform software load for a Session Server unit, regardless of installed application software. This procedure can be used as a standalone task or as part of a higher level activity.

Limitations and Restrictions

There are no restrictions to performing this procedure

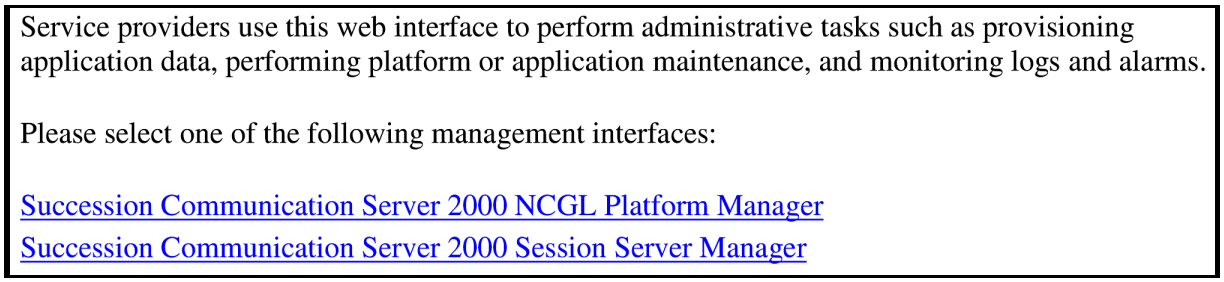
Prerequisites

This procedure has no prerequisites.

Action

At the Session Server GUI or Integrated EMS client

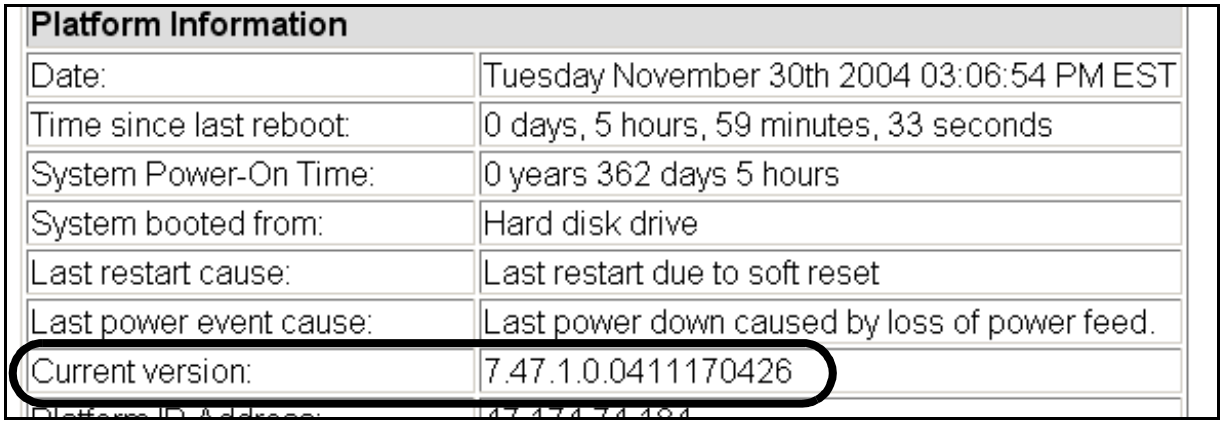
1 Select ***Succession Communication Server 2000 NCGL Platform Manager*** from the launch point menu.


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

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Review the **System/Platform Information** page for the NCGL platform version information.



Platform Information	
Date:	Tuesday November 30th 2004 03:06:54 PM EST
Time since last reboot:	0 days, 5 hours, 59 minutes, 33 seconds
System Power-On Time:	0 years 362 days 5 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to soft reset
Last power event cause:	Last power down caused by loss of power feed.
Current version:	7.47.1.0.0411170426

3 You have completed this procedure.

Alternate command line interface method- (existing SN08 platforms)

At the Session Server console interface

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Verify the installed software versions for this unit by typing

`# cat /opt/apps/webint/version_info.txt`

and pressing the **Enter** key.

The system responds:

```
=======================================================
Session Server Load Info
=======================================================
Release  = NGSS_08_Bld_int
Version  = NGSS_08_Bld_49_b
Build Date = Mon Nov 29 14:47:17 EST 2004
=======================================================
=======================================================
NCGL Platform Load Info
=======================================================
BUILDVERSION=7.47.1.0.0411170426
=======================================================
```

3 You have completed this procedure.

Alternate command line interface method- (existing SN07 platforms)

At the Session Server console interface

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Verify the installed software versions for this unit by typing

`# cat /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/html/version_info.txt`

and pressing the **Enter** key.

The system responds:

```
=======================================================
Session Server Load Info
=======================================================
Release  = NGSS_08_Bld_int
Version  = NGSS_08_Bld_49_b
Build Date = Mon Nov 29 14:47:17 EST 2004
=======================================================
=======================================================
NCGL Platform Load Info
=======================================================
BUILDVERSION=7.47.1.0.0411170426
=======================================================
```

3 You have completed this procedure.

Determine the current version of software loads

Purpose of this procedure

Use this procedure to determine the version of the software loads for the SIP Gateway application on the active unit. This procedure can be used as a standalone task or as part of a higher level activity.

Limitations and Restrictions

The version information for the NCGL platform load is only accurate if a maintenance release has not been applied to the load. If a maintenance release has been applied to the NCGL platform load, its version information is not accurately shown on this page. To accurately determine the NCGL platform load version that the unit is operating on, use procedure View the operational status of a Session Server NCGL platform on page 1228 and go to the ***System Info*** page. As an alternative, you can use the procedure Use the procedure Alternate command line interface method- (existing SN08 platforms) on page 1195 or Alternate command line interface method- (existing SN07 platforms) on page 1195 to determine the correct NCGL platform load version.

The version information for the SIP Gateway application is accurately shown even if a maintenance release is applied to the application.

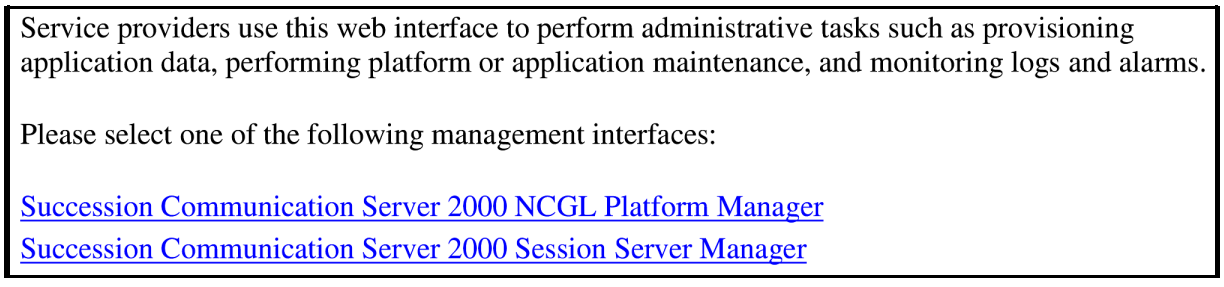
Prerequisites

This procedure has no prerequisites.

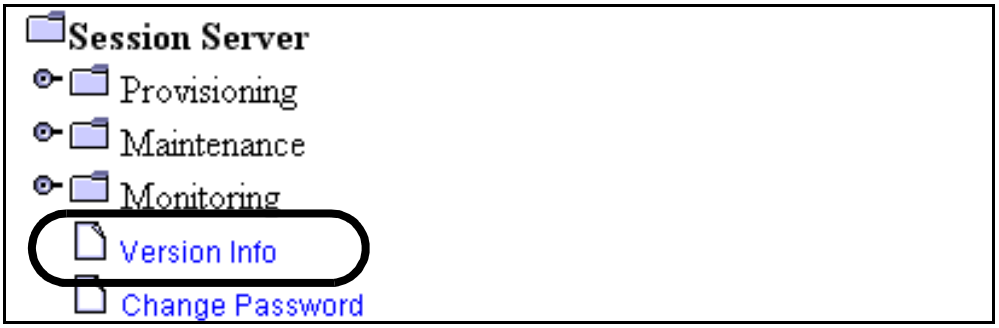
Action

At the Session Server GUI or Integrated EMS client

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

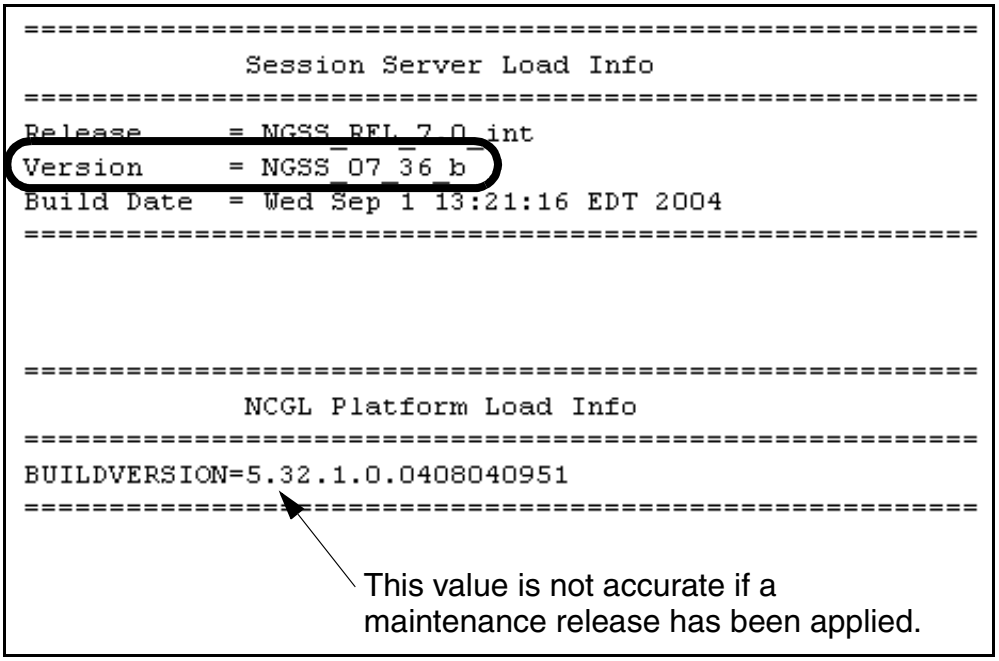


2 At the Session Server folder, click the **Version Info** link.



3 Review and record the software load version information for the SIP Gateway application (top).

Note: The version information for the NCGL platform load is only accurate if a maintenance release has not been applied to the load. However, if a major upgrade is applied, the version info will be accurately reflected in the view. If a maintenance release is applied behind a major upgrade to the NCGL platform load, then the version information is not accurately reflected on this page. Use the procedure Alternate command line interface method- (existing SN08 platforms) on page 1195 or Alternate command line interface method- (existing SN07 platforms) on page 1195 to determine the correct NCGL platform load version.



4 You have completed this procedure.

Alternate command line interface method- (existing SN08 platforms)

At the Session Server console interface

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Verify the installed software versions for this unit by typing

`# cat /opt/apps/webint/version_info.txt`

and pressing the **Enter** key.

The system responds:

```
=========================================================
Session Server Load Info
=========================================================
Release  = NGSS_08_Bld_int
Version  = NGSS_08_Bld_49_b
Build Date = Mon Nov 29 14:47:17 EST 2004
=========================================================
=========================================================
NCGL Platform Load Info
=========================================================
BUILDVERSION=7.47.1.0.0411170426
=========================================================
```

3 You have completed this procedure.

Alternate command line interface method- (existing SN07 platforms)

At the Session Server console interface

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Verify the installed software versions for this unit by typing

`# cat /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/html/version_info.txt`

and pressing the **Enter** key.

The system responds:

```
=========================================================
Session Server Load Info
=========================================================
Release  = NGSS_08_Bld_int
Version  = NGSS_08_Bld_49_b
Build Date = Mon Nov 29 14:47:17 EST 2004
=========================================================
=========================================================
NCGL Platform Load Info
=========================================================
BUILDVERSION=7.47.1.0.0411170426
=========================================================
```

3 You have completed this procedure.

Inhibit a system SwAct (Jam)

Purpose of this procedure

The jam command is used to manually prevent a SwAct (switch of activity) of the active and stand-by units by inhibiting the toggling of operational states of both units, thereby preventing the stand-by unit from going active.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as in cases of a replacing a faulty standby unit or upgrading the software for a standby unit.

ATTENTION

This procedure can only be performed from the active unit. You cannot Jam the active unit if the inactive unit is out of service.

CAUTION

This procedure prevents the Session Server node from operating in a duplex, fault-tolerant mode and prevents the SIP Gateway application from being able to SwAct between Session Server units as needed. Keep a jam in effect only as long as is necessary.

Prerequisites

There are no prerequisites for performing this procedure.

Action

At the Session Server GUI or IEMS client for the active unit

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

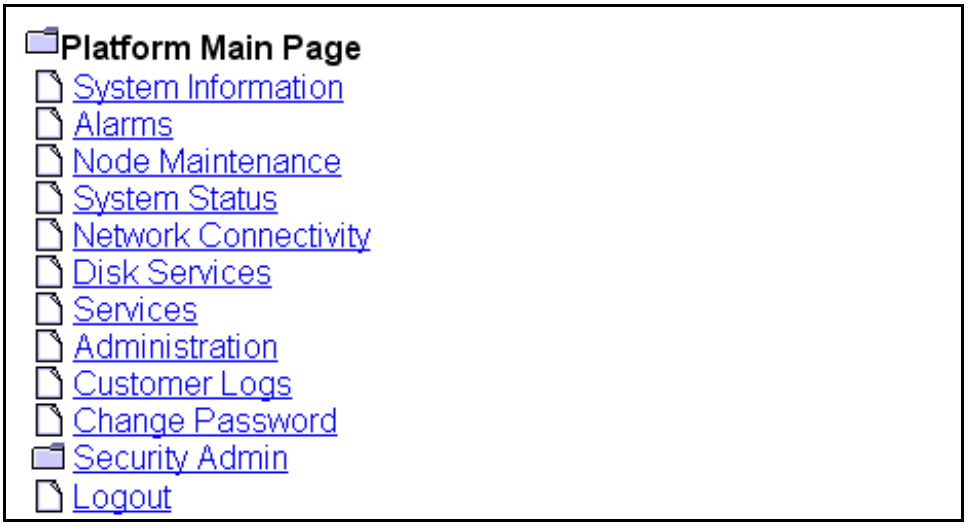
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

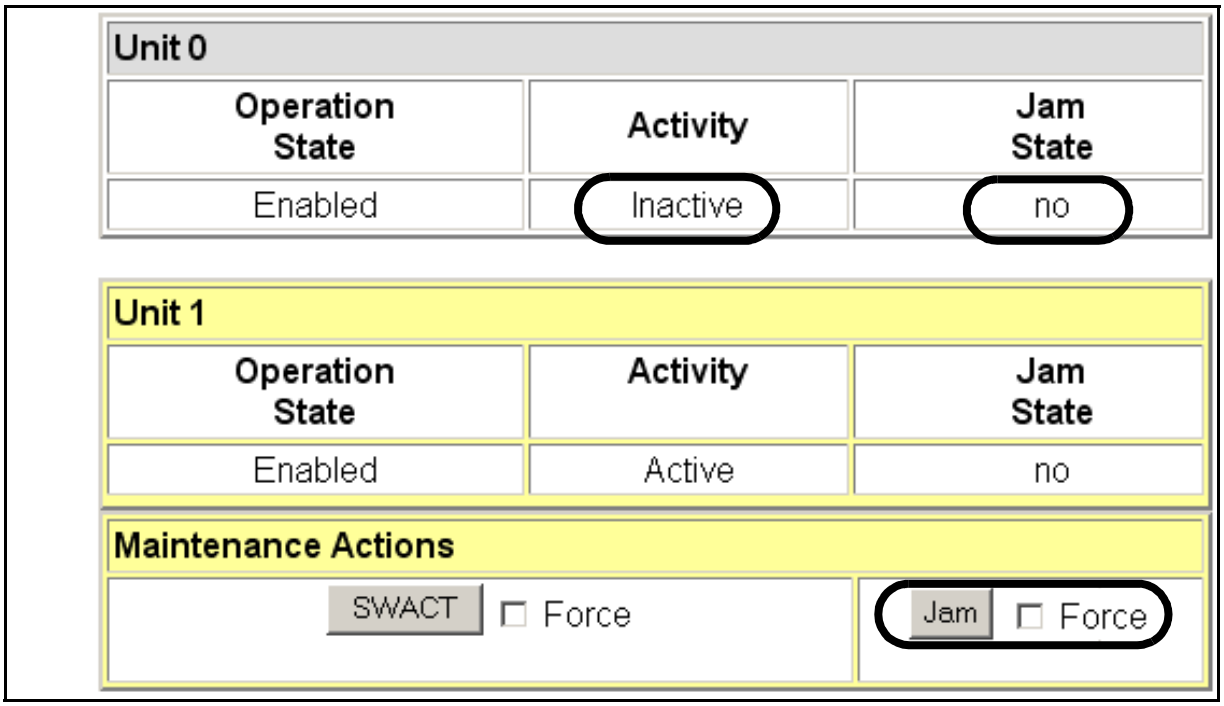
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Node Maintenance** link.

The Node Maintenance page is displayed.



3 Determine if the Jam State of the standby unit is Yes or No. If it is Yes, then the unit is already jammed and you are done with this procedure. If it is No, then continue with the next step.



Note: Refer to procedure Enable a system SwAct (Unjam) on page 1267 to unjam a standby Session Server unit.

4 Click the **Jam** button.

or

If you want to override any pre-Jam queries, first click the **Force** check box, then click the **Jam** button.

The system responds

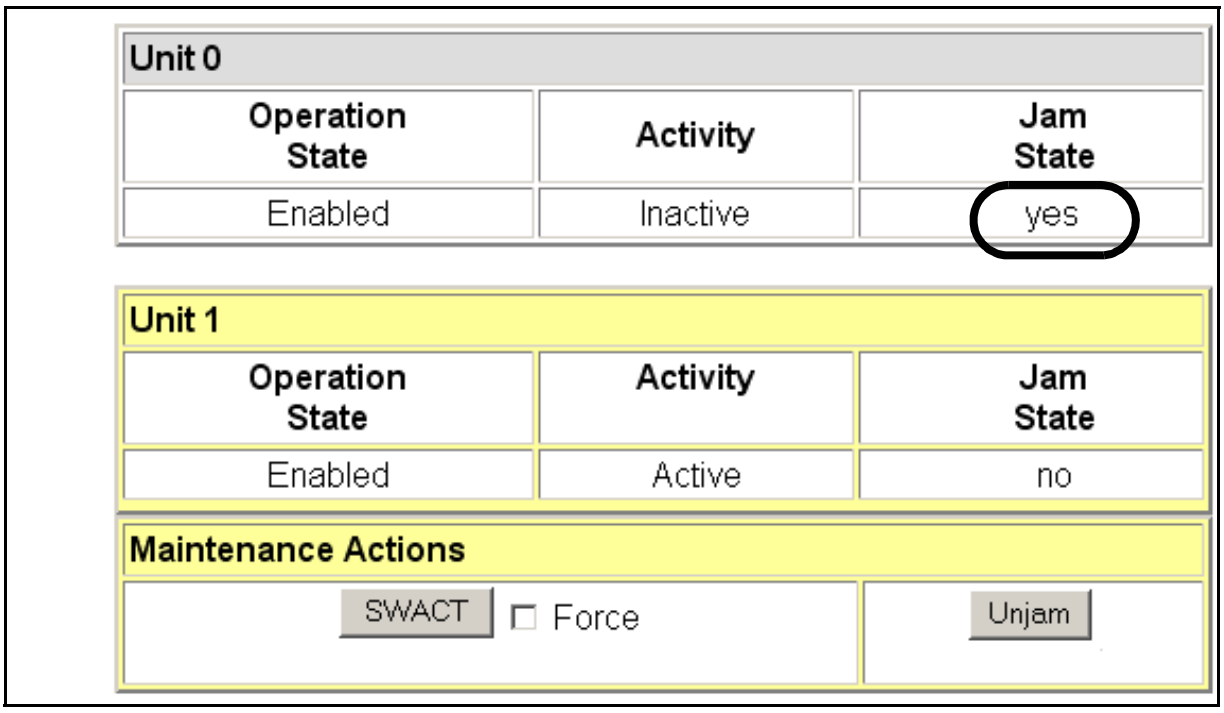
```
Are you sure you wish to perform jam action?

This will prevent the switch of activity to the
inactive node.
Click OK to confirm node jam or cancel to abort.
```

5 Click **OK** to proceed with the jam activity.

The system responds:

```
Info: Jam - Command passed.
```

6 Observe the Jam state for the standby Session Server unit transitions from No to Yes.



7 This procedure is complete.

To Jam or Force Jam?

The Jam action does not work if critical faults exist on the active unit. Using the Jam command with the Force option overrides any pre-checks. A Forced Jam forces a Jam of the inactive unit even if critical faults exist on the active unit, in which case, a full service outage could occur on the Session Server node if the active unit fails.

Upgrade Session Server NCGL platform software

Purpose of this procedure

This procedure describes how to use the CS 2000 NCGL Platform Manager GUI to apply a maintenance release or major release upgrade to an NCGL platform load.

ATTENTION

This procedure should only be used as part of the high level activity *Upgrading from a previous major release* or *Applying a maintenance release upgrade* in the Session Server Upgrades NTP, NN10349-461.

Limitations and Restrictions

You can upgrade the NCGL platform load from the local DVD-ROM drive, from an ISO image located on the system disk drive, or from a Session Server CD/DVD disk mounted elsewhere in the network (via FTP). The following upgrade protocols (methods) are selectable from the CS 2000 NCGL Platform Manager GUI:

- Local CDROM - the local DVD-ROM drive (labeled in the software as the local CD-ROM)
- Local file - an iso image, or load.tgz file copied from the local CD/DVD disk to the hard drive using the secure copy program, **scp**, to transfer the data
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the FTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in cleartext format across the network.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service.

Prerequisites

For the prerequisites of performing any upgrade, refer to section *Prepare for a maintenance release upgrade* or section *Prepare for a maintenance release upgrade* in the Session Server Upgrades NTP, NN10349-461.

Action

At the Session Server GUI or Integrated EMS client

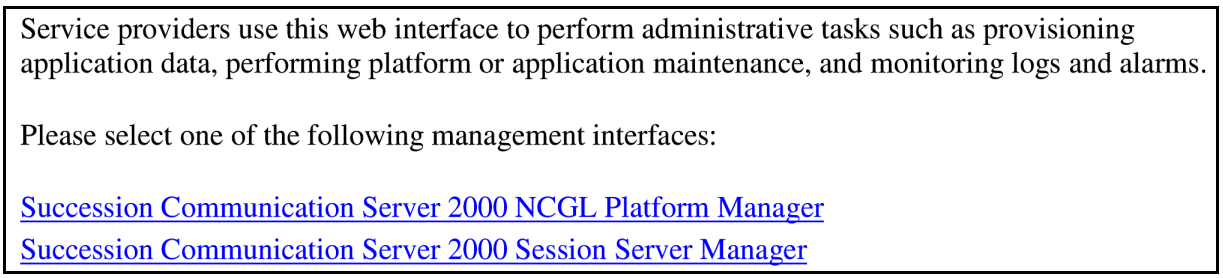
1 If software is delivered in CD/DVD, then insert the disk in the drive of the **inactive** unit now.

If software is delivered by ESD, ensure the image is mounted. Refer to Extract an ISO image from an Electronic Software Delivery (ESD) on page 1185 for assistance.

Note: If one unit has been upgraded and this procedure is being performed on the second unit, the ISO image does not need to be untarred. Perform only step 7 of Extract an ISO image from an Electronic Software Delivery (ESD) on page 1185 and return to this step.

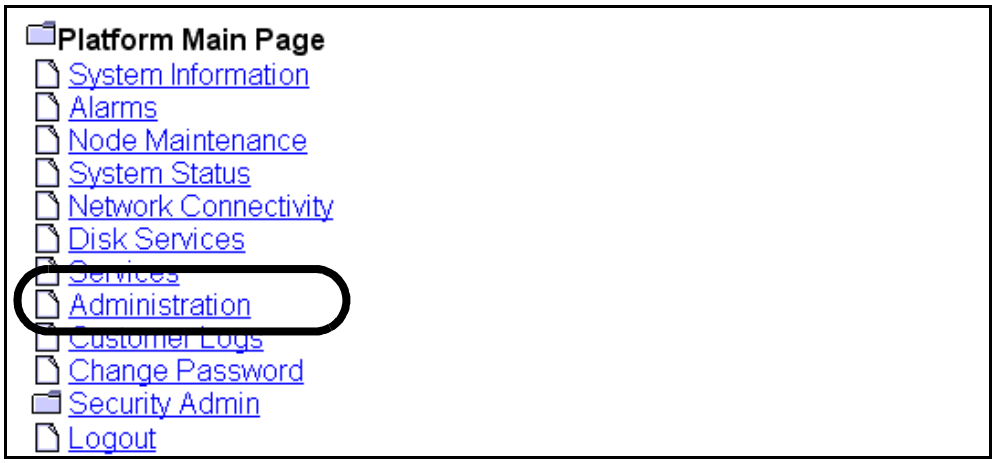
2 Select **Succession Communication Server 2000 NCGL Platform Manager** from the launch point menu.

Note: Access the **inactive** NCGL Platform Manager GUI using the IP address of the **inactive** NGSS unit.

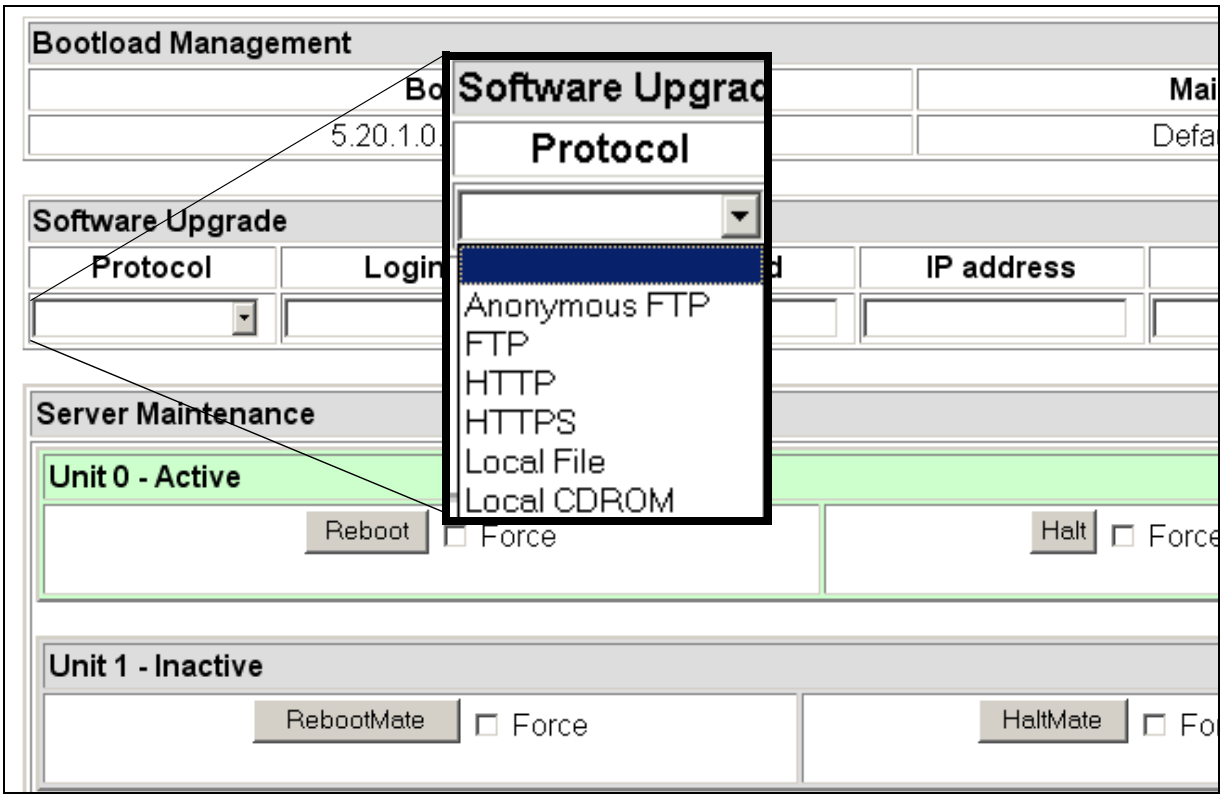


The Platform Main Page menu is displayed.

3 Click the **Administration** link.



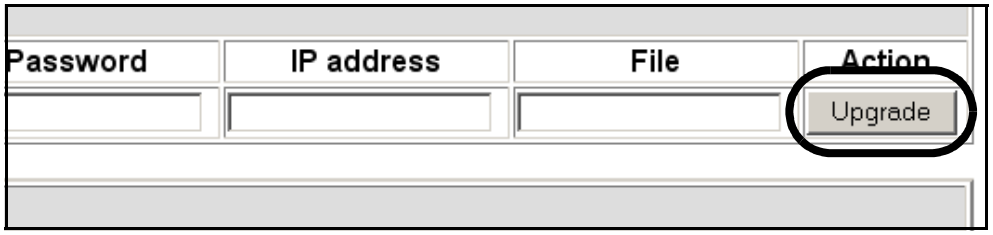
4 Click the **Protocol** drop down menu and select an upgrade protocol. Refer to the following table to help you determine the appropriate protocol:



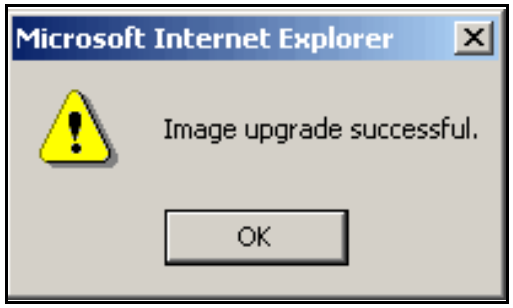
If the Protocol selection is	Do
Anonymous FTP	Enter the IP address of the remote server which has the bootload image in the IP address text box. Enter the location (as a relative path on the remote server) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 5
FTP	Enter your username in the Login ID text box. Enter your password in the Password text box. Enter the IP address of the remote server which has the bootload image in the IP address text box. Enter the location (as a relative path) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 5

If the Protocol selection is	Do
HTTP or HTTPS	Enter the IP address of the remote server which has the bootload image in the IP address text box. Enter the location (as a relative path on the remote server) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 5
Local File	If the ISO file is mounted, put in the local file and path as /cdrom/load.tgz instead of using /opt/swd/<load.iso> where the actual load name must be known. then continue with step 5
Local CDROM	Ensure that the CD/DVD disk is inserted into the drive then continue with step 5

5 Click the **Upgrade** button.



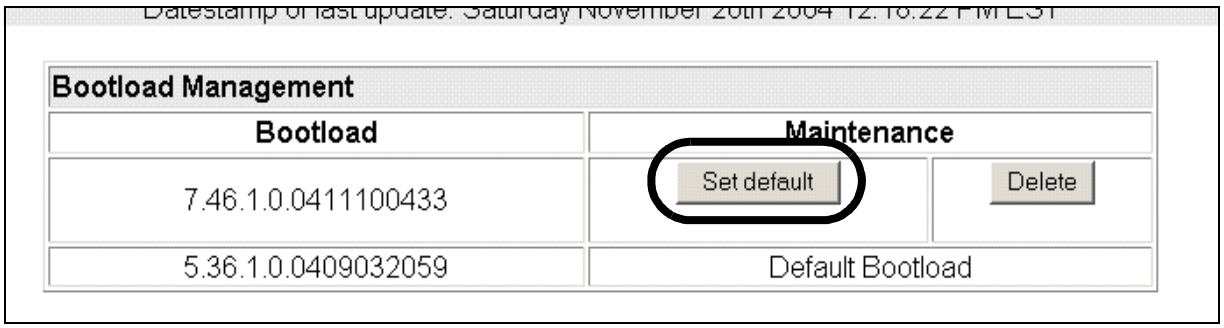
6 Verify that the load files were successfully copied by clicking **OK** on the popup window.



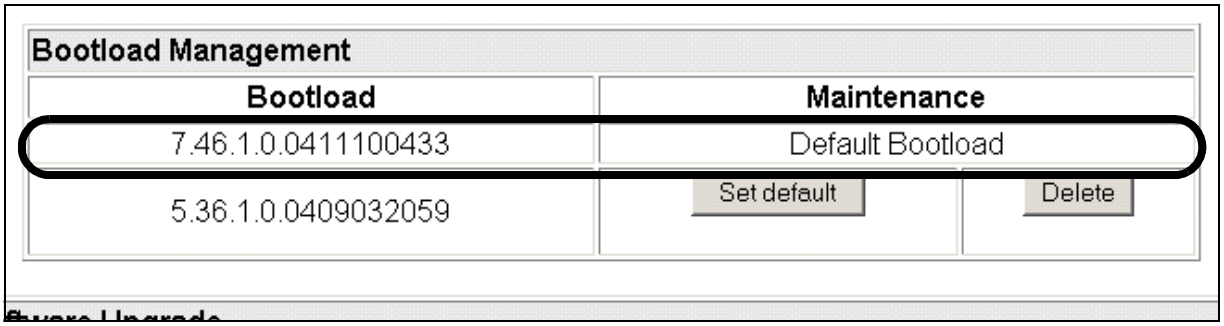
ATTENTION

Refer to the Troubleshooting Upgrades on page 1206 section if the popup window does not indicate a successful image upgrade.

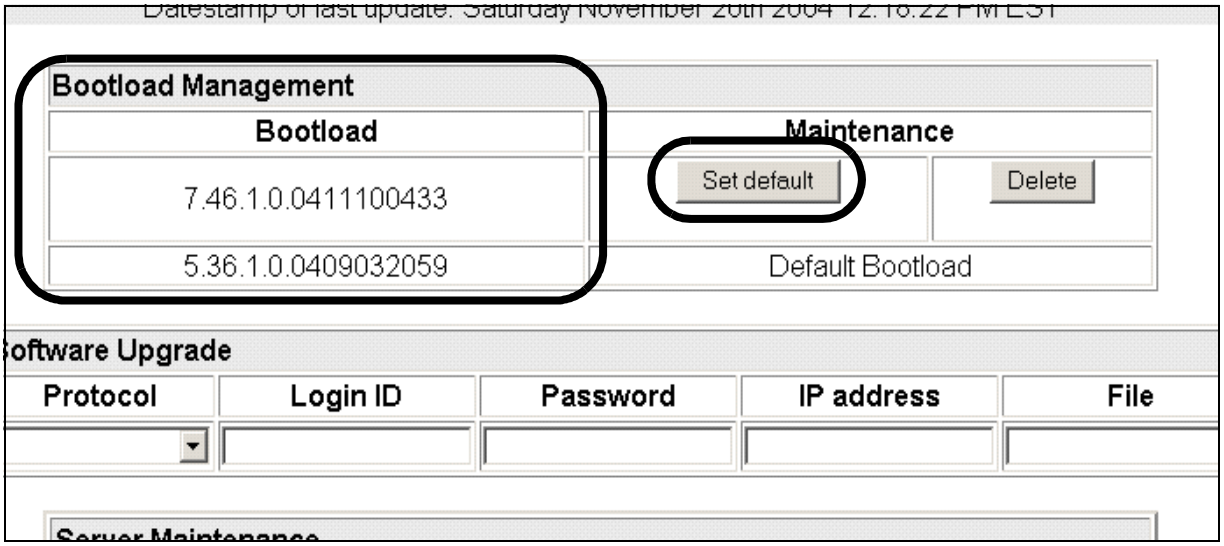
7 Click the **Set Default** button to the right of the new (upgraded) bootload.



The system responds by setting the newly installed load as the default load, as shown below.



8 Once the selected NCGL load has been successfully copied to the unit, look for the load number to appear in the Bootload Management panel.



9 Verify that you have set the correct bootload to be the default.

10 If you upgraded using the Local CD-ROM protocol, remove the CD/DVD disk from the drive.

11 You have completed this procedure. Return to the high-level activity *Prepare for a maintenance release upgrade* or section *Prepare for a maintenance release upgrade* in the Session Server Upgrades NTP, NN10349-461.

Troubleshooting Upgrades

For step 6 of this procedure, review the message in the popup window. The following possible error messages and their meaning are described:

- Error: Failed to update image /usr/bin/copy_boot_image -f /opt/swd/load.tgz Invalid load file content. Exiting

  Indication: If the bootload file is corrupt, the system software indicates that the bootload contains invalid content.

- Error: Failed to update image /usr/bin/copy_boot_image -u https://10.40.5.62//tmp/load.tgz: Failed to retrieve file from the network.

  Indication: The user has attempted to perform a software upgrade where the file path or the IP address used is not correct. You need to validate that the IP address is correct, also, make sure the file path is correct.

- Error: Failed to update image /usr/bin/copy_boot_image -u ftp://mtc:mtc@10.40.5.59//usr/load.tgz: Failed to retrieve file from the network.

  Indication: The user has attempted to perform a software upgrade where the file path or the user ID or password used is not correct. You need to validate that the file path is correct and make sure to check the user ID and password.

- Error: Failed to update image /usr/bin/copy_boot_image -u ftp://mtc:mtc@10.40.5.59//usr/load.tgz: 10.40.5.59 IP address is not responding.

  Indication: The user has attempted to perform a software upgrade from a host that is not responding. You need to check that the host IP address is available and try again.

- Error: Failed to update image /usr/bin/copy_boot_image -f load.tgz: Could not find load.tgz

  Indication: The user has attempted to perform a software upgrade where the file path is not correct. Validate that the file path is correct.

- Error: Failed to update image /usr/bin/copy_boot_image -c : Failed to mount the cdrom RC=32

Indication: If the CDROM is not placed in the CDROM drive and an attempt is made to upgrade software with the “Local CDROM” option, the above message appears. Verify that the CDROM is in the drive. If the CDROM is inserted, verify that the drive is functioning properly.

or

The user has attempted to perform a software upgrade where there is a problem with mounting the CD-ROM drive. Mount or remount the CD-ROM drive before attempting another software upgrade process.

- Error: Failed to update image /usr/bin/copy_boot_image -u https://10.40.5.62/load.tgz : Unable to decompress /opt/base/upgrade/29335/load.tgz Exiting

  Indication: The user has attempted to perform a software upgrade, which uses filesystem (/opt/base) that is full. You need to remove unwanted files and make sure there is enough space in the targeted filesystem.

Reboot a Session Server unit

Purpose of this procedure

Use this procedure to perform a graceful shutdown and reboot of the NCGL operating system running on a Session Server unit. Use this procedure only as part of a high-level activity such as maintenance or fault clearing activities or as part of a software upgrade activity.

ATTENTION

This procedure causes a 3-4 minute service interruption of the affected unit and should only be used when recommended by Nortel support personnel.

Limitations and Restrictions

ATTENTION

Nortel recommends performing this procedure only on the standby unit, however, this procedure can only be performed from the active Session Server unit.

CAUTION

This procedure halts all call processing activity and billing record generation on the affected unit and prevents the Session Server node from operating in a fault-tolerant mode.

Prerequisites

Use procedure View the operational status of a Session Server NCGL platform on page 1228 to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

Ensure that you have your bootable software installation CD/DVD disk available, in case you have trouble rebooting the unit.

Action

At the Session Server GUI or IEMS client for the active unit

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

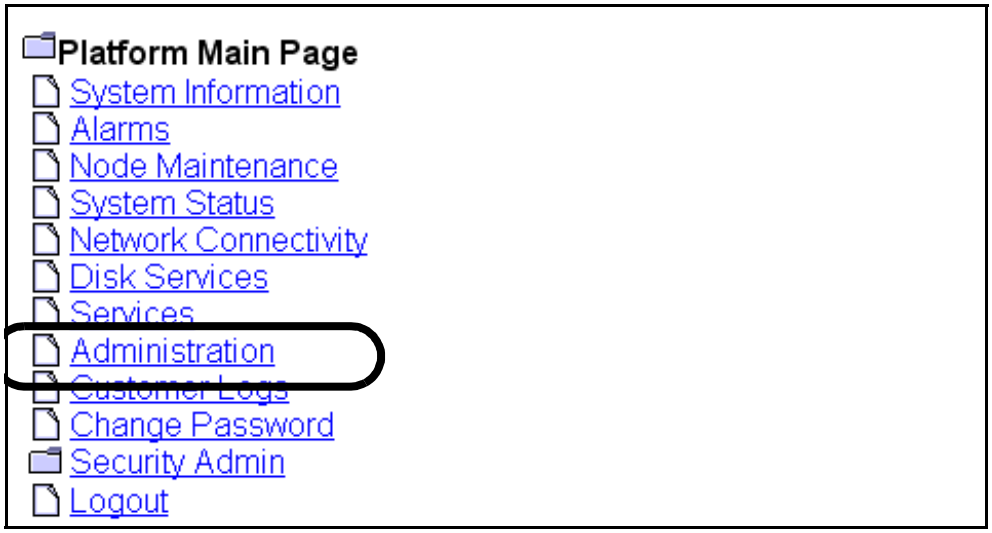
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

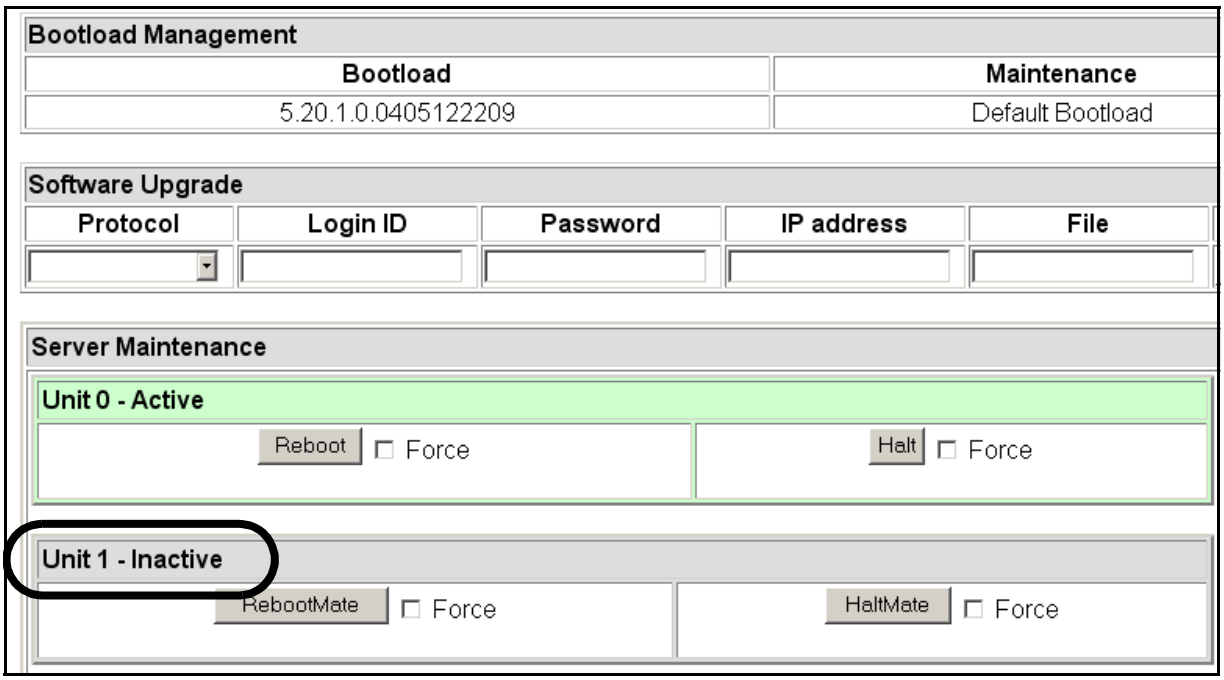
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Administration** link.

The Administration page is displayed.



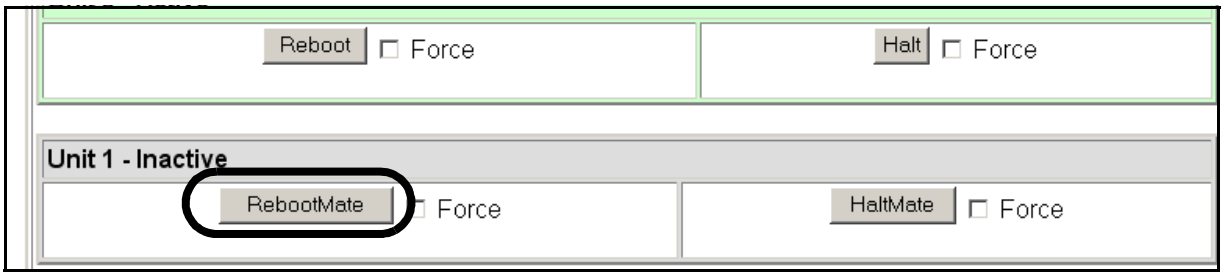
3 Review the status of the unit you want to reboot. If it is available, the **Reboot** or **RebootMate** buttons are accessible.



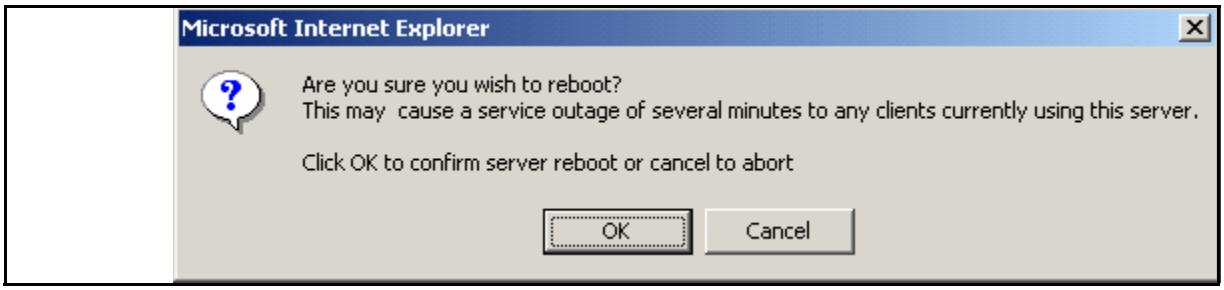
4 Reboot the Session Server unit indicated in the high-level activity that directed you to this procedure, using the corresponding **Reboot** or **RebootMate** button.

Note 1: If you want to override any pre-reboot queries including a pre-check by applications running on the unit, click the **Force** check box before clicking the **Reboot** or **RebootMate** button.

Note 2: In a system operating in fault-tolerant (duplex) mode, only the inactive unit can be rebooted using RebootMate or a Forced RebootMate. A Reboot or Forced Reboot can only be performed if the system is operating in simplex mode.

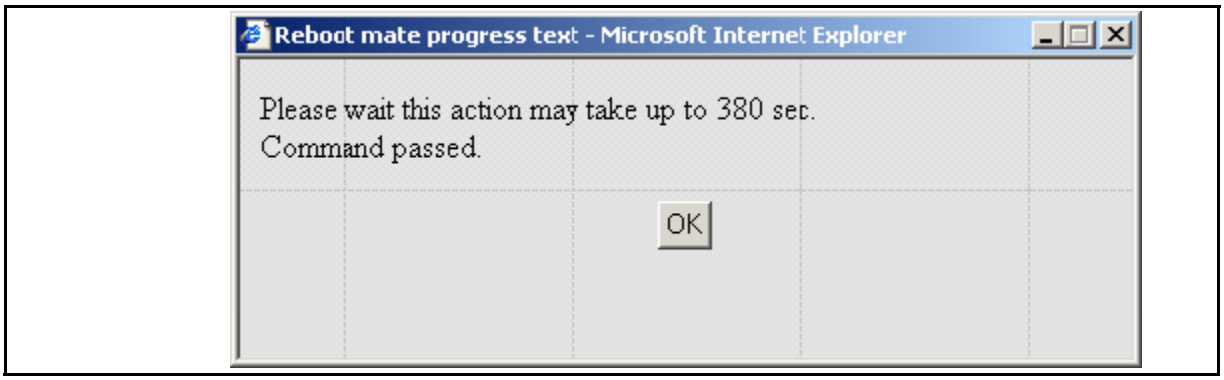


The system responds with the following message box:



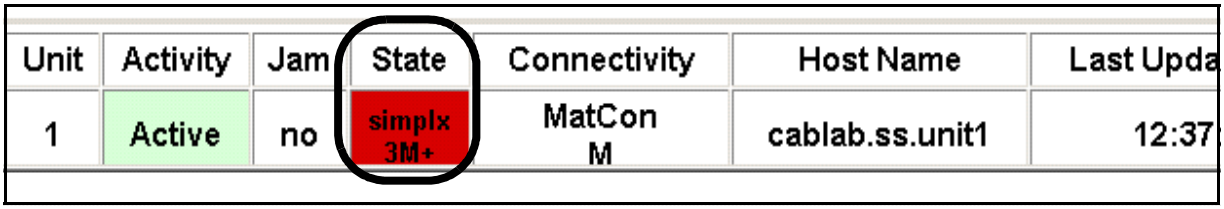
5 Click **OK** to confirm the reboot operation.

The NGCL and all call activity on the affected unit is shutdown and the unit begins to reboot. The system responds with the following message box:



6 Click **OK** to close the dialog box.

7 Monitor the recovery of the rebooting unit using procedure View the operational status of a Session Server NCGL platform on page 1228 to confirm the recovery of the unit after reboot. Continue monitoring the active unit until you see the State field in the alarm panel change back to duplex.



8 This procedure is complete.

Alternate command line interface (CLI) method

CAUTION

This procedure halts all call processing activity and billing record generation on the affected unit and prevents the Session Server node from operating in a fault-tolerant mode.

Halting the active unit will cause loss all call processing and billing generation for the entire Session Server node.

ATTENTION

All prerequisites and restrictions shown on page 1208 apply when using this procedure.

At Session Server CLI or Integrated EMS client

1 Log onto the active Session Server unit CLI and change to the root user.

2 Reboot the selected Session Server unit by typing

`# mtccli rebootmate` (to reboot the inactive unit)

or

`# mtccli reboot` (to reboot the active unit operating in simplex mode)

and pressing the **Enter** key.

3 Use procedure View the operational status of a Session Server NCGL platform on page 1228 to confirm the recovery of the unit after reboot.

4 You have completed this procedure.

Troubleshooting reboots

The following possible error messages received during a reboot attempt and their meaning are described:

Error: Command failed. Reason: Mate not available.
You must reboot the unit using the Alternate command line interface (CLI) method on page 1212.

Error: Reboot - Command rejected. Reason: Mate is available.
You have attempted to reboot the active server when the inactive server is available.

Error: Halt - Command rejected. Reason: Mate is available.
You have attempted to halt the active server when the inactive server is available.

Error: Command failed. Reason: PRECHECK FAILED: application rejected request.
The user has attempted a rebootmate or haltmate command and the application rejected the request. The user should check /var/log/designlog to determine the name of the application that rejected the maintenance command.

Actions:

- Using the Force option overcomes a pre-check failure by any application running on the unit.
- Try the operation again later. If the problem persists, then contact Nortel Networks support personnel for assistance.

Validate a certificate chain

Purpose of this procedure

This procedure uses the certificate management tool to validate a certificate chain. It is part of the process for provisioning a CA-signed certificates. This procedure should only be used as part of a high level task for creating or updating security certificates.

Limitations and restrictions

The private key that was generated by the certificate signing request must be the same private key currently stored in /opt/base/share/ssl. The certificate management tool will verify that the certificate provided as the user certificate matches the private key file server.key located in /opt/base/share/ssl.

Prerequisites

You must first complete procedure Prepare to validate a certificate chain on page 1177.

The following certificate files are required from a signing authority and must be located in the /opt/base/share/ssl directory to complete this procedure:

- Server.crt - contains the local certificate
- Trusted.crt - contains the CA chain in top down with the root CA at the top

The following restrictions apply to migrating CA-signed certificates:

- You must be a root user to use the certificate management tool.
- Only PEM formatted, CA-signed certificates are supported on Session Server.
- CA chain is required in PEM format in a trusted.crt file, top down with the root CA at the top
- This procedure cannot be performed on self-signed certificates. Migrating self-signed certificates is not supported. If your site uses self-signed certificates, you must create new ones during the upgrade activity.

Action

At the Session Server CLI or Integrated EMS client

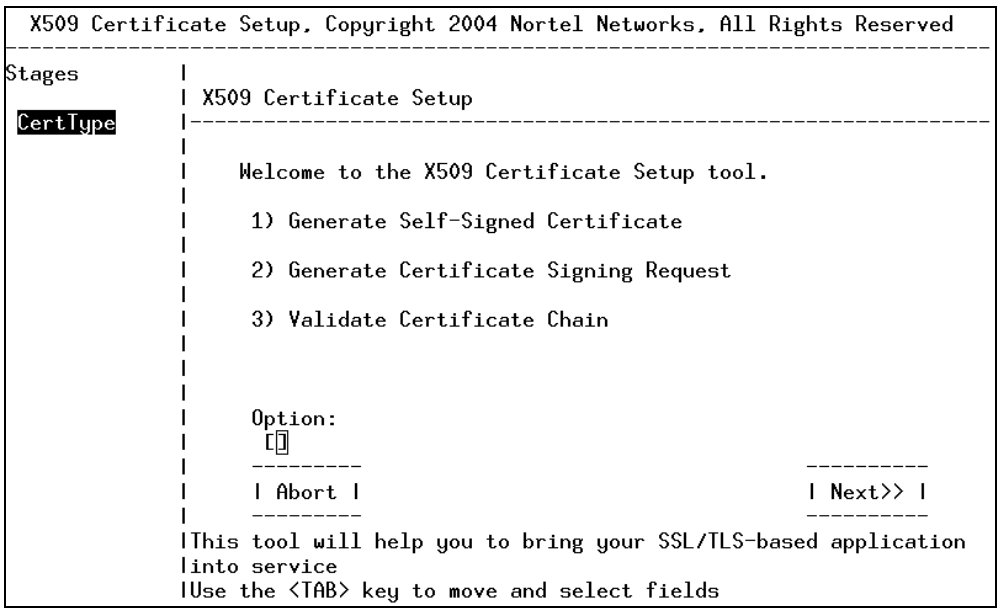
1 Complete procedure Prepare to validate a certificate chain on page 1177.

2 Log onto the standby Session Server unit and change to the root user.

3 Start the certificate management tool by typing

cert_mgnt

After a few seconds the Introduction screen is displayed.



4 Press **3** for the option to validate a certificate chain, position the cursor on the **Next** button and press **Enter**.

Note: In general, use the **Tab** key or the < and > keys to navigate between fields on the screen and use **Enter** to select a field or entry.

The configure CA-signed certificate screen appears.

```
 X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
------------------------------------------------------------------------------
Stages          |
                | Configure the Certificate Authority certificate filename
 CertType       |-----------------------------------------------------------
 CAFile         |
 CertFile       |    Please enter a CA certificate filename
 Summary        |
                |     [ ]
                |
                |
                |
                |
                |
                |
                |
                |     ----------                              ----------
                |     | <<Back |                              | Next>> |
                |     ----------                              ----------
                |
                | Use '<' and '>' keys to move if left and right arrows don't work
                |
```

5 Enter the full path and filename where the CA certificate can be found by typing

`/opt/base/share/ssl/trusted.crt`

position the cursor on the **Next** button and press **Enter**.

Note: The tool will not proceed unless the CA certificate trusted.crt file exists in the location specified.

The configure server certificate screen appears.

```
 X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
------------------------------------------------------------------------------
Stages          |
                | Configure the CA-signed certificate filename
 CertType       |-----------------------------------------------------------
 CAFile         |
 CertFile       |    Please enter the user certificate filename
 Summary        |
                |     [ ]
                |
                |
                |
                |
```

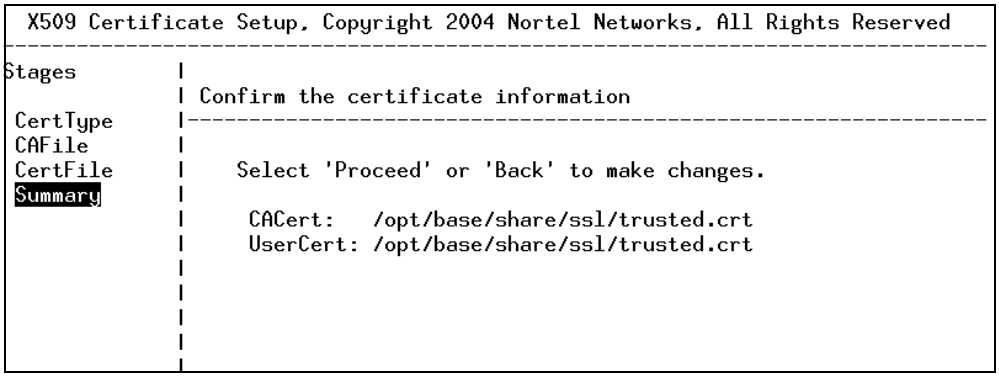
6 Enter the full path and filename where the server.crt certificate can be found by typing

`/opt/base/share/ssl/server.crt`

position the cursor on the **Next** button and press **Enter**.

Note: The tool will not proceed unless the server.crt file exists in the location specified.

The summary screen appears.



7 Review the information summary. Position the cursor on the **Proceed** button and press **Enter**, otherwise click **Back** to make revisions.

The tool validates the certificates chain and the trusted certificate files. Upon success, the tool displays the following:

```
Provisioning CA Certificate
Verifying certificate/key pair
spawn openssl verify -CAfile /opt/base/share/ssl/trusted.crt
/opt/base/share/ssl/server.crt
/opt/base/share/ssl/server.crt: OK
server.crt: OK
Certificate validation succeeded
Exporting certificate/key pair to PKCS#12 keystore
Certificate/key pair has been successfully exported to PKCS#12
format
Changing permissions on key file
Changing permissions on keystore file
```

8 The procedure is complete.

Troubleshooting

The private key in the server.key file must correspond to the certificate in the server.crt file for validation to be successful. If you require assistance with completing this procedure, please contact Nortel GNPS.

Generate self-signed security certificates

Purpose of this procedure

This procedure uses the certificate management tool to generate self-signed security certificates used for both Session Server units. This procedure should only be used as part of a high level task for updating security certificates.

A successful completion of this procedure creates a self-signed certificate composed of the following files:

- server.crt - contains the local certificate
- server.key -contains the private key corresponding to the local certificate
- trusted.crt - is an empty file if it did not already exist before the certificate management tool was run
- certificate.keystore - contains the private key and local certificate

Limitations and restrictions

You must be a root user to use the certificate management tool.

ATTENTION

The certificate management tool sets the appropriate file permissions for when the certificate files are generated. These file permissions should not be changed.

Prerequisites

Please read the complete disclaimer, found in section Self-signed certificate security disclaimer on page 1226.

Action

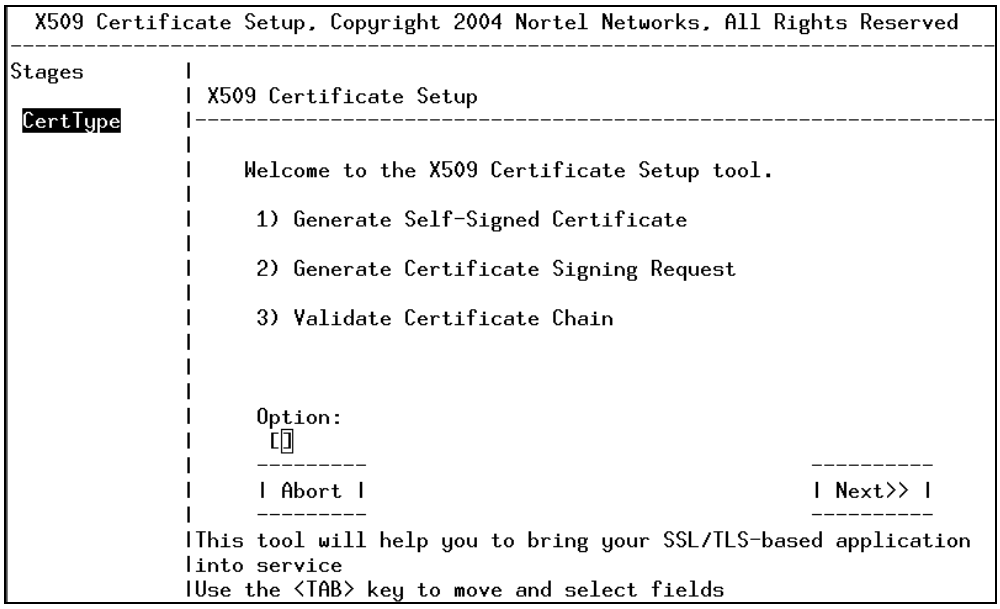
At the Session Server CLI or Integrated EMS client

1 Log onto the standby Session Server unit and change to the root user.

2 Start the certificate management tool by typing

`cert_mgnt`

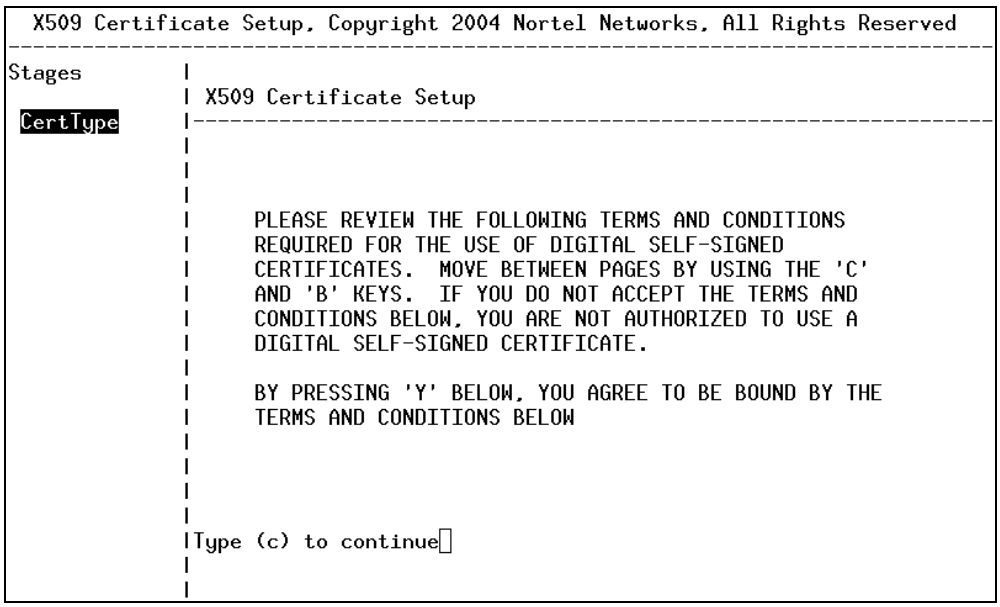
After a few seconds the Introduction screen is displayed.



3 Type **1** for the option to generate a self-signed certificate type, position the cursor on the **Next** button and press **Enter**.

Note: In general, use the **Tab** key or the < and > keys to navigate between fields on the screen and use **Enter** to select a field or entry.

A security disclaimer screen appears.

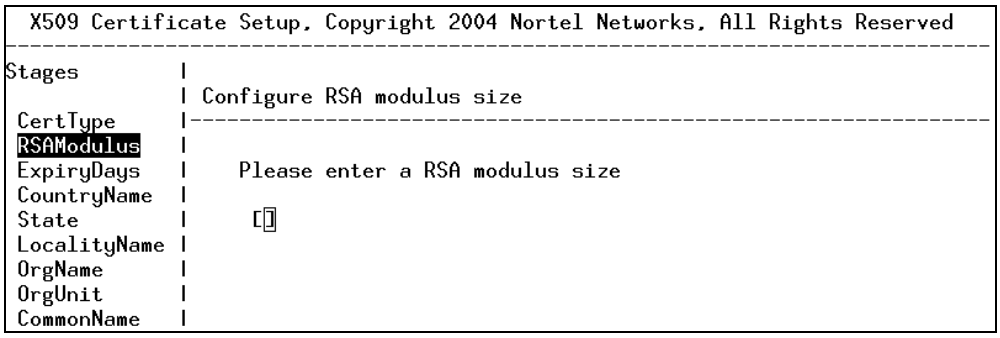


4 Carefully read the series of screens displaying the terms and conditions of the security certificate tool. Press **c** to continue to the next disclaimer page or press **b** to go back to the previous disclaimer page.

5 At the final disclaimer page, accept the terms and conditions of the security certificate tool by pressing **y**.

Otherwise you can reject the terms and conditions of the security disclaimer by pressing **n.** You are returned to the main menu.

The RSA modulus size screen appears.



6 Enter the RSA modulus (key) size, position the cursor on the **Next** button and press **Enter**. Supported values are 1024, 1536 or 2048 bits. (1024 is recommended)

Note: The larger the key size, the stronger the private key. There may be a performance impact when using larger key sizes.

7 Use the following table to determine your next step:

If	Do
you receive the message that the RSA private key already exists and you do not want to reuse the key	step 8
you receive the message that the RSA private key already exists and you want to reuse the key	Press **y** and skip to step 12
you do not receive any message that an RSA private key already exists	step 12

8 If you do not want to reuse the key, press **n**.

The system prompts that the RSA key is about to be deleted.

9 Use the following table to determine your next step:

If	Do
you do not want to delete the existing RSA key	Press **n** to abort the delete operation and go to step 10.
you are sure you want to proceed with deleting the existing RSA private key	Skip to step 11.

10 Press any key and return to step 6.

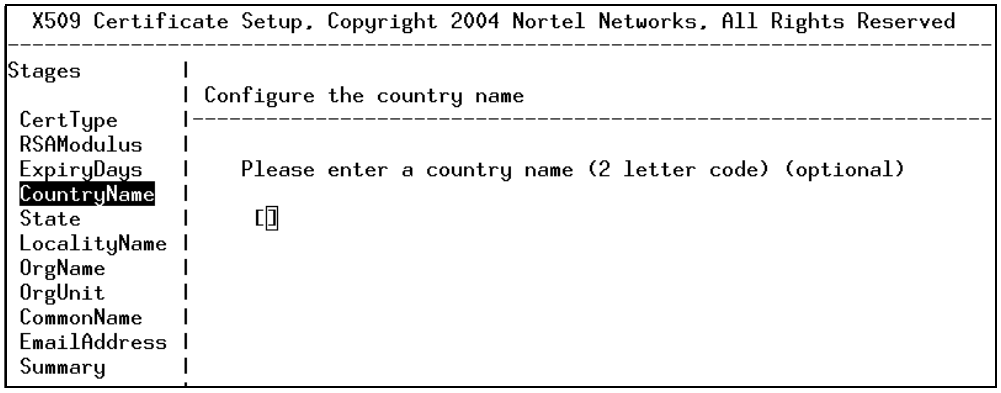
11 If you want to delete the existing RSA key, press **y**.

A backup of the existing key is made to a file in the same directory and a customer log is generated. The expiration configuration screen appears.

```
 X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Configure the certificate expiry days
 CertType       |-----------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Please enter a expiry days value
 CountryName    |
 State          |     [ ]
 LocalityName   |
```

12 At the certificate expiry days screen, enter the number of days you want the certificate to be valid, position the cursor on the **Next** button and press **Enter**. Supported expiration values range from 30 (30 days from the date of creation) to 7300 (20 years from the date of creation).

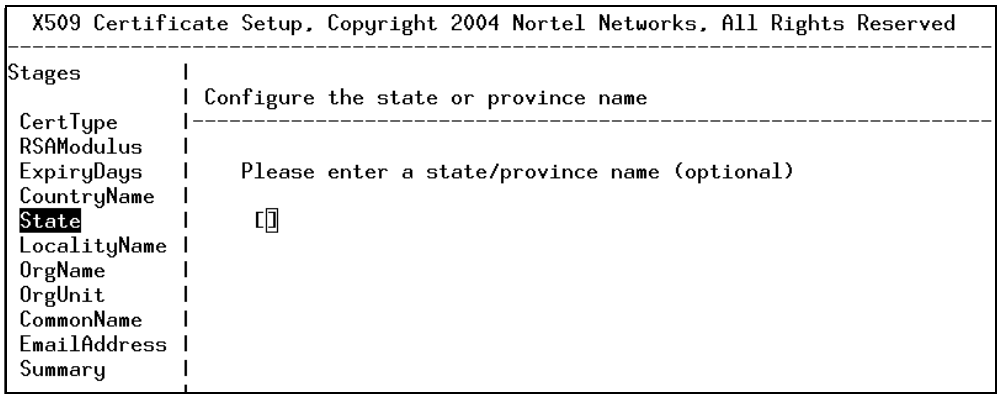
The country name configuration screen appears.



13 If applicable, enter the optional ISO 3166-1-alpha-2 two-letter country code, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

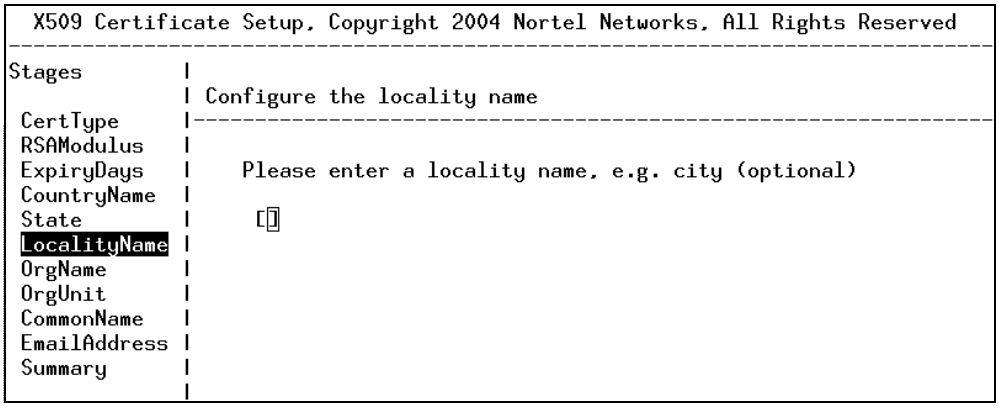
The state/province configuration screen appears.



14 If applicable, enter the optional state or province name, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

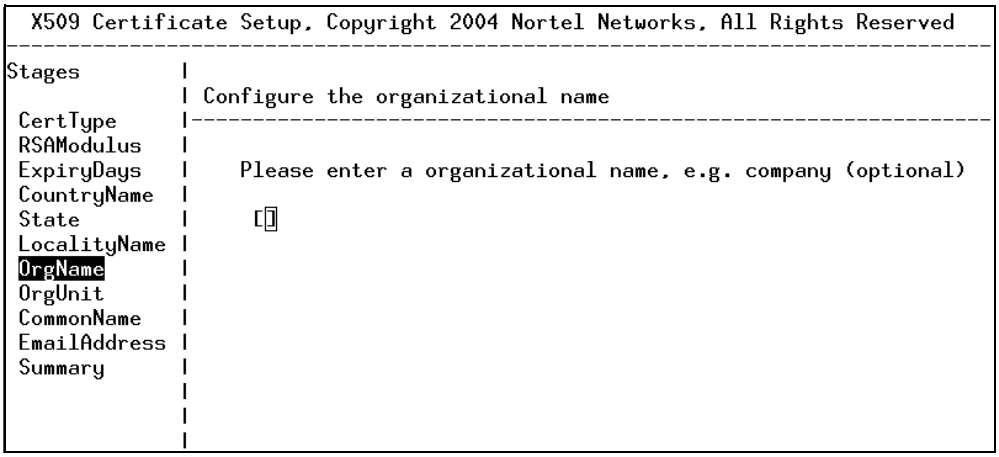
The locality configuration screen appears.



15 If applicable, enter the optional name of the locality or city, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

The organizational configuration screen appears.



16 If applicable, enter the optional name of the organization, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

The organizational unit configuration screen appears.

```
 X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Configure the organizational unit name (e.g. section)
 CertType       |----------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Please enter a organizational unit name (optional)
 CountryName    |
 State          |     []
 LocalityName   |
 OrgName        |
 OrgUnit        |
 CommonName     |
 EmailAddress   |
 Summary        |
                |
```

17 If applicable, enter the optional name of the organizational unit, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

The server common name configuration screen appears.

```
 X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Configure the server common name
 CertType       |----------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Please enter a common name for this certificate
 CountryName    |
 State          |     []
 LocalityName   |
 OrgName        |
 OrgUnit        |
 CommonName     |
 EmailAddress   |
 Summary        |
                |
                |
                |
```

18 Enter a common name for the Session Server node to which this certificate applies using one of the following methods:

- use the active IP address for the Session Server in the format: xxx.xxx.xxx.xxx
- use a hostname of up to 64 alphanumeric characters, with hyphens, underscores and periods allowed. The hostname used must be in FQDN (fully-qualified domain name) format. If you chose to use a host name, this same hostname must also be used as in the mgcHostName field when datafilling the SIP Gateway application configuration parameters. To datafill the mgcHostName, refer to procedure Configure SIP

Gateway application parameters, in NTP Session Server Configuration Management, NN10338-511.

Note: The common name value is used for mutual authentication between the Session Server and the remote application server. There is no validation of the common name at this stage of the configuration operation.

19 Position the cursor on the **Next** button and press **Enter**.

An email configuration screen appears.

```
 X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Configure an email address
 CertType       |----------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Please enter an email address (optional)
 CountryName    |
 State          |     [ ]
 LocalityName   |
 OrgName        |
 OrgUnit        |
 CommonName     |
 EmailAddress   |
 Summary        |
                |
                |
```

20 If applicable, enter the optional email address of the organization, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity. There is no validation of the email address.

A certificate summary information screen appears.

```
 X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Confirm the certificate information
 CertType       |----------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Select 'Proceed' or 'Back' to make changes.
 CountryName    |
 State          |     Modulus Size:   1024
 LocalityName   |     Expiry Days:    7300
 OrgName        |     Country Name:   CA
 OrgUnit        |     State/Province: Ontario
 CommonName     |     Locality Name:  Ottawa
 EmailAddress   |     Org. Name:
 Summary        |     Org. Unit:
                |     Common Name:    172.16.182.16
                |     Email Address:
```

21 Review the information summary. Position the cursor on the **Proceed** button and press **Enter**, otherwise click **Back** to make revisions.

The system responds by creating the security certificate:

```
Exporting certificate/key pair to PKCS#12
keystore
Certificate/key pair has been successfully
exported to PKCS#12 format
Changing permissions on key file
Changing permissions on keystore file
```

22 The procedure is complete.

Self-signed certificate security disclaimer

The following text contains the complete security disclaimer for using self-signed certificates. It is recommended that you read and understand this disclaimer before creating self-signed certificates.

“PLEASE REVIEW THE FOLLOWING TERMS AND CONDITIONS REQUIRED FOR THE USE OF DIGITAL SELF-SIGNED CERTIFICATES. MOVE BETWEEN PAGES BY USING THE 'C' AND 'B' KEYS. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS BELOW, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE.”;

“DISCLAIMER OF WARRANTY: THIS DIGITAL SELF-SIGNED CERTIFICATE IS PROVIDED BY NORTEL 'AS IS' AND NEITHER NORTEL NOR ANY OF ITS SUPPLIERS MAKE, AND SPECIFICALLY DISCLAIM, ANY AND ALL REPRESENTATIONS, WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, STATUTORY, ARISING BY USAGE OF TRADE OR OTHERWISE, INCLUDING WITHOUT LIMITATION, REPRESENTATIONS, WARRANTIES AND CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK OF THE USE OF ANY DIGITAL SELF-SIGNED CERTIFICATE SHALL BE BORNE SOLELY BY YOU.”;

“LIMITATION OF LIABILITY: IN NO EVENT SHALL NORTEL OR ANY OF ITS SUPPLIERS AND THEIR RESPECTIVE, EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS OR BUSINESS OPPORTUNITIES, LOSS OF GOODWILL, PROFITS OR DATA, BUSINESS INTERRUPTION, LOST SAVINGS OR OTHER SIMILAR PECUNIARY LOSS, ARISING FROM OR IN CONNECTION

WITH THE USE, PERFORMANCE OR NON-PERFORMANCE OF THE DIGITAL SELF-SIGNED CERTIFICATE, WHETHER ARISING IN LAW OR EQUITY, ARISING FROM CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE) OR ANY OTHER THEORY OF LIABILITY AND REGARDLESS OF WHETHER NORTEL OR ITS SUPPLIERS WERE AWARE OF THE POSSIBILITY THEREOF. BY ENTERING 'Y', YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS JUST REVIEWED. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS JUST REVIEWED, ENTER 'N' BELOW. IF YOU DO NOT ACCEPT THESE TERMS AND CONDITIONS, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE.";

View the operational status of a Session Server NCGL platform

Purpose of this procedure

Use the following procedure to view the service status of the Session Server platform hardware and NCGL operating system using the CS 2000 NCGL Platform Manager. This procedure may be used as a standalone task or as part of a high-level activity.

Limitations and restrictions

This procedure provides instructions for determining the service status of the Session Server NCGL platform only. For instructions on determining the status of the SIP Gateway application, refer to procedure *View the operational status of the SIP Gateway application* in the Session Server Configuration Management NTP, NN10338-511.

Although some activities described in this procedure can be accomplished using the CS 2000 Session Server Manager, they are described instead using the more complete CS 2000 NGCL Platform Manager.

This procedure does not describe how to change platform or NCGL settings such as changing BIOS settings or platform provisioning. Refer to the appropriate procedures in the Session Server Configuration Management NTP, NN10338-511, for changing these settings.

This procedure does not describe how to view customer logs or alarms or how to change the root password. For detailed instructions on viewing customer logs or alarms, refer to procedures in the Session Server Fault Management NTP, NN10332-911. For instructions on how to change the platform root password, refer to the Session Server Security and Administration NTP, NN10346-611.

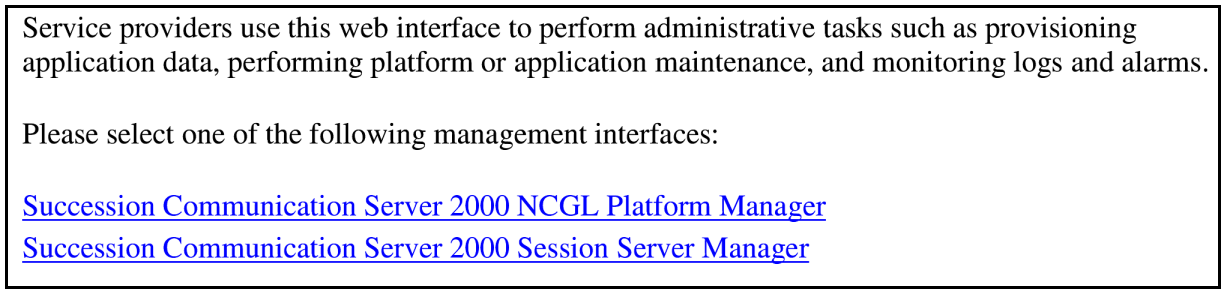
Prerequisites

There are no prerequisites for using this procedure.

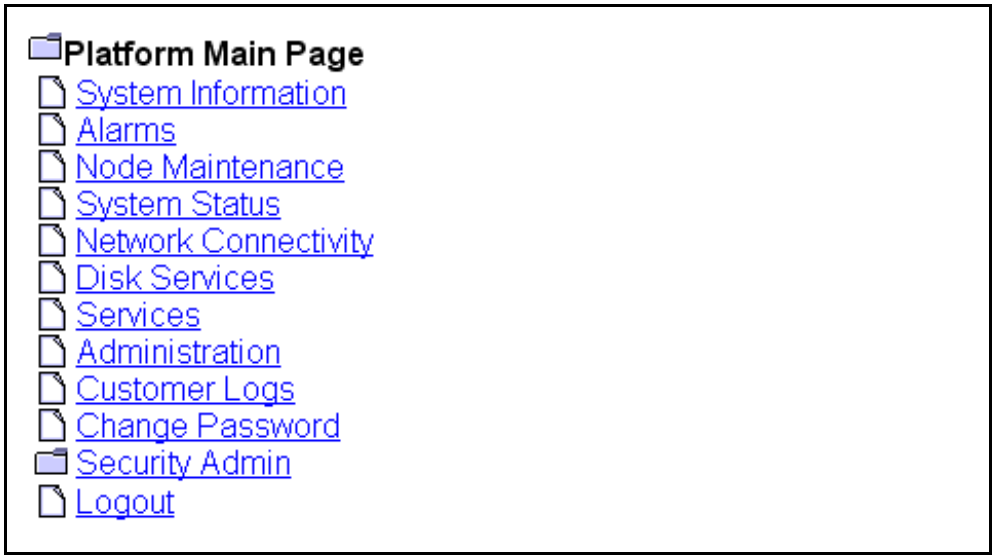
Action

At the Session Server GUI or Integrated EMS client

1 Select **Succession Communication Server 2000 NCGL Platform Manager** from the launch point menu.



The Platform Main Page menu is displayed.



2 Use the following table to determine your next step:

If	Do
you want to review the version of the platform software load, boot statistics and platform IP address	Click the **System Information** link and go to step 3.
you want to review existing platform alarms	Skip to step 17 and go to procedure *View Session Server alarms* in the Session Server Fault Management NTP, NN10332-911.
you want to review node maintenance status	Click the **Node Maintenance** link and go to step 5.

If	Do
you want to review the status of system processes, CPU load and memory or related alarm thresholds	Click the **System Status** link and go to step 7.
you want to review the connectivity status of the network links. To perform link management activities, refer to the Session Server Security and Administration NTP, NN10346-611	Click the **Network Connectivity** link and go to step 9.
you want to review storage related information including array status, disk capacity and disk alarm thresholds	Click the **Disk Services** link and go to step 10.
you want to review details about platform services including the network time protocol servers	Click the **Services** link and go to step 12.
you want to review platform version information only	Click the **Administration** link and go to step 14.
you want to review customer logs	Skip to step 17 and go to procedure *View Session Server logs* in the Session Server Fault Management NTP, NN10332-911.
you want to change root passwords	Skip to step 17 and go to procedure *Manage user passwords with the Session Server GUI* in the Session Server Security and Administration NTP, NN10346-611.
you want to view TLS security information or manage security certificates	Skip to step 17 and refer to the Session Server Security and Administration NTP, NN10346-611 to manage security certificates. Refer to the Session Server Configuration Management NTP, NN10338-511 to review TLS security settings.
you are finished reviewing information and want to logout from the GUI	step 16.

3 Review the system information page and use the following table to review the description of the various fields of the Platform (System) Information page:

Note: The Platform (System) Information panel does not update automatically. Click the **System Information** link again to update it.

Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
0	Active	no	.	.	sp2k-1	07:57:32

The Platform Information panel does not update automatically!
Datestamp of last update: Thursday June 10th 2004 06:58:07 PM EST

Platform Information	
Date:	Thursday June 10th 2004 06:58:07 PM EST
Time since last reboot:	2 days, 7 hours, 58 minutes, 11 seconds
System Power-On Time:	0 years 189 days 11 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to soft reset
Last power event cause:	Last power down caused by loss of power feed.
Current version:	5.20.1.0.0405122209
Platform IP Address:	47.174.74.184
Platform EM Client IP Address:	47.102.176.118
Server Location:	RTP
Host Name:	sp2k-1

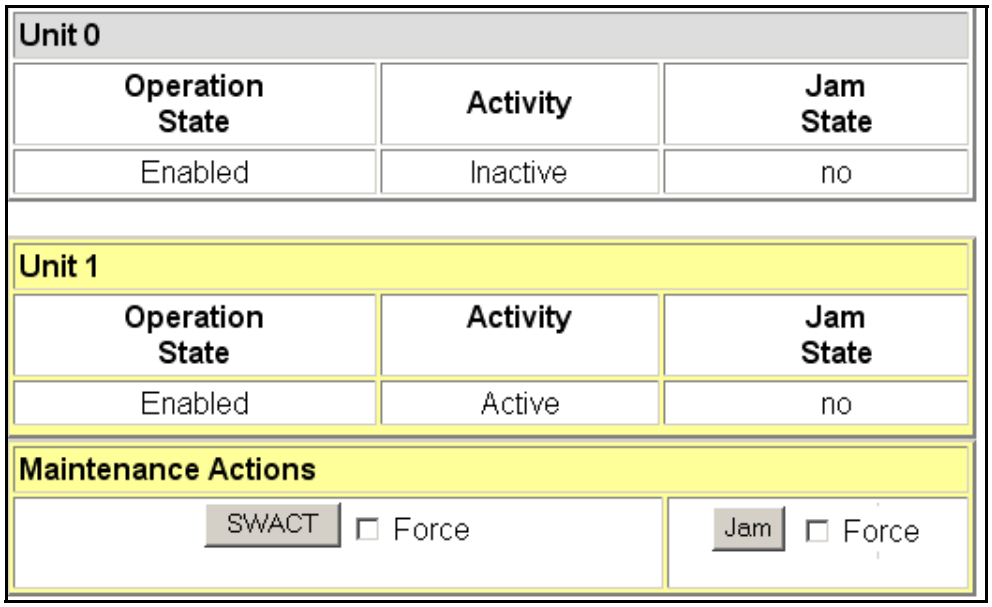
Field	Description
Unit	The unit number in the node that you are logged into.
Activity	Indicates the activity of the unit (either active or standby).
Jam	Indicates if an activity Jam has occurred on the active Session Server unit. This prevents the standby unit from becoming active, regardless of any failures on the active unit.

Field	Description
State	Indicates if the Session Server node is operating in a duplex (fault-tolerant) mode or a simplex mode (the standby unit is off-line).
Connectivity	Indicates the state of the network links on the node.
Host Name	Indicates the name of the Session Server unit (not node).
Date	Indicates the system date as maintained by the network time protocol (NTP) server.
Time since last reboot:	Indicates the amount of time that has elapsed since the Session Server was last rebooted for any reason.
System Power-On Time:	Indicates the recorded system time that the Session Server has been powered up.
System booted from:	Indicates whether the Session Server is currently booted from the hard drive, or DVD-ROM drive.
Last restart cause:	Indicates any event that forced a platform reboot (manual or system generated).
Last power event cause:	Indicates any event that affected the power supply subsystem of the unit chassis.
Current version:	Indicates the installed version of the Session Server platform software. (Does not include the SIP Gateway application or other co-resident applications.) Refer to the Session Server Upgrades NTP, NN10349-461, for more procedures on acquiring version information.
Platform IP Address:	Indicates the IP address of the Session Server platform.
Platform EM Client IP Address:	Indicates the IP address of the Session Server client web interface. This is the IP address of the PC or Unix client from which the GUI was launched. When a web proxy is used, the IP address is the SSPFS proxy IP address.
Server Location:	Indicates the physical location of the Session Server.
Host Name:	Indicates the name of the Session Server unit.

4 When you have completed reviewing System Information page, return to step 2.

5 Review the Node Maintenance page and use the following table to review the description of the various fields of the Node Maintenance page:

Note: The Node Maintenance panel is refreshed every 45 seconds.



Field	Description
Operation State (unit 0 or 1)	Indicates the operational state of the platform software.
Activity (unit 0 or 1)	Indicates the activity state of the platform software.
Jam State (active unit only)	Indicates whether or not an activity jam has been requested.
Maintenance Actions (active unit only)	Maintenance panel for performing node SwAct activity and to unjam node activity. Refer to the Session Server Security and Administration NTP, NN10346-611, for procedures on performing a SwAct or Jam/unJam of the active unit.

6 When you have completed reviewing the Node Maintenance page, return to step 2.

7 Review the System Status page and use the following table to review the descriptions of the various fields of the System Status page:

Note: The Chassis Information panel is not automatically refreshed.

Chassis Information

Self Test	Chassis Subsystems
Self tests passed.	Chassis subsystems OK.

CPU Load

1 min. load average	5 mins. load average	15 mins. load average	Minor alarm threshold 1 min.	Major alarm threshold 1 min.	Critical alarm threshold 1 min.
0.02	0.01	0.00	10.00	20.00	40.00

CPU Utilization

5 mins. Utilization average	20 mins. Utilization average	30 mins. Utilization average	Minor alarm threshold 5 min.	Major alarm threshold 20 min.	Critical alarm threshold 30 min.
0.77	0.62	0.62	95.00%	99.00%	99.00%

Process Information

Number of processes	Number of zombie process(es)	Zombie		
		Minor alarm threshold value	Major alarm threshold value	Critical alarm threshold value
165	0	5	10	15

Memory Information

Total memory (MB)	Free memory (MB)	Available memory (MB)	Minor alarm threshold value (MB)	Major alarm threshold value (MB)	Critical alarm threshold value (MB)
3,787.31	2,951.86	3,539.29	500.00	250.00	100.00

Field	Description
Chassis information: Self Test	Indicates the status of the self test performed on the platform at boot up.
Chassis information: Chassis Subsystems	Indicates the status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections.
CPU Information: load average	Indicates the 1, 5 and 15 minute load averages for the CPU utilization.
CPU information: load average threshold values	Indicates the 1 minute CPU load average utilization threshold value. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.
Chassis Utilization: Utilization average	Indicates the 5, 20 and 30 minute CPU utilization average. When the threshold value is exceeded, an alarm is raised.
Chassis Utilization: alarm threshold values	Indicates the 5, 20 and 30 minute CPU utilization average threshold value. When the set threshold value is exceeded, an alarm is raised.
Process Information: Number of Processes	Indicates the total number of processes (non-threaded) that are running on the Session Server Platform.
Process Information: Number of zombie processes	Indicates the number of defunct or terminated NCGL zombie processes. ***Note:*** A zombie process is a process that has terminated either because it has been killed by a signal or because it has called an exit() and whose parent process has not yet received notification of its termination. A zombie process exists solely as a process table entry and consumes no other resources.
Process Information-zombie: minor alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a minor alarm is raised indicating that the set threshold has been exceeded.

Field	Description
Process Information-zombie: major alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a major alarm is raised indicating that the set threshold has been exceeded.
Process Information-zombie: critical alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a critical alarm is raised indicating that the set threshold has been exceeded.
Memory Information: Total Memory (MB)	The total amount of RAM installed on the motherboard of each Session Server unit. Both units must have the same amount.
Memory Information: Free Memory (MB)	The amount of memory available unallocated for use.
Memory Information: Available memory (MB)	The amount of memory available for programs.
Memory Information: minor alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a minor alarm is raised.
Memory Information: major alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a major alarm is raised.
Memory Information: critical alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a critical alarm is raised.

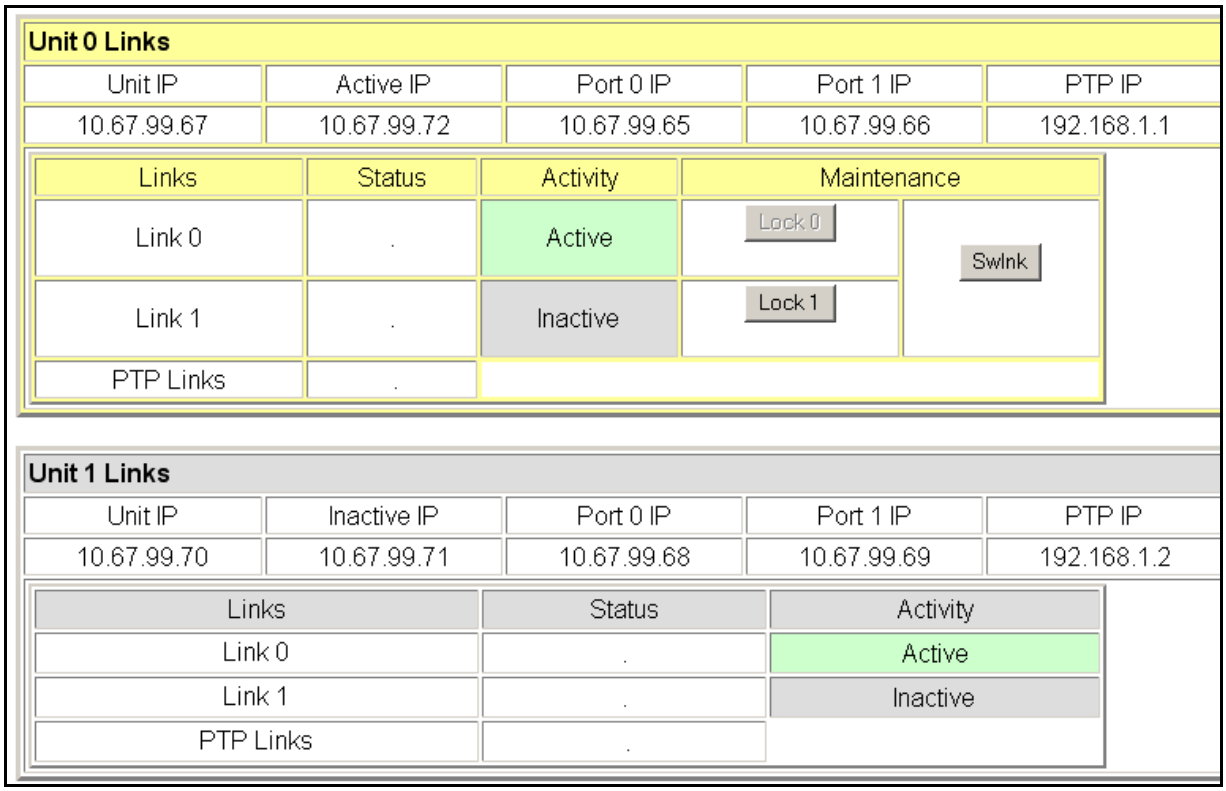
8 When you have completed reviewing the System Status, return to step 2.

9 Review the Network Connectivity page and use the following table to review the description of the various fields of the Network Connectivity page:

ATTENTION

Do not perform link management activities such as Lock, Suspend or Swlink using this procedure. Refer to the Session Server Security and Administration NTP, NN10346-611, to perform these activities.

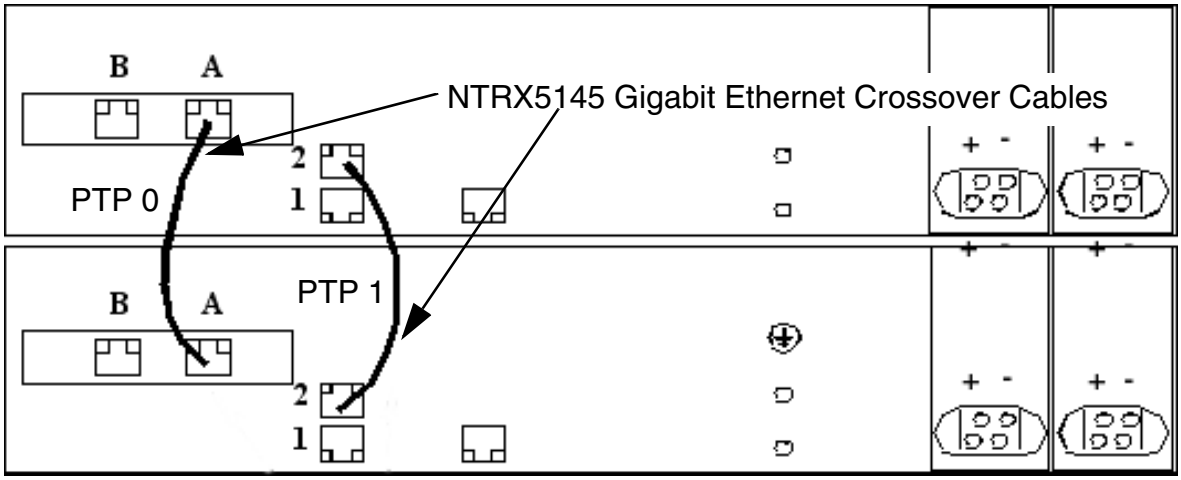
Note: The Network Connectivity panel is refreshed every 45 seconds.



Field	Description
Unit 0,1 Links	Indicates which ethernet IP links are installed on the Session Server units (each unit has two links).
Unit 0,1 Status	Indicates the status of the ethernet links.

Field	Description
Unit 0,1 Activity	Indicates the activity status of the ethernet links; either active or inactive.
Unit 0,1 Maintenance	Indicates the maintenance actions that can be performed on the ethernet links; either Lock, Unlock or Swlink. Refer to the Session Server Security and Administration NTP, NN10346-611, to perform link management.
Unit 0,1 PTP Links status	Indicates the status of the PTP links between both units in the node.
Unit IP	The network IP address of the Session Server unit.
Active IP	The IP address of the local (active) Session Server unit.
Inactive IP	The IP address of the mate (inactive) Session Server unit.
Port 0 IP	The IP address of the active or inactive ethernet port 0.
Port 1 IP	The IP address of the active or inactive ethernet port 1.
PTP IP	The IP address of the active or inactive PTP link.

Crossover and LAN ethernet cable connections for Session Server units



Ethernet Ports:

Ports 1 and B (both sets) go to CS-LAN Switch

Ports 2 (PTP1) and A (PTP0) are point-to-point connections between Session Server units

10 Review the Disk Services page and use the following table to review the description of the various fields of the Disk Storage page:

Note 1: The Disk Services panel does not update automatically. Click the **Disk Services** link again to update it.

Note 2: To create and remove file systems, refer to applicable procedures in the Session Server Configuration Management NTP, NN10338-511.

RAID Array Status

Name	Size (GB)	State	Disk 0	Disk 1	Status
/boot	0.10	.	.	.	Array is operating normally
ntvg	68.26	.	.	.	Array is operating normally

Disk Maintenance

Disk Number	Disk Size (GB)	Disk State	Disk Action
0	68.37	.	Remove
1	68.37	.	Remove

Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)	Total Space Available (%)	Minor Alarm Threshold (%)	Major Alarm Threshold (%)	Critical Alarm Threshold (%)
	/	.	61.47	58.29	100.00	0.00	0.00	85.00	90.00	95.00
No	/boot	.	98.65	19.08	21.00	74.48	79.00	-	-	-
Yes	/opt/base	.	699.31	0.46	1.00	698.85	99.00	85.00	90.00	95.00
No	/opt/apps	.	507.31	314.31	62.00	193.00	38.00	-	-	-
Yes	/tmp	.	123.31	0.31	1.00	123.00	99.00	85.00	90.00	95.00
Yes	/var/log	.	507.31	9.61	2.00	497.71	98.00	85.00	90.00	95.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00	-	-	-
No	/opt/apps/webint	.	1,494.00	209.78	15.00	1,284.22	85.00	-	-	-
No	/opt/apps/database	.	10,006.00	48.19	1.00	9,957.81	99.00	-	-	-
No	/opt/apps/logs	.	507.31	206.34	41.00	300.98	59.00	-	-	-
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00	-	-	-

Create/Remove Filesystem

Create New Filesystem | Remove Filesystem

Volume Group Information

Volume Group Name	Volume Group Size (GB)	Total Space Allocated (GB)	Total Space Allocated (%)	Total Space Available (GB)	Total Space Available (%)
ntvg	68.22	23.84	34.95	44.38	65.05

Field	Description
RAID Array Status: Name	Indicates the name of each RAID-1 array in the system.
RAID Array Status: Size (GB)	Indicates the size of the partition in gigabytes.

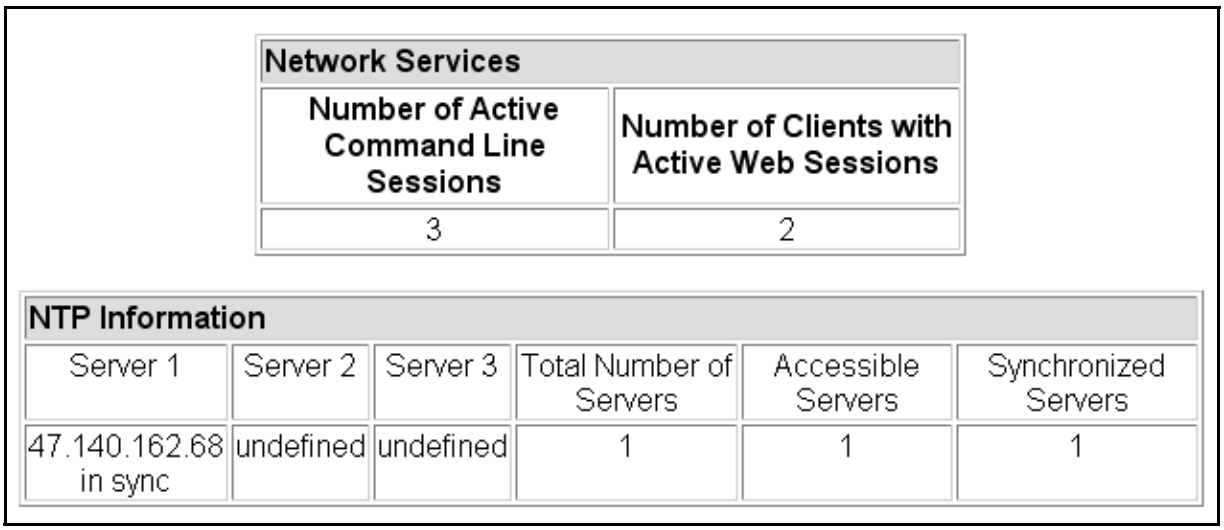
Field	Description
RAID Array Status: State	Indicates a high level state for the array: - ".": indicates the array is functioning normally. - Missing: a disk was removed from the array. - Failed: a disk in the array has failed and needs to be replaced. - Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.
RAID Array Status: Disk 0	Indicates the service status of disk 0.
RAID Array Status: Disk 1	Indicates the service status of disk 1.
RAID Array Status: Status	Indicates the status of the array. Values are: - The array is operating normally - Missing - Failed - Rebuild.
Disk Maintenance: Disk Number	Indicates the disk number in the array; 0 or 1.
Disk Maintenance: Disk Size (GB)	Indicates the total capacity of the disk drive in gigabytes.
Disk Maintenance: Disk State	Indicates the installation state of the disk.
Disk Maintenance: Disk Action	Indicates whether a hard disk can be inserted into the operating system. For more information about the **Remove** and **Insert** commands, refer to the Session Server Upgrades NTP, NN10349-461.
Filesystem Information: Monitor	Indicates the status of individual filesystems on the disk array. For more information about the **Monitor** command, refer to procedures in the Configuration Management NTP, NN10338-511.
Filesystem Information: Filesystem Name	Indicates the name of the filesystem on the disk array. Some filesystem names are reserved.
Filesystem Information: Test Results	Indicates the results of any tests run on the filesystems. Tests are run approximately every 10 minutes to verify that all of the basic filesystem operations are working on each of the filesystems.
Filesystem Information: Total Space (MB)	Indicates the total amount of disk space (in MB) allocated for this filesystem.

Field	Description
Filesystem Information: Total Space Used (MB)	Indicates the total amount of disk space (in MB) in use on this file system.
Filesystem Information: Total Space Used (%)	Indicates the total amount of disk space (in %) in use on this file system.
Filesystem Information: Total Space Available (MB)	Indicates the percent of total disk space (in MB) free for use on this filesystem.
Filesystem Information: Total Space Available (%)	Indicates the amount of disk space (in %) available for use by platform processes and applications.
Filesystem Information: Minor Alarm Threshold (%)	Indicates the maximum amount of disk space (in %) that can be utilized before a minor alarm is raised indicating that the set threshold has been exceeded.
Filesystem Information: Major Alarm Threshold (%)	Indicates the maximum amount of disk space (in %) that can be utilized before a major alarm is raised indicating that the set threshold has been exceeded.
Filesystem Information: Critical Alarm Threshold (%)	Indicates the maximum amount of disk space (in %) that can be utilized before a critical alarm is raised indicating that the set threshold has been exceeded.
Volume Group Information: Volume Group Name	Indicates the name of the volume group in the array.
Volume Group Information: Volume Group Size (GB)	Indicates the total size of the volume group in the array.
Volume Group Information: Total Space Allocated (GB)	Indicates the amount of volume group space, in gigabytes, currently allocated to filesystems.
Volume Group Information: Total Space Allocated (%)	Indicates the amount of volume group space (in %) currently allocated to filesystems.
Volume Group Information: Total Space Available (GB)	Indicates the amount of unallocated volume group space, in gigabytes, available for filesystems.
Volume Group Information: Total Space Available (%)	Indicates the amount of unallocated volume group space (in %) available for filesystems.

11 When you have completed reviewing the Disk Services page, return to step 2.

12 Review the Services page and use the following table to review the description of the various fields of the Platform Services page:

Note: The Services panel does not update automatically. Click the **Services** link again to update it.



Network Services	
Number of Active Command Line Sessions	Number of Clients with Active Web Sessions
3	2

NTP Information					
Server 1	Server 2	Server 3	Total Number of Servers	Accessible Servers	Synchronized Servers
47.140.162.68 in sync	undefined	undefined	1	1	1

Field	Description
Network Services: Number of Active Command Line Sessions	Indicates the number of command line interface (CLI) sessions (both remote and local) on the Session Server.
Network Services: Number of Clients with Active Web Sessions	Indicates the number of clients running one or more web GUI sessions.
NTP Information: Server1 - Server 3	Indicates the IP address of up to 3 Network Time Protocol (NTP) servers in the network, along with the status of the connection.
NTP Information: Total Number of Servers	Indicates the number of NTP servers registered with the CS-LAN network.
NTP Information: Accessible Servers	Indicates the number of NTP servers accessible to the Session Server.
NTP Information: Synchronized Servers	Indicates the number of NTP servers to which the Session Server is synchronized.

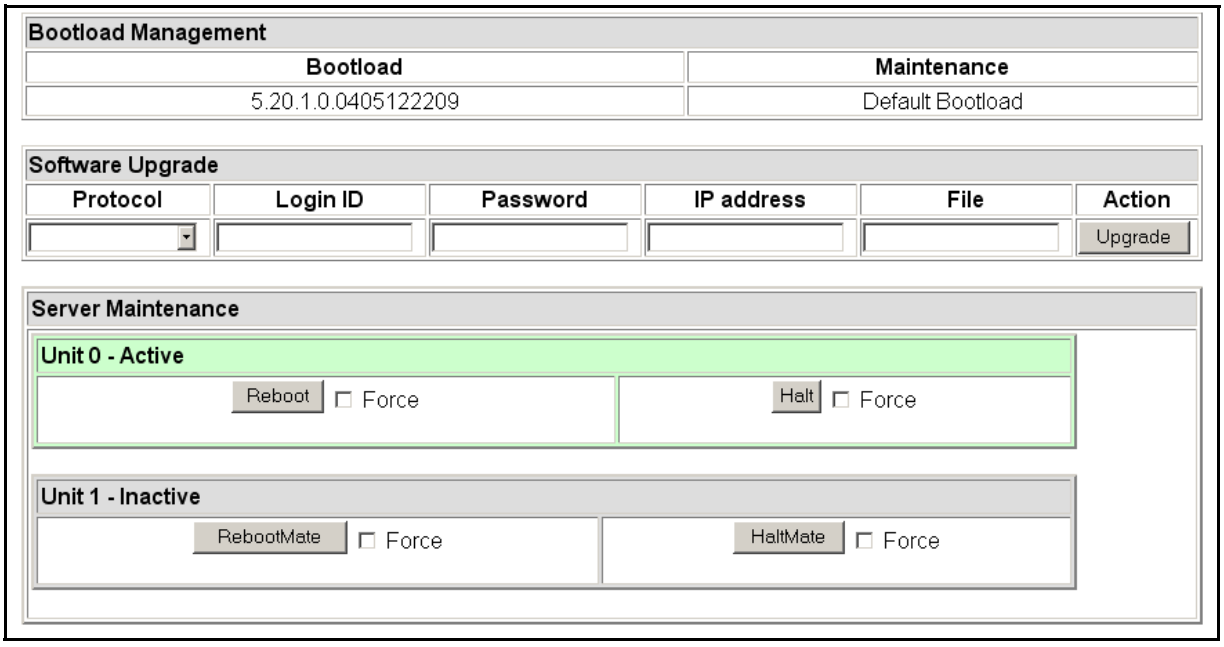
13 When you have completed reviewing Platform Services status, return to step 2.

14 Review the Administration page and use the following table to review the description of the various fields of the Administration page:

Note: The Administration panel does not update automatically. Click the link again to update it.

ATTENTION

To perform software upgrades to the NCGL platform, refer to the Session Server Upgrades NTP, NN1010349-461.



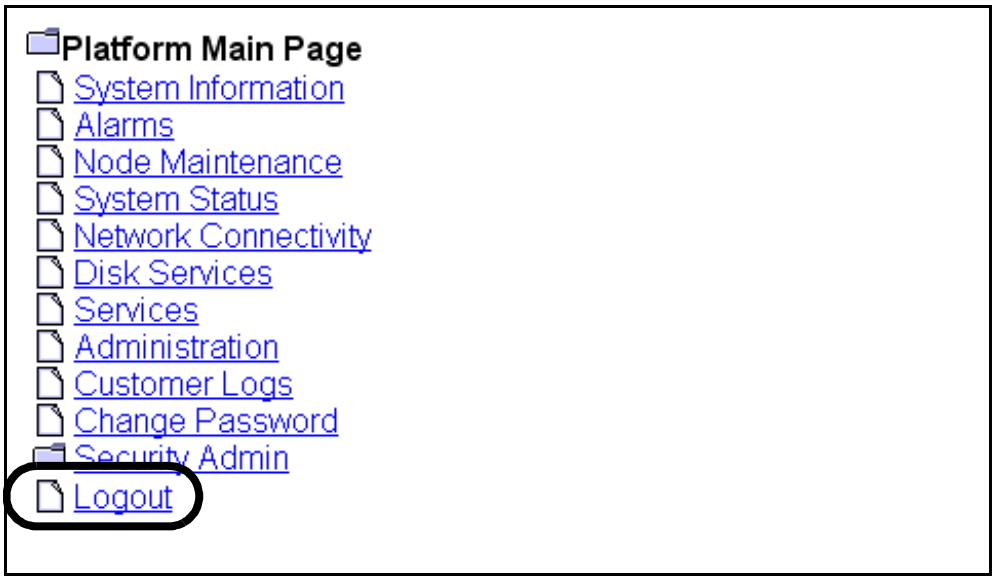
Field	Description
Bootload Management: Bootload	Indicates the load ID for the NCGL platform software load.
Bootload Management: Maintenance	Indicates whether the Bootload is the default. May also allow choosing a new default bootload if there is more than one load available. Additional loads can come from maintenance releases.

Field	Description
Software Upgrade: Protocol	Indicates the file transfer protocol or source location for the platform software upgrade: FTP, Anonymous FTP, HTTP, HTTPS, Local File, Local CDROM.
Software Upgrade: Login ID	If a login ID is required to access the upgrade platform load from another server in the network, a login ID can be entered here.
Software Upgrade: Password	If a password is required to access the upgrade platform load from another server in the network, a password can be entered here.
Software Upgrade: IP Address	If it is required to access the upgrade platform load from another server in the network, an IP address can be entered here.
Software Upgrade: File	The target upgrade load path and filename is entered here.
Software Upgrade: Action Upgrade button	The **Upgrade** button initiates a platform NCGL upgrade. Refer to the Session Server Upgrades NTP, NN10349-461, for instructions on using this function.
Server Maintenance (active and inactive units)	To execute the **Reboot**, **Halt**, **Rebootmate** and **Haltmate** functions, refer to the applicable procedures in the Session Server Security and Administration NTP, NN10346-611.

15 When you have completed reviewing the Administration page, return to step 2, or continue with step 16.

16 If you want to logout from platform GUI, click the **Logout** button.

You are returned to the login page



17 The procedure is complete.

Acquire patch files

Purpose of this procedure

Use this procedure to identify NCGL patch files from a CD/DVD disk or ESD archive file and copy them to an appropriate patch holding directory on each Session Server unit. This procedure may be used as a standalone task or as part of a higher level activity found in activities *Patching the NCGL operating system and installed applications* or *Applying a maintenance release upgrade*, both found in the Session Server Upgrades NTP, NN10349-461, or Upgrading from a previous major release - SN07 to SN08 on page 1159.

Limitations and Restrictions

As this is not a service impacting procedure, it can be performed on either the active or inactive units.

Prerequisites

If locating patch files from a CD/DVD disk, ensure that the upgrade, maintenance release or patching CD/DVD disk is inserted into the unit DVD-ROM drive.

If locating patch files from an ESD delivered ISO archive file, ensure that the software archive file has been extracted and put into the /opt/swd directory on both units using procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 1185.

Action

If locating patch files from a CD/DVD disk, proceed with procedure Procedure: Acquire patch files from a CD/DVD disk.

If locating patch files from an ESD delivered ISO maintenance release image file, then go to Procedure: Acquire patch files from an ESD delivered ISO image on page 1249.

Procedure: Acquire patch files from a CD/DVD disk

At the Session Server CLI or Integrated EMS client

1. Log onto either Session Server unit and change to the root user.
2. Insert the CD/DVD disk into the disk drive.
3. At the prompt, type

   ```
   $ cd /
   ```

   and press Enter.

4 Mount the DVD-ROM drive by typing

```
$ mount /cdrom
```

and pressing the Enter key.

5 Change directories to the mounted DVD-ROM filesystem by typing

```
$ cd /cdrom
```

and pressing the Enter key.

6 Locate the patch files by typing

```
$ ls
```

and pressing the Enter key.

The system responds by displaying a list of files. Locate the patch files with the following filename format:

ncgl_samxts_patch_<rel#>.<wk#>.<major#>.<minor#>

Example
ncgl_samxts_patch_5.31.1.1

ncgl_samxts_patch_5.31.1.2

7 For NCGL patches, copy the patch files from the CD/DVD disk to the patch holding directory on the Session Server unit by typing

```
$ cp <patchfilename> /patch/patchholding
```

and pressing the Enter key.

where

patchfilename
is the file name for the patch file

8 Change directories to root by typing

```
$ cd /
```

and pressing the Enter key.

9 Unmount the DVD-ROM drive by typing

```
$ umount /cdrom
```

and pressing the Enter key.

10 Repeat this procedure on the mate Session Server unit.

11 You have completed this procedure.

Procedure: Acquire patch files from an ESD delivered ISO image

At the Session Server CLI or Integrated EMS client

1 Log onto either Session Server unit and change to root user.

2 Change directories to the directory where the maintenance or upgrade release ISO image (and associated patch files) is located by typing

```
$ cd /opt/swd/<ESD_ISO_directory>
```

and pressing the Enter key.

where

<ESD_ISO_directory>
is the directory containing the version of the ISO image and associated patch files.

Note: There may be multiple directories containing different versions of ISO images.

3 Locate the patch files by typing

```
$ ls
```

and pressing the Enter key.

The system responds by displaying a list of files. Locate patch files with the following filename format:

ncgl_samxts_patch_<rel#>.<wk#>.<major#>.<minor#>

Example
ncgl_samxts_patch_5.31.1.1

ncgl_samxts_patch_5.31.1.2

4 For NCGL patches, copy the patch files from the CD/DVD disk to the patch holding directory on the Session Server unit by typing

```
$ cp <patchfilename> /patch/patchholding
```

and pressing the Enter key.

where

patchfilename
list the file name for the patch file

5 Repeat the previous step for additional patch files you need to install.

6 Repeat this procedure on the mate Session Server unit.

7 You have completed this procedure.

Apply and commit an NCGL patch

Purpose of this procedure

Use this procedure to apply patch files to the inactive Session Server unit. This procedure should only be used as part of the high level activity *Patching the NCGL operating system and installed applications* in the Session Server Upgrades NTP, NN10349-461.

Restrictions and Limitations

ATTENTION
NCGL patch files should only be applied the inactive unit.

Patching activities must be completed on both units in the node.

Prerequisites

The patch files must have already been put into the **/patching/patchholding** directory on the Session Server hard drive. Contact your network administrator to determine if this has already been done. Refer to section *Patching the NCGL operating system and installed applications* in the Session Server Upgrades NTP, NN10349-461, to copy patch files to the hard drives.

Use the patching or upgrade release notes to verify if any NCGL patches must first be removed before applying new patches.

Action

At the Session Server CLI or Integrated EMS client

1. Log onto the inactive Session Server unit and change to the root user.
2. Change directory to the patchholding directory by typing

   `$ cd /patching/patchholding`

   and pressing the Enter key.
3. Retrieve and untar the patch files from the patch archive to the /patching/<patch_version>/ directory, and fill the patching subsystem's database with the patch information. At the prompt, type:

   # patch_ha -f <patch_file_name> -o Fetch

   and press the Enter key.

where

patch_file_name
is the name of the patch archive you want to extract patch files from.

4 Validate the patch file to verify that the patch file is sane, and the patch is ready to be applied. At the prompt type:

 # patch_ha -v <patch_version> -o Validate

and press the Enter key.

where

patch_version
is the name of the patch file to be applied

5 Apply the patch file. Type:

 # patch_ha -v <patch_version> -o Apply

and press the Enter key.

where

patch_version
is the name of the patch file to be applied

ATTENTION
NCGL patches are not automatically committed when applied. In order for a patch to reapply the next time the unit is rebooted, it must first be committed.

6 Commit the patch so it is auto-applied at each reboot of the unit. Type:

patch_ha -v <patch_version> -o Commit

and press the Enter key.

where

patch_version
is the name of the patch file to be committed

7 If necessary, allow the unit to reboot or if requested, perform a reboot using procedure Reboot a Session Server unit on page 1208. Otherwise go to the next step.

8 Perform a status check of the unit including checking for newly generated logs and alarms, to ensure the inactive unit is operating without error. Refer to the Session Server Fault Management NTP, NN10332-911, for applicable procedures. If

errors occur that are related to the patching activity, contact your next level of support.

Note: Checking unit status may entail different activities depending on the what type of software item has been patched and any special patch application requirements. For example, some software subsystem processes may require a reboot before a patch can become active, whereas other subsystem processes restart with the new patched version once patch application is complete.

9 You have completed this procedure. If you were patching files as part of an upgrade activity, then return to the high-level activity.

View web proxy settings in SSPFS for Session Server

Purpose of this procedure

Use the following activity to view the configuration of existing Session Server node web proxy services on the SSPFS server (part of the CS 2000 Management Tools server). This procedure may be used as a standalone task or as part of a higher level activity such as a major upgrade activity.

Limitations and restrictions

If the web proxy entry for a particular Session Server node requires changing, you must configure a new proxy entry with the modified values, then remove the obsolete proxy entry. Do not use this procedure to add a new Session Server node to the proxy service configuration. To perform this activity, refer to procedure *Add a Session Server node to the SSPFS server web proxy*, found in the Session Server Configuration NTP, NN10338-511.

Prerequisites

Ensure that the account you use to log into the CS 2000 Management Tools server has root privileges.

Observe all limitations and prerequisites applicable to other procedures referenced in this activity.

Refer to section *Understanding Session Server IP addressing*, found in the Session Server Configuration NTP, NN10338-511, for more information about Session Server IP addressing and naming schemes needed to complete this activity. The following IP addresses are referenced in this activity:

- Unit 0 (the IP address of physical unit0)
- Unit 1 (the IP address of physical unit 1)
- Active unit (the IP address of the logically active unit, also used for accessing the CS 2000 Session Server Manager GUI)

If necessary, refer to procedure *Configuring the Apache Web Server for HTTPS proxy*, in the ATM/IP Solution-level Configuration Management NTP, NN10409-500, for assistance.

Action

At the Session Server CLI or Integrated EMS client

1 Verify that a security certificate has been installed on the CS 2000 Management Tools Server SSPFS platform. For assistance use procedure *Installing an HTTPS certificate on a Sun server* found in the NTP, Carrier Voice over IP Network Upgrade Overview, NN10440-450.

2 Log onto the CS 2000 Management Tools server. If necessary, refer to procedure *Configuring the Apache Web Server for HTTPS proxy*, in the ATM/IP Solution-level Configuration Management NTP, NN10409-500, for assistance.

3 Change to the root user by typing

`su - root`

and pressing the Enter key.

4 Enter the root password and press Enter.

5 Start the command line interface application by typing

`cli`

and pressing the Enter key.

The system responds:

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

6 Access the Configuration level by typing

2

and pressing the Enter key.

The system responds:

```
Configuration

 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 .
 .
 18 - snmp_poller (SNMP Poller Configuration)
 X - exit
select -
```

7 Access the Apache Proxy Configuration level by typing

2

and pressing the Enter key.

The system responds:

```
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 -
```

8 List the current Apache Proxy Configuration entries by typing

3

and pressing the Enter key.

The system responds:

```
=== Executing "list_proxy_conf"
```

```
#Begin Proxy Config
<IfModule mod_proxy.c>
  ProxyRequests On
  # Add Proxy Entries Here
  ProxyPass /47.174.74.184/ https://47.174.74.184:443/
  ProxyPassReverse /47.174.74.184/ https://47.174.74.184:443/
  ProxyPass /47.142.209.118/ https://47.142.209.118:443/
 ProxyPassReverse /47.142.209.118/ https://47.142.209.118:443/
  ProxyPass /47.142.209.116/ https://47.142.209.116:443/
 ProxyPassReverse /47.142.209.116/ https://47.142.209.116:443/
  ProxyPass /prov/ https://47.174.74.184:8443/prov/
  ProxyPassReverse /prov/ https://47.174.74.184:8443/prov/
  AllowCONNECT 433
  <Proxy *>
    Order deny,allow
    Allow from all
  </Proxy>

      </IfModule>
      #End Proxy Config
      === "list_proxy_conf" completed successfully
```

9 Locate the proxy entry for the active unit GUI used by the CS 2000 Session Server Manager GUI. Refer to the following figure for assistance in locating this entry.

ProxyPass /10.65.99.67/ https://10.65.99.67:443/	Entry for physical unit 0
ProxyPassReverse /10.65.99.67/ https://10.65.99.67:443/	
ProxyPass /10.65.99.70/ https://10.65.99.70:443/	Entry for physical Unit 1
ProxyPassReverse /10.65.99.70/ https://10.65.99.70:443/	
ProxyPass /10.65.99.72/ https://10.65.99.72:443/	Entry for active unit
ProxyPassReverse /10.65.99.72/ https://10.65.99.72:443/	
*ProxyPass **/prov/** https://10.67.99.72:8443**/prov/***	Entry for active unit GUI
*ProxyPassReverse **/prov/** https://10.67.99.72:8443**/prov/***	

10 If necessary, record the label for the remote hostname/tag associated with the Session Server active unit.

ATTENTION

If necessary, please refer to section Selecting and using tag names in SN08 and beyond on page 1257 for more information about using remote tag names. The tag name shown must match the tag name used by the SIP Gateway application for the same Session Server node when you installed or upgrading it.

11 Exit the Apache Proxy Configuration level by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

12 Exit the Configuration level by typing

```
x
```

and pressing the Enter key.

You are returned to the SSPFS operating system.

13 Exit the CLI by typing

```
x
```

and pressing the Enter key.

You are returned to the SSPFS operating system.

14 If applicable, logout from the workstation.

Selecting and using tag names in SN08 and beyond

Tag names for the active Session Server unit GUI web proxy entries, must match the tag name entered when installing or upgrading the SIP Gateway application. Failure to use the same tag name will prevent access to the Session Server GUIs after the SSPFS web proxy services restart.

ATTENTION

If you are upgrading fromSN07, or rolling back to SN07, the SSPFS web proxy server must be using the “prov” tag name.

If the remote tag name for a Session Server node does not match that used during installation or upgrade of the SIP Gateway application, you must configure a new proxy entry using the correct remote tag name, then remove the obsolete proxy entry. To perform this activity, refer to procedure *Add a Session Server node to the SSPFS server web proxy*, found in the Session Server Configuration NTP, NN10338-511.

Upgrade/rollback/reinstall a Session Server application

Purpose of this procedure

Use the following procedure to install any version of a Session Server application onto a Session Server unit including:

- reinstalling a current version of the SIP Gateway Application
- upgrading to a newer version of the SIP Gateway Application
- rolling back to a previous version of the SIP Gateway Application

ATTENTION

It is recommended that this procedure only be used as part of the high level activity Upgrading from a previous major release - SN07 to SN08 on page 1159 or *Applying a maintenance release upgrade*, found in the Session Server Upgrades NTP, NN10349-461.

Limitations and restrictions

If the Session Server node is in operation and performing call processing activities, only perform this procedure on the standby unit.

This procedure must be performed on both Session Server units based on the upgrade or rollback activity being performed.

Prerequisites

CAUTION

Use care when using this procedure. This procedure may cause the loss of customer data. Ensure that you have backed up the SIP Gateway application database before executing this procedure.

Action

If you are reinstalling, upgrading or rolling back the SIP Gateway application from a CD/DVD disk, proceed with procedure Procedure: Reinstall, upgrade or rollback the SIP Gateway application from a CD/DVD disk.

If reinstalling, upgrading or rolling back the SIP Gateway application from an ESD delivered ISO image file, then go to Procedure: Reinstall, upgrade or rollback the SIP Gateway application from an ISO image file on page 1262.

Procedure: Reinstall, upgrade or rollback the SIP Gateway application from a CD/DVD disk

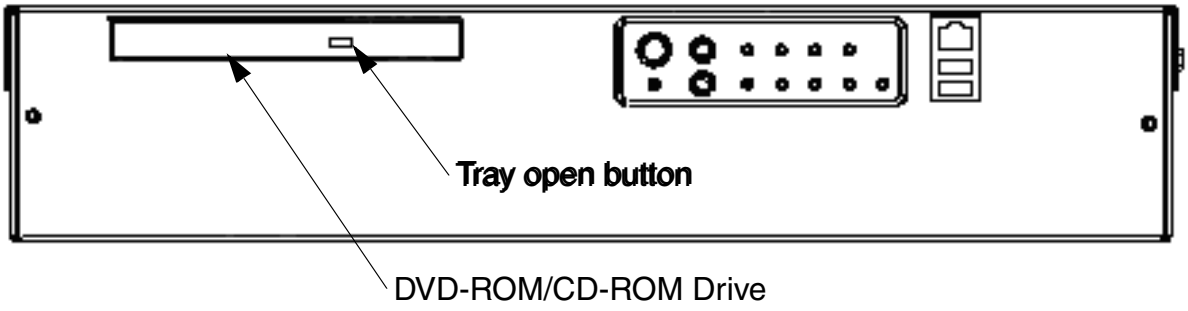
At the Session Server CLI or Integrated EMS client

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Ensure that the CD/DVD disk containing the SIP Gateway Application is inserted before continuing.

Note: In some cases the SIP Gateway Application may be on its own disk or it may be on the NCGL CD/DVD disk.

Session Server Front Panel



3 At the prompt, type

cd /

and press Enter.

4 At the prompt, type

mount /cdrom

and press Enter.

The operating system may respond with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

5 As you should only be upgrading the inactive unit you need to determine if this is the correct unit, at the prompt, type

`mtccli status`

and press Enter.

The system will respond with the following output:

```
$ mtccli status
Unit 1 Status:
   Jam: Link0: Link1: PTPLink: OperationState:
Unit0 Inact no . Inact . Act . Enabled
Unit1 Act no . Inact . Act . Enabled
```

Note: The field after 'Unit0' or 'Unit1' identifies the status of the unit as it relates to being either active or inactive. In this example, 'Unit0 Inact' indicates that this is the inactive unit.

6 From the root level, at the prompt, type

`/cdrom/Tools/InstallApps`

and press Enter.

The operating system responds:

```
The NGSS Application layer is currently
installed. Do you wish to uninstall the previous
application and install the newer version? (yes,
no)
```

7 Type

yes

and press Enter.

The inactive unit begins installing the application. You will see messages scrolling on the screen. No action is needed. Ignore any “No such file or directory" messages.

8 For upgrading to SN08 only, when prompted, enter a remote tag name for this unit, of up to 64 alphanumeric characters, including period, hyphen and underscore and press Enter. For the Session Server node you are upgrading from SN07, you must reuse the existing SN07 tag names “prov” or “/prov”.

ATTENTION

The tag name you select must match the tag name used by the SSPFS web proxy server.

ATTENTION

If you are rolling back to SN07 from SN08, the SSPFS web proxy server must be using the “prov” tag name. Use procedure *View web proxy settings in SSPFS for Session Server*, in the Session Server Configuration Management NTP, NN10338-511, to verify the tag name currently in use.

Note 1: If you are performing an SN08 or greater maintenance release and changing the remote tag name, the following labels cannot be used for a remote tag name:

- spc
- ROOT
- webdav
- admin.xml
- manager.xml

Note 2: Starting in SN08, multiple Session Server nodes, made up of two units per node, can be installed in the CS-LAN network. Therefore, each node installed on the CS-LAN must have its own unique remote tag name (used on both units in the node). Failure to follow this rule will prevent you from accessing a node’s GUIs properly. Refer to section “Using multiple tag names for multiple Session Server nodes”, part of procedure *Add a Session Server node to the SSPFS server web proxy*, in the Session Server Configuration Management NTP, NN10338-511, for more information about using multiple remote tag names.

9 After the SIP application has completed installation, at the prompt, type

cd /

and press Enter.

10 Unmount the disk drive by typing

umount /cdrom

and pressing the Enter key.

11 Press the tray open button and remove the CD/DVD disk from the drive.

12 You have completed this procedure. If applicable, return to the high-level activity.

Procedure: Reinstall, upgrade or rollback the SIP Gateway application from an ISO image file

At the Session Server CLI or Integrated EMS client

1 Log onto the inactive Session Server unit using a secure shell by typing

> **ssh -l <userid> <inactive_SS_IP_address>**

and pressing the Enter key.

where

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

inactive_SS_IP_address
is the IP address or host name of the Session Server unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your 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 the DVD-ROM drive is not currently mounted to the /cdrom directory by typing

umount /cdrom

and pressing the Enter key.

6 At the prompt, type

mount -o loop /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO> /cdrom

and press **Enter**.

where

ESD_file_ISO
is the name of the maintenance release or upgrade ISO file

Example
mount -o loop /opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO. /cdrom

The operating system responds with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

7 From the root level, at the prompt, type

`/cdrom/Tools/InstallApps`

and press Enter.

The operating system responds:

```
The NGSS Application layer is currently
installed. Do you wish to uninstall the previous
application and install the newer version? (yes,
no)
```

8 Type

yes

and press Enter.

The inactive unit begins installing the application. You will see messages scrolling on the screen. No action is needed. Ignore any “No such file or directory" messages.

9 For upgrading to SN08 only, when prompted, enter a remote tag name for this unit, of up to 64 alphanumeric characters, including period, hyphen and underscore and press Enter. For the Session Server node you are upgrading from SN07, you must reuse the existing SN07 tag names “prov” or “/prov”.

ATTENTION

The tag name you select must match the tag name used by the SSPFS web proxy server.

ATTENTION

If you are rolling back to SN07 from SN08, the SSPFS web proxy server must be using the “prov” tag name. Use procedure *View web proxy settings in SSPFS for Session Server*, in the Session Server Configuration Management NTP, NN10338-511, to verify the tag name currently in use.

Note 1: If you are performing an SN08 or greater maintenance release and changing the remote tag name, the following labels cannot be used for a remote tag name:

- spc
- ROOT
- webdav
- admin.xml
- manager.xml

Note 2: Starting in SN08, multiple Session Server nodes, made up of two units per node, can be installed in the CS-LAN network. Therefore, each node installed on the CS-LAN must have its own unique remote tag name (used on both units in the node). Failure to follow this rule will prevent you from accessing a node's GUIs properly. Refer to section "Using multiple tag names for multiple Session Server nodes", part of procedure *Add a Session Server node to the SSPFS server web proxy*, in the Session Server Configuration Management NTP, NN10338-511, for more information about using multiple remote tag names.

10 After the application has completed installation, at the prompt, type

cd /

and press Enter.

11 Unmount the ISO image by typing

umount -f /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO>

and pressing Enter.

Example
umount -f
/opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO

12 You have completed this procedure. If applicable, return to the high-level activity.

Verify synchronization status of Session Server units

Purpose of this procedure

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

Limitations and restrictions

There are no restrictions for performing this procedure.

Prerequisites

There are no prerequisites for performing this procedure.

Action

At the Session Server GUI or Integrated EMS client

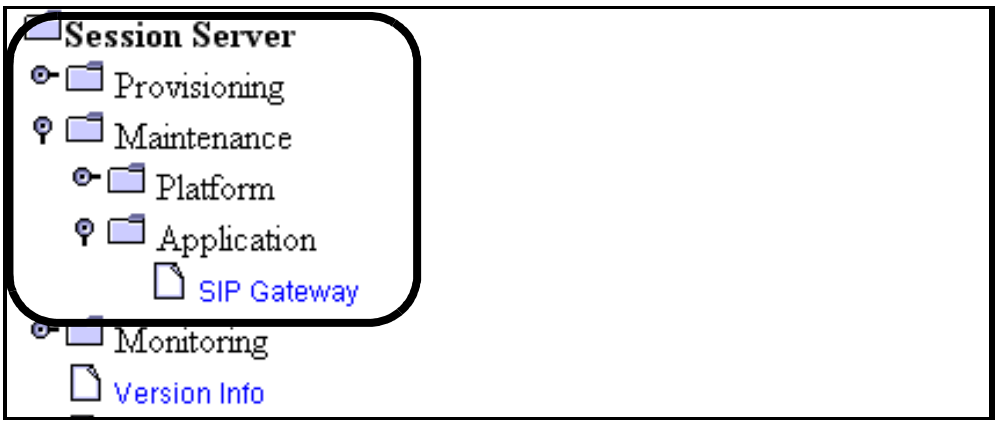
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

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

Please select one of the following management interfaces:

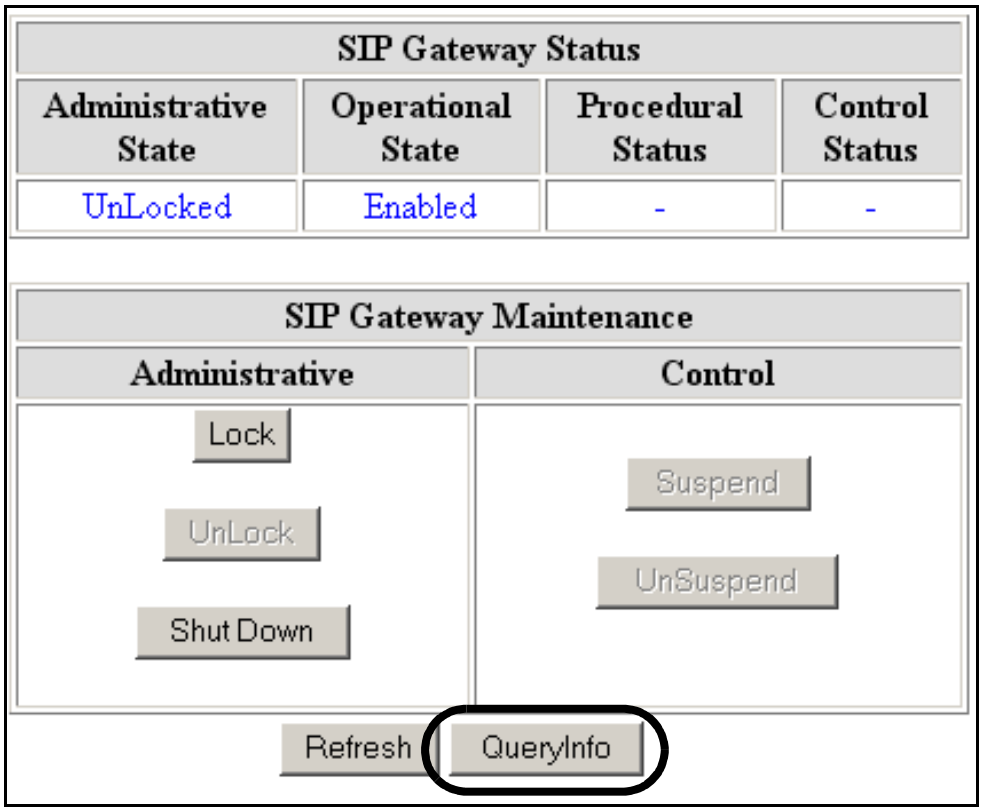
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



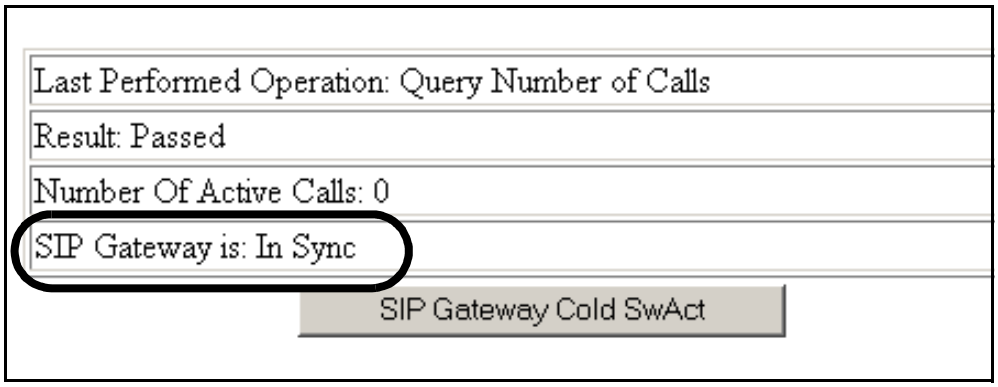
3 Click on the **SIP Gateway** folder to open it.

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



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

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



6 The procedure is complete.

Enable a system SwAct (Unjam)

Purpose of this procedure

The Unjam command is used to manually enable a SwAct (switch of activity) of the active and stand-by units by allowing the two units to toggle their operational states.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as replacing a faulty standby unit or upgrading a standby unit.

ATTENTION
This procedure can only be performed from the active unit.

Prerequisites

There are no prerequisites for performing this procedure.

Action

At the Session Server GUI or Integrated EMS client

1 Select Succession Communication Server NCGL Platform Manager from the launch point menu.

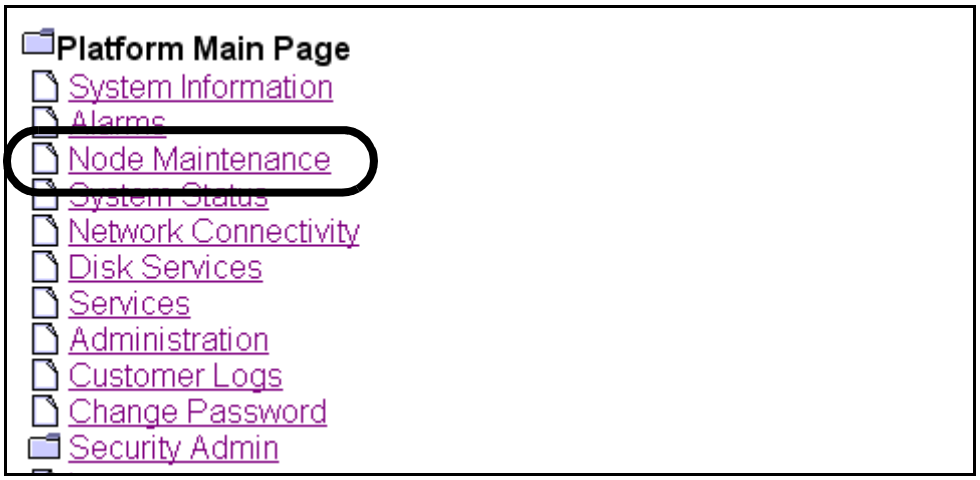
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

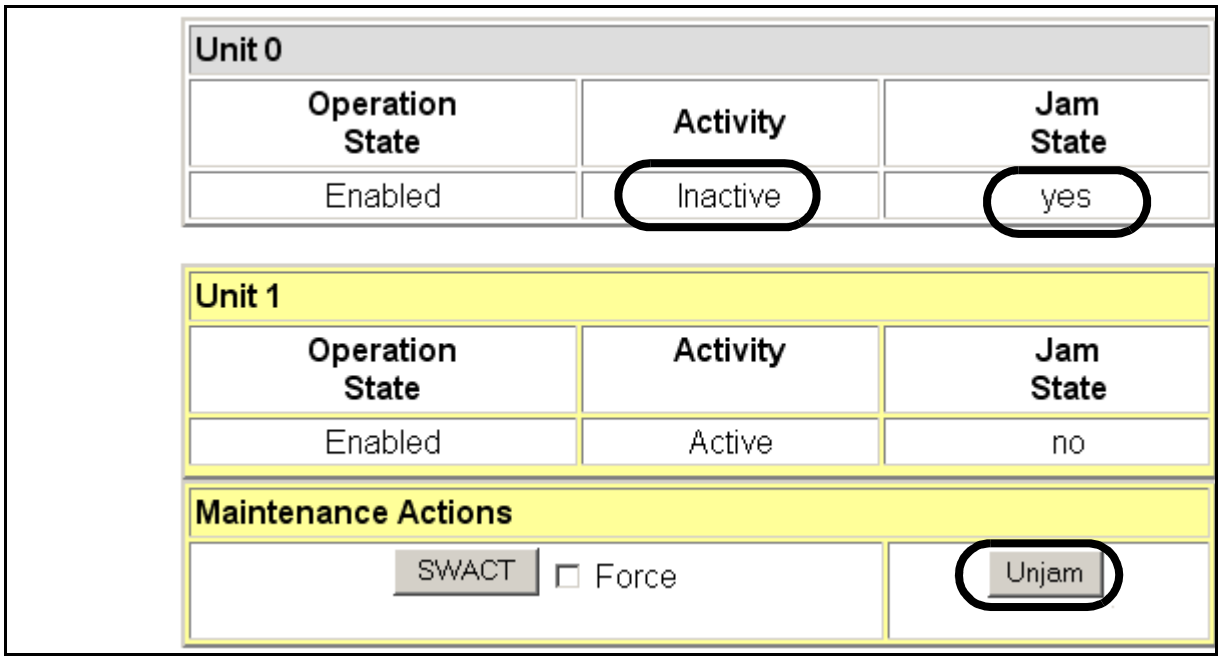
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Node Maintenance** link.

The Node Maintenance page is displayed.



3 Determine if the Jam State of the standby unit is Yes or No. If it is No, then the unit is already unjammed and you are done with this procedure. If it is Yes, then continue with step 4.

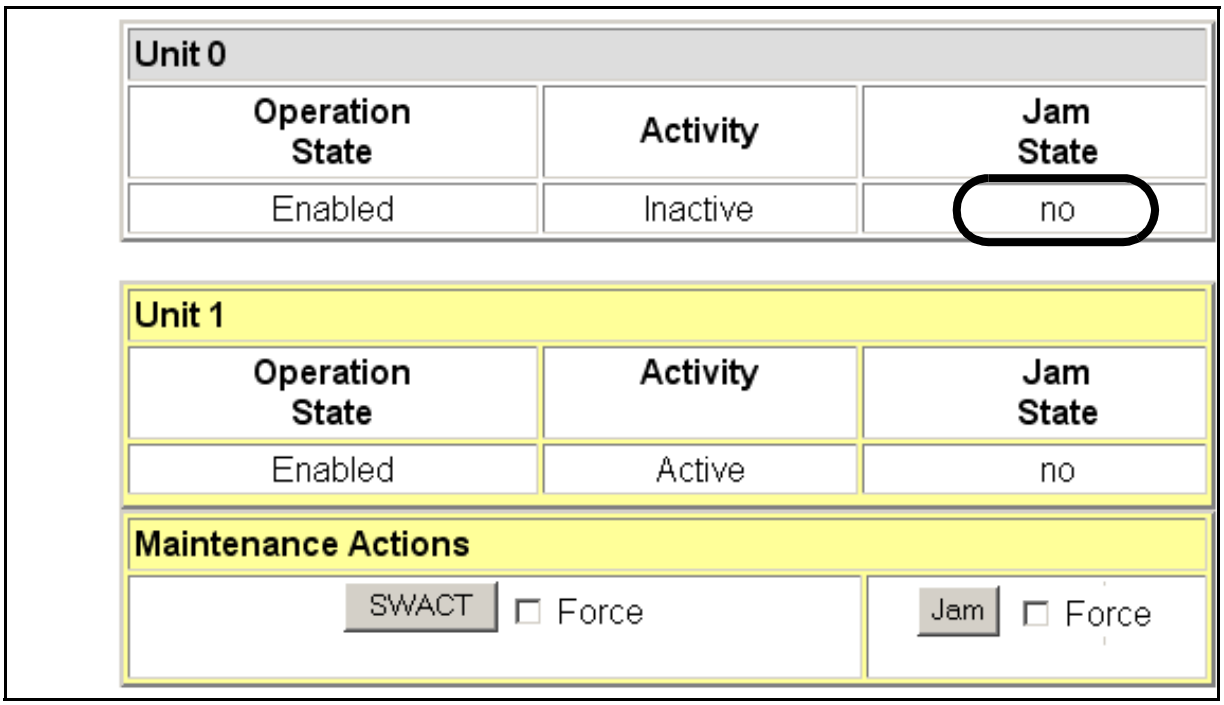


4 Click the **UnJam** button.

The system responds:

```
Info: Unjam - Command passed.
```

5 Observe the Jam state for the standby session server unit transitions from Yes to No.



6 This procedure is complete.

Invoke a maintenance SwAct of the Session Server platform

Purpose of this procedure

This procedure manually performs a maintenance SwAct (switch of activity) of the Session Server platform. A SwAct gracefully transitions call processing activity from the active Session Server unit to the standby unit without first reloading and reinitializing the SIP Gateway application on the standby unit.

Use this procedure as a standalone task or as part of a maintenance or fault clearing activity like replacing a faulty standby unit or a high-level activity such as upgrading a standby unit.

Note: An automatic failover SwAct can be initiated by the platform NCGL in cases of critical faults on the active unit. For more information about conditions required for a SwAct, refer to section *Understanding conditions for a SWACT,* found in the Session Server Security and Administration NTP, NN10346-611.

Limits and Restrictions

ATTENTION
A maintenance SwAct should only be performed when both the active and standby units are operationally enabled and their databases are synchronized.

You cannot SwAct Session Server units if the active unit Jam state is *jammed*. If the unit Jam state is jammed, refer to procedure Enable a system SwAct (Unjam) on page 1267 to unjam the unit.

ATTENTION
Logins to the Session Server do not survive a platform SwAct.

During an unforced maintenance SwAct, new calls are set up on the standby unit, while existing calls continue to be processed on the active unit until they are terminated. SIP-T calls in the process of setup during a SwAct can be lost. Over SIP-T trunks, the far end continues to receive the setup alert (ringing) until one of the following events occur:

- The end user answers and terminates the call.
- A GWC system audit runs and clears the trunks (once every 10 minutes).

Prerequisites

If you are executing a Forced SwAct, confirm that there are no alarm conditions.

Action

At the Session Server GUI or IEMS client of the active unit

1 Select Succession Communication Server NCGL Platform Manager from the launch point menu.

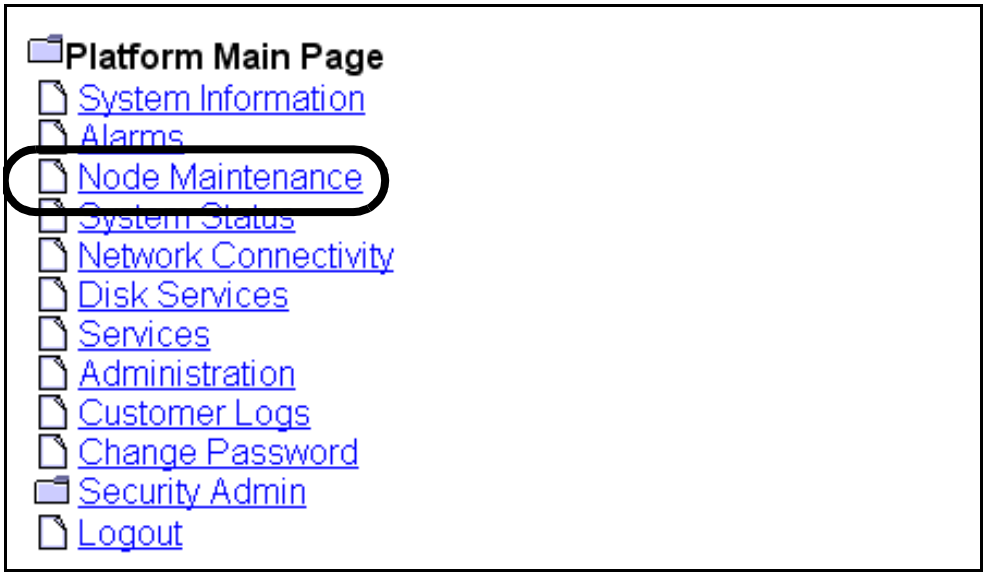
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

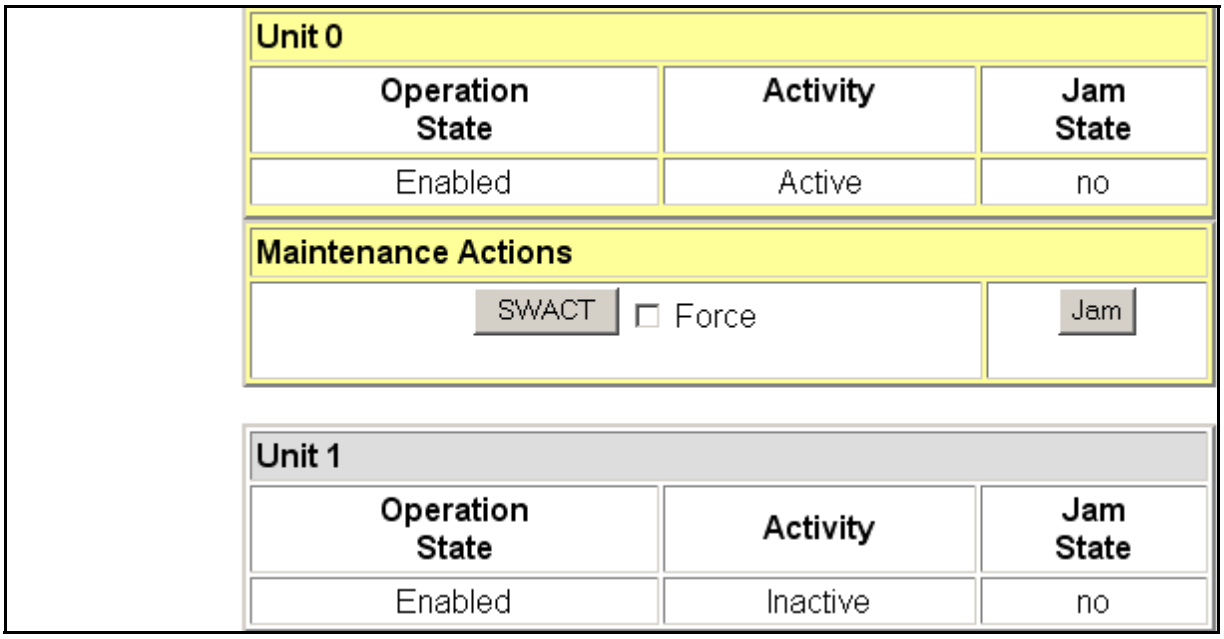
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Node Maintenance** link.

The Node Maintenance page is displayed.



3 Refer to the table in section Additional status information on page 1273 to review the description of the various fields of the Node Maintenance page.



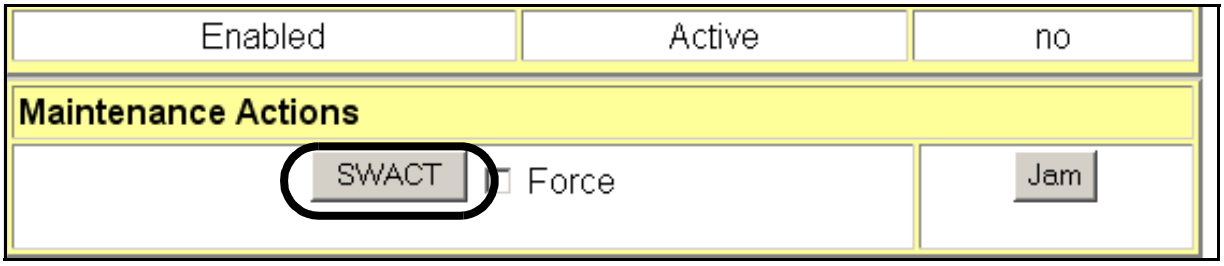
4 To SwAct the Session Server units, click the **SWACT** button.

or

To override any pre-SwAct queries, first click the **Force** check box, then click the **SWACT** button. Refer to section To SWACT or Force a SWACT? on page 1274 for details regarding which type of SWACT to chose.

CAUTION

Due to the risk for loss of data and service outage, it is recommended that the Forced SWACT option not be used except when instructed by your Nortel customer support representative.



The system responds:

```
Are you sure you wish to swact? This may cause
a service interruption to applications running
on this server. Click OK to confirm server swact
or cancel to abort.
```

5 Click **Yes** to confirm either the SwAct or forced SwAct.

6 Observe the *Activity* field for each unit. Each unit's activity status (whether Active or Inactive) swaps.

7 The procedure is complete.

Additional status information

The following table describes the various fields of the Node Maintenance panel.

Field	Description
Operation State (unit 0 or 1)	The operational state of the platform software, either enabled or disabled.
Activity (unit 0 or 1)	The activity state of the platform software, either active or inactive.
Jam State (active unit only)	Indicates whether or not the unit has been "jammed", preventing the standby unit from being able to become active, regardless of any failures on the active unit. States are either jammed, where a SwAct is disabled, or unjammed, where a SwAct is enabled.
Maintenance Actions (active unit only)	Maintenance panel for performing node SWACT activity and to jam or unjam node activity switches.

To SWACT or Force a SWACT?

A forced SWACT overrides any SWACT pre-checks and is not recommended. SWACT pre-checks monitor the inactive unit for critical faults on the platform that should prevent a SWACT. In addition, the pre-check ensures that the SIP Gateway application is in-sync. A SWACT force may result in a full service outage on the Session Server node if the inactive unit is not in-sync. There is potential for loss of provisioned data if a SWACT to an unstable unit is completed.

Copy security certificates to the mate unit

Purpose of this procedure

The following procedure is used to copy security certificates from one Session Server unit to another.

Use this procedure any time new security certificates are created, or when the system is changed from using self-signed certificates to CA-signed certificates. This procedure may also be used as part of a major release upgrade activity.

Limitations and Restrictions

There are no restrictions for performing this procedure.

Prerequisites

New certificates, either self-signed or CA-signed must be installed on the inactive unit.

Action

Perform the following steps to complete this procedure.

At the Session Server CLI or Integrated EMS client

1 Log in to the active Session Server unit and change to the root user.

2 Change directories to the security certificates level by typing

```
# cd /opt/base/share/ssl
```

and pressing the Enter key.

3 Secure copy the server.key file to the mate Session Server unit by typing

```
$ scp server.key
mtc@<mate_SS_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_SS_IP_address
is the IP address of the mate Session Server unit

Note: For initial connections to the mate unit, confirm that you want to continue connecting by entering “yes.”

The mate unit responds by prompting for the password for the mtc user.

4 Enter the password for the mtc user at the password prompt.

The server.key file is copied to the /users/mtc directory on the mate Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

5 Secure copy the certificate.keystore file to the mate Session Server unit by typing

```
$ scp certificate.keystore
mtc@<mate_SS_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_SS_IP_address
is the IP address of the mate Session Server unit

The mate unit responds by prompting for the password for the mtc user.

6 Enter the password for the mtc user at the password prompt.

The certificate.keystore file is copied to the /users/mtc directory on the mate Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

7 Secure copy the server.crt file to the mate Session Server unit by typing

```
$ scp server.crt
mtc@<mate_SS_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_SS_IP_address
is the IP address of the mate Session Server unit

The mate unit responds by prompting for the password for the mtc user.

8 Enter the password for the mtc user at the password prompt.

The server.crt file is copied to the /users/mtc directory on the mate Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

9 If you have a CA-signed certificate, secure copy the trusted.crt file to the mate Session Server unit by typing

```
$ scp trusted.crt
mtc@<mate_SS_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_SS_IP_address
is the IP address of the mate Session Server unit

The mate unit responds by prompting for the password for the mtc user.

10 If applicable, enter the password for the mtc user at the password prompt. Otherwise, skip to the next step.

The trusted.crt file is copied to the /users/mtc directory on the mate Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

At your workstation CLI or Integrated EMS client

11 Log into to the mate Session Server and change to the root user.

12 Change directories to the /users/mtc level by typing

```
cd /users/mtc
```

and pressing the Enter key.

13 Move the server.key file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv server.key /opt/base/share/ssl
```

and pressing the Enter key.

14 If necessary, confirm overwriting any existing server.key file by typing **y** and pressing Enter.

15 Move the certificate.keystore file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv certificate.keystore /opt/base/share/ssl
```

and pressing the Enter key.

16 If necessary, confirm overwriting any existing certificate.keystore file by typing **y** and pressing Enter.

17 Move the server.crt file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv server.crt /opt/base/share/ssl
```

and pressing the Enter key.

18 If necessary, confirm overwriting any existing server.crt file by typing **y** and pressing Enter.

19 If you have a CA-signed certificate, move the trusted.crt file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv trusted.crt /opt/base/share/ssl
```

and pressing the Enter key.

20 If necessary, confirm overwriting any existing trusted.crt file by typing **y** and pressing Enter.

21 Change directories to the security certificates level by typing

```
# cd /opt/base/share/ssl
```

and pressing the Enter key.

22 Change the key file's owner and group to *root* by typing

```
# chown root:root server.key
```

and pressing the Enter key.

23 Change the keystore file's owner and group to *root* by typing

```
# chown root:root certificate.keystore
```

and pressing the Enter key.

24 Change the certificate's owner and group to *root* by typing

```
# chown root:root server.crt
```

and pressing the Enter key.

25 If you have a CA-signed certificate, change the trusted certificate file's owner and group to *root* by typing

```
# chown root:root trusted.crt
```

and pressing the Enter key.

26 Set the key file permissions by typing

```
# chmod 600 server.key
```

and pressing the Enter key.

27 Set the keystore file permissions by typing

```
# chmod 600 certificate.keystore
```

and pressing the Enter key.

28 Set the certificate permissions by typing

```
# chmod 644 server.crt
```

and pressing the Enter key.

29 If you have a CA-signed certificate, set the keystore file permissions by typing

```
# chmod 644 trusted.crt
```

and pressing the Enter key.

30 You have completed this procedure. If you completed this procedure as part of an upgrade activity, return to the high level activity.

If you did not complete this procedure as part of an upgrade, you must complete procedure *Apply security certificates* in the Session Server Security and Administration NTP, NN10346-611.

SAM21 Shelf Controller

Before upgrading the SAM21 Shelf Controller

Perform the required prerequisite upgrade as follows:

Network	SAM21 Shelf Controller applies to:	Previous Upgrade
ATM	UA-AAL1	Media Gateway (MG) 9000 Manager on page 1103
IP	UA-IP[1]	Media Gateway (MG) 9000 Manager on page 1103
	PT-IP[2]	Session Server on page 1158
	IAC - North America	Peripheral Modules on page 1065
	IAC - International, IAW and CHS[3]	CS 2000 Management Tools and Clients (CMT) on page 523
Tri-Modal	all applications	one of above based on configuration

1.Includes IP International: UA-IP
2.Includes IP International: PT-IP
3.Includes IP International: CHS

After upgrading the SAM21 Shelf Controller

Perform the next required upgrade as follows:

Network	SAM21 Shelf Controller applies to:	Next Upgrade
ATM	UA-AAL1	Gateway Controller on page 1330
IP	PT-IP, UA-IP, IAC, IAW, and CHS[1]	Gateway Controller on page 1330
Tri-Modal	all applications	Gateway Controller on page 1330

1.Includes IP International: CHS, PT-IP, IAC, and UA-IP

About the SAM21 Shelf Controller

Services Application Module 21(SAM21) shelves are mounted in a Nortel Networks PTE2000 frame. PTE2000 frames have two

configurations, the Call Control Frame (CCF), and the SAMF frame. The SAMF frame is deployed with CS 2000 XA-Core switches and can also be deployed with CS 2000 - Compact switches when additional Gateway Controllers (GWC) are needed. Two SAM21 Shelf Controllers are required for each shelf.

Electronic Software Delivery (ESD) for SAM21 Shelf Controller

Software loads for the SAM21 Shelf Controller are available for electronic transfer from Nortel to a customer dropbox.

Audience

This procedure is intended for use by operating company personnel who have an ESD agreement with Nortel. When the agreement was established, the operating company furnished Nortel with the location of an electronic dropbox and a username and password pair for delivering software loads. When Nortel delivers a software load to the dropbox, an electronic mail notification is sent to the email 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:

- SAM20080.n.R.NCL.NAP.vault.nn.D.tar.gz — NCL
- SAM2M0080.n.R.NCL.NAP.vault.nn.D.tar.gz — MNCL

n
is an integer value such as 8 and is part of the product order code

vault
is a string that identifies the Nortel software vault that holds the software

nn
is an integer value that indicates the repository version of the software

Prerequisites

The image file must be uncompressed and available on your ESD load repository server.

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 Display the available disk space in the directory by typing

```
# df -k
```

and pressing the Enter key.

Example response

```
# df -k
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2         3082223  144125 2876454    5%    /data/iso_esd
```

4 Record the amount of available disk space, which is provided in kilobytes. You will need the information later in this procedure.

5 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.

6 Change the transfer mode to binary.

```
ftp> bin
```

a List the contents of the drop box by typing

```
ftp> ls
```

7 Locate the uncompressed image file you want to transfer, and identify the size of the file, which is provided in bytes.

Note: Divide the number of bytes by 1024 to convert the size to kilobytes.

8 Compare the size of the uncompressed image file with the amount of available space you recorded in step 4.

9 Use the following table to determine your next step.

If	Do
the server has enough available disk space	step 11
otherwise	step 10

10 Clear additional disk space following local office policy, before you continue with this procedure. If necessary, contact your next level of support.

11 Retrieve the ESD software load:

```
ftp> get <esd_filename>
```

12 Repeat steps 7 through 11 for all ESD software loads recorded in the notification from Nortel and then end the FTP session:

```
ftp> bye
```

13 Change directory to the newly created directory:

```
$ cd <esd_filename>
```

14 Become the root user:

```
$ su - root
```

A prompt for the root password is presented. Enter the root password.

15 Mount the ISO image 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)


 X - exit


select -
```

c Enter the number next to the "mount_image" option in the menu.

If the response is	Do
Enter the full path of the ISO image	substep e
ISO Image Already Mounted	substep d

d Enter the number next to the "mount_image" option in the menu and retry substep c.

Note: If the umount_image or mount_image command is unsuccessful a second time, contact your next level of support.

e When prompted, enter the full path name of the ISO image on the server from the root.

The contents of the ESD software file are placed in directory /tmpmnt

Note: Do not attempt to access the /tmpmnt directory until the mount command is complete.

If the response is	Do
It 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.	step f
Provided full path to ISO image does not exist	Verify the location and name of the ISO 9660 image.
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 your next level of support.
ERROR MOUNTING <ESD_filename>	This response indicates that either the ISO 9660 file is corrupt, or the /tmpmnt directory has been deleted. Repeat this procedure, and if it fails a second time, contact your next level of support.

f Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

```
select - x
```

and pressing the Enter key.

16 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.

When asked if you want to continue, enter y.

The system displays messages telling of its progress through the process of installing the rpm package. The final messages it displays are as follows:

```
   Installation of Platform Load Complete.

******* Please hit ENTER key to continue ******
```

Note: If you want to install the software later, proceed as follows. 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 16, except specify the location of the software instead of /tmpmnt/noarch.

17 Press the Enter key.

System response:

```
     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:
```

18 Exit from the platform installation tool. At the prompt, enter x.

System response:

```
Exiting Installation Tool, GoodBye
```

19 Unmount the ISO image 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)


 X - exit


select -
```

c Enter the number next to the "umount_image" option in the menu.

d Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

```
select - x
```

and pressing the Enter key.

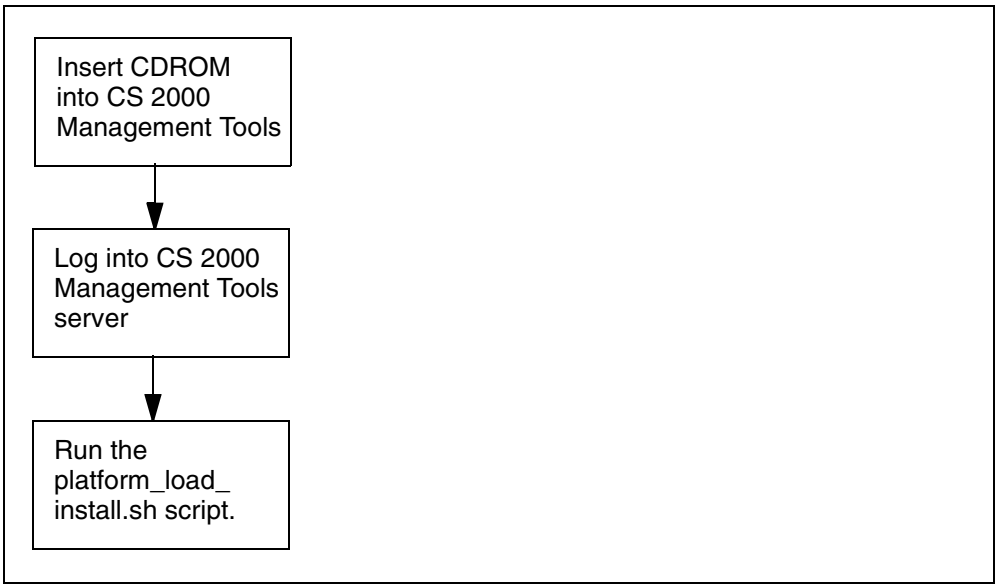
20 This procedure is complete.

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.

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. It is recommended to have a minimum of 25 Megabytes of available disk space. If required, follow the procedure listed in section Old fileset removal on CS 2000 Core Manager on page 1294. Use procedure Old fileset removal on CBM on page 1296 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, SAM20008, 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. It is recommended to have a minimum of 25 Megabytes of available disk space. If there is enough disk space in the volume, skip the procedure and continue with "Upgrading software on the SAM21 Shelf Controller" in *Upgrading the SAM21 Shelf Controller*, NN10067-461.

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 1290 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. It is recommended to have a minimum of 25 Megabytes of available disk space. If there is enough disk space in the volume, skip the procedure and continue with "Upgrading software on the SAM21 Shelf Controller" in *Upgrading the SAM21 Shelf Controller*, NN10067-461.

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.

Testing the inactive Shelf Controller blade before an upgrade

CAUTION
Possible upgrade failure
Make sure the shelf has NOT been provisioned with new software before you begin this procedure. Hardware must take place before the software upgrade.

Perform the following procedure to test the inactive Shelf Controller blade before an upgrade of SAM21 Shelf Controller software. Repeat this procedure as necessary to test each Shelf Controller blade before a software upgrade.

Perform this procedure no more than 24 hours before the upgrade of SAM21 Shelf Controller software.

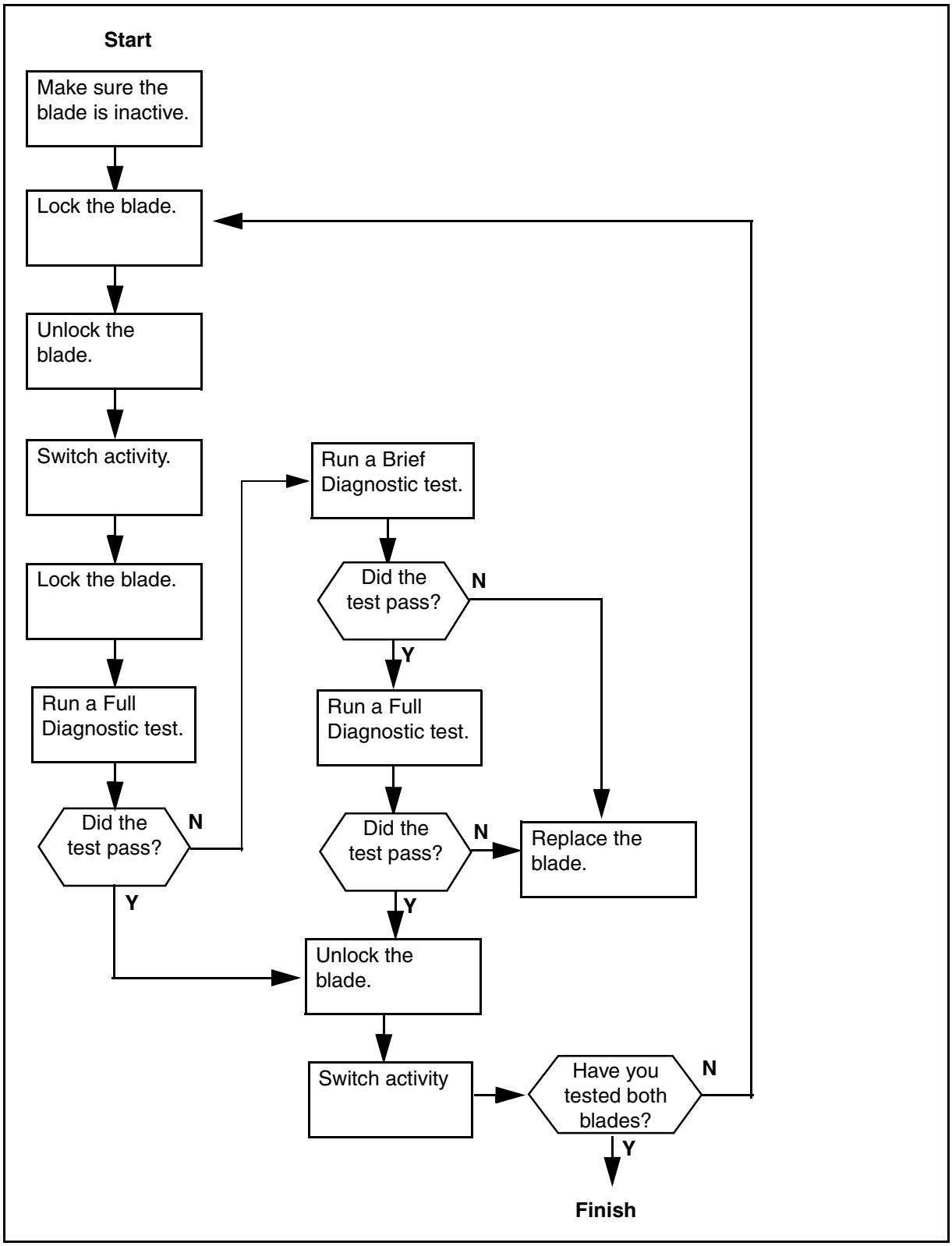
Prerequisites

This procedure has no prerequisites.

Action

The following flowchart shows a high-level summary of the tasks performed during this procedure. Use the step-by-step instructions after the flowchart to perform the procedure.

Testing the inactive Shelf Controller blade before an upgrade



Testing the inactive Shelf Controller blade before an upgrade

At the CS 2000 SAM21 Manager

1 Make sure you are at the Shelf View of the SAM21 shelf with the inactive Shelf Controller blade you want to upgrade.

2 Go to the Card View of the inactive Shelf Controller. Right-click the icon of the inactive Shelf Controller blade and select Card View from the list of commands.

Response

The Card View window appears.

3 Click the States tab and make sure the Status of the selected Shelf Controller is Inactive.

4 Use the following table to determine your next step.

If the status is	Do
Active	Close this window and return to step 1.
Inactive	step 5

5 Lock the blade. On the left side of the Card View window, right-click the Shelf Controller icon and select Lock from the list of commands.

Response

The CS 2000 SAM21 Manager locks the selected Shelf Controller blade.

6 Use the following table to determine your next step.

If the lock is	Do
successful	step 7
not successful	Repeat step 5. If the second attempt fails, go to step 30

7 Unlock the inactive Blade. On the left side of the Card View window, right-click the Shelf Controller icon and select Unlock from the list of commands.

Response

The CS 2000 SAM21 Manager unlocks the selected Shelf Controller blade.

8 Use the following table to determine your next step.

If the unlock is	Do
successful	step 9
not successful	Repeat step 7. If the second attempt fails, go to step 30.

9 Switch activity between the Shelf Controller blades. On the left side of the Card View window, right-click the Shelf Controller icon and select Swact from the list of commands.

Response

The CS 2000 SAM21 Manager switches activity between the Shelf Controller blades.

10 Use the following table to determine your next step.

If the switch of activity is	Do
successful	step 11
not successful	Repeat step 9 If the second attempt fails, go to step 30

11 Lock the inactive blade. On the left side of the Card View window, right-click the Shelf Controller icon and select Lock from the list of commands.

Response

The CS 2000 SAM21 Manager locks the selected Shelf Controller blade.

12 Use the following table to determine your next step.

If the lock is	Do
successful	step 13
not successful	Repeat step 11. If the second attempt fails, go to step 30

13 Click the Diags tab.

14 Run a Full Diagnostic test on the locked Shelf Controller blade. At Type, select Full from the pull-down menu and click the Start button.

Response

A window asking you to confirm the diagnostic run appears. The window shows the estimated time to complete the test.

15 In the Confirm Diag Run window, click the Yes button.

Response

The CS 2000 SAM21 Manager performs a full diagnostic test on the selected Shelf Controller blade. When the test finishes, a window appears indicating success or failure.

16 Use the following table to determine your next step.

If the Full Diagnostic test	Do
passes	step 23
fails	step 17

17 Run a Brief Diagnostic test. At Type, select Brief from the pull-down menu and click the Start button.

Response

A window asking you to confirm the diagnostic run appears. The window shows the estimated time to complete the test.

18 In the Confirm Diag Run window, click the Yes button.

Response

The CS 2000 SAM21 Manager performs a brief diagnostic test on the selected Shelf Controller blade. When the test finishes, a window appears indicating success or failure.

19 Use the following table to determine your next step.

If the Brief Diagnostic test	Do
passes	step 20
fails	step 30

20 Run a second Full Diagnostic test. At Type, select Full from the pull-down menu and click the Start button.

Response

A window asking you to confirm the diagnostic run appears. The window shows the estimated time to complete the test.

21 In the Confirm Diag Run window, click the Yes button.

Response

The CS 2000 SAM21 Manager performs a full diagnostic test on the selected Shelf Controller blade. When the test finishes, a window appears indicating success or failure.

22 Use the following table to determine your next step.

If the second Full Diagnostic test	Do
passes	step 23
fails	step 30

23 Unlock the Shelf Controller Blade. On the left side of the Card View window, right-click the Shelf Controller icon and select Unlock from the list of commands.

Response

The CS 2000 SAM21 Manager unlocks the selected Shelf Controller blade.

24 Use the following table to determine your next step.

If the unlock is	Do
successful	step 25
not successful	Repeat step 23. If the second attempt fails, go to step 30.

25 Close the Card View of the inactive Shelf Controller.

Response

The Shelf View window appears.

26 Go to the card view of the active Shelf Controller. Right-click the icon of the active Shelf Controller blade and select Card View from the list of commands.

Response

The Card View Window appears.

27 Switch activity between the Shelf Controller blades. On the left side of the Card View window, right-click the Shelf Controller icon and select Swact from the list of commands.

Response

The CS 2000 SAM21 Manager switches activity between the Shelf Controller blades.

28 Use the following table to determine your next step.

If the switch of activity is	Do
successful	step 29
not successful	Repeat step 27 If the second attempt fails, go to step 30

29 Use the following table to determine your next step.

If you have successfully tested	Do
one Shelf Controller Blade	step 5
both Shelf Controller blades	step 31

30 Replace the Shelf controller blade before you continue with this software upgrade. If necessary contact your next step level of support.

31 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

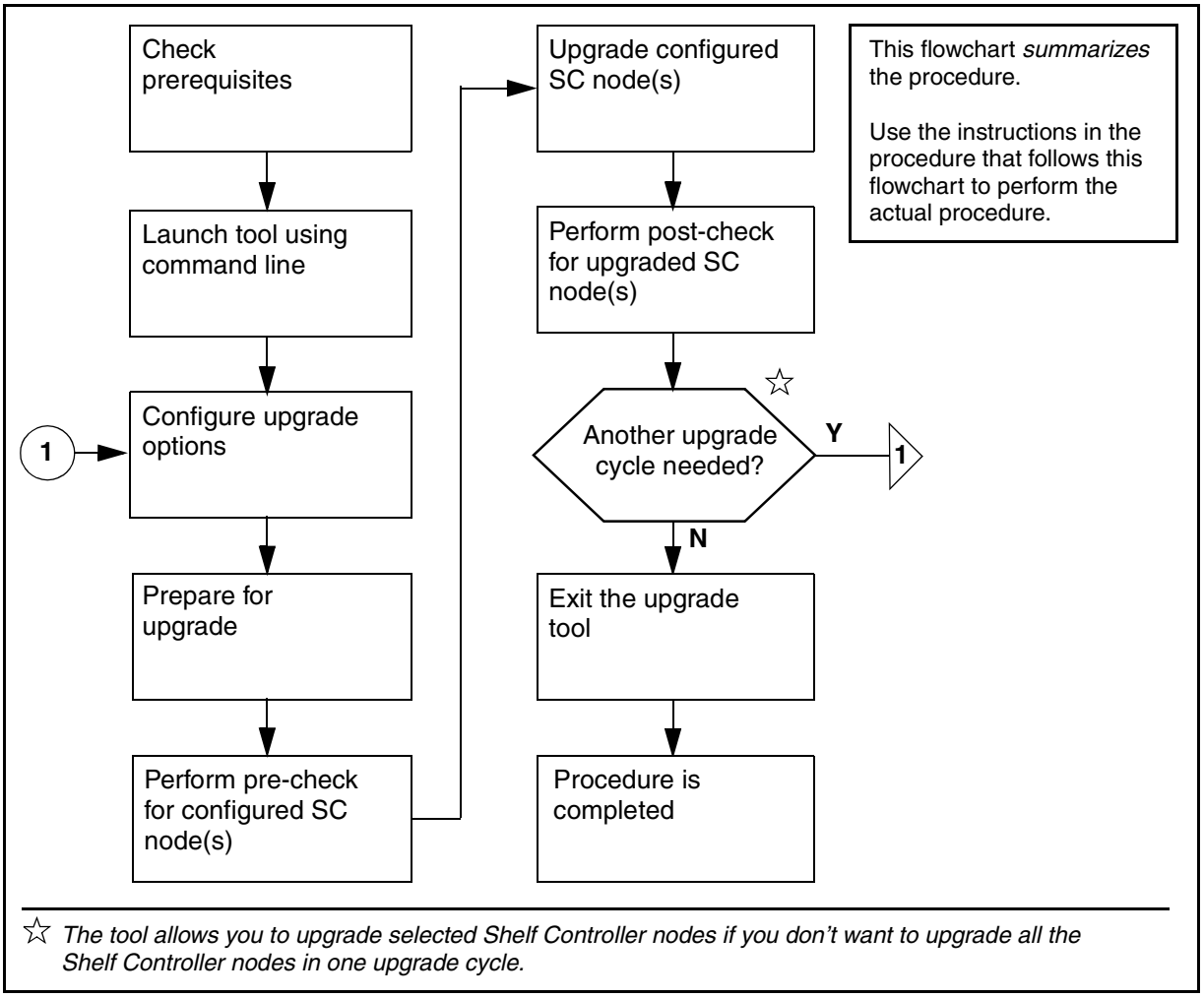
Upgrading the Shelf Controller using the Shelf Controller Upgrade Tool

The Shelf Controller Upgrade Tool is a subcomponent of the upgrade manager in the Carrier Voice over IP Upgrade Management Architecture. The tool supports Shelf Controller software upgrades via the command line user interface (CLUI) The tool automatically performs the following required manual operations:

- locks and unlocks the inactive unit
- swacts the inactive unit
- locks and unlocks a newly inactive unit

The following figure provides an overview of these steps.

Automatic upgrade overview



The automated Shelf Controller Upgrade tool supports the following upgrade modes:

- single, which allows you to upgrade one or more configured Shelf Controller nodes one at a time
- bulk, which allows you to upgrade all configured Shelf Controller nodes simultaneously

If you want to upgrade a Shelf Controller node using the manual method, refer to procedure “Manual software upgrade procedure” in document *Upgrading the SAM21Shelf Controller*, NN10067-461.

Prerequisites

Before upgrading the Shelf Controller software with the automatic upgrade tool, perform the following prerequisite actions.

At the CS2000 Management Tool interface

1 Ensure that the Shelf Controller software load filesets are installed on the CBM or CS 2000 Core Manager (SDM). Refer to procedure Installing SAM21 Platform software.

2

CAUTION
Possible upgrade failure if blade not tested
Test each Shelf Controller no more than 24 hours before the software upgrade. An unhealthy Shelf Controller blade can cause the software upgrade to fail.

Test each Shelf Controller blade. Perform Testing the inactive Shelf Controller blade before an upgrade.

3 Check to be sure that all prerequisites in the previous sections of this document are met. Return to this procedure and perform additional prerequisite steps 4 through 8.

4 Ensure that the operator belongs to one of the following groups that can launch the upgrade tool: mgcmtc, mgcadm, emsmtc or emsadm.

If the operator	Do
belongs to group mgcmtc, mgcadm, emsmtc or emsadm	step 5
does not belong to group mgcmtc, mgcadm, emsmtc or emsadm	add the operator to one of the required groups. (Refer to procedure "Setting up local user accounts on an SSPFS-based server" in *ATM/IP Solution-level Security and Administration*, NN10402-600.) When the operator has been added, return to this procedure and go to step 5.

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

If the operator	Do
belongs to group mgcmtc or emsmtc	step 6
belongs to group mgcadm or emsadm	telnet into the CMT server using the CMT gui userid and password, and go to step 6.

6 Enter:

```
> id -a
```

System response:

```
$ id -a
uid=104(ptm)  gid-104(succssn)
groups=105(succssn),1001(trkadm(,1006(1nadm),1001
(mgcadm),1016(mgadm),1021(emsadm)
$
```

Group names

Refer to the following table to determine your next step.

If	Do
you are logged in as root	step 8
you are not logged on as root	step 7

7 Use the su command (switch user) to log in as the root user. Proceed as follows.

a At the system prompt, type

su - root

and press the Enter key.

System response:

```
Password:
```

b Type

<password>

and press the Enter key

where

<password> is the root password

8 Check the status of the SAM21 element server and CORBA server and ensure they are running properly. Enter:

```
> servquery -status all
```

System response:

```
$ servquery -status all
APP NAME              STATUS
========              ======
DATABASE              RUNNING
CINOTIFIER            RUNNING
BACKUP_MANAGER        Group Started. Current status unavailable
BOOTP                 RUNNING
WEBSERVER             RUNNING
CORBA                 RUNNING
OMPUSH                RUNNING
SESMService           RUNNING
WEBSERVICES           RUNNING
DDMSPROXY             RUNNING
ORA_AUTO_BACKUP       RUNNING
DELEGATE              RUNNING
ORA_ARCHIVE_ROTATOR   RUNNING
NPM                   RUNNING
PROP_SRV              RUNNING
SAM21EM               RUNNING
SNMP_POLLER           Group Started. Current status unavailable
QCA                   RUNNING
```

Server states

9 Use the su command (switch user) to log in using your own user ID. Proceed as follows.

a At the system prompt, type

su - <user-ID>

and press the Enter key

where

<user-ID> is your own user ID

System response:

```
Password:
```

b Type

<password>

and press the Enter key

where

<password> is the your own password

At the core manager

10 Ensure the Shelf Controller load is on the core manager as follows:

a Establish a telnet connection to the core manager, which can be either the CS 2000 Core Manager or the Core and Billing Manager (CBM).

b Log in to the core manager using the root user ID and password.

c Change directory by typing

```
cd <directory>
```

where

directory
is either /swd/sam21 for the CS 2000 Core Manager, or /sam21 for the CBM

d List the contents of the directory by typing

```
ls -arlt
```

and pressing the Enter key.

The system displays the loads in the order they were installed from earlierst to the most recent.

11 The prerequisite steps are completed. To begin the upgrade process, continue with step 1 in the following Detailed procedure.

Detailed procedure

CAUTION
Interruption of upgrade
Do not exit the automatic upgrade tool before the upgrade is completed.

CAUTION
Termination of automatic upgrade tool
Do not press CTRL+C or close the TERM window. These actions terminate the upgrade tool.

ATTENTION
The scuptool does not support rollback for automatic upgrades. If problems occur during the upgrade, you can terminate the upgrade and use the manual rollback procedure *Rollback software on the SAM21 Shelf Controller* in NN10067-461.

At the CS 2000 Management Tool interface

1 Launch the upgrade tool (**scuptool**) to display the Main menu for the Shelf Controller upgrade tool. Enter:

```
> /opt/nortel/sam21em/bin/scuptool.sh
```

Example of system response:

```
$ /opt/nortel/sam21em/bin/scuptool.sh
Starting ....

Main menu for SC upgrade tool
1  - Display all SC pairs
2  - Configure upgrade-related options
3  - List current upgrade configurations
4  - Enter Upgrade Menu

x  - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

2 Configure the upgrade options. Use the following steps:

a Select Configure upgrade-related options from the main menu. Enter:

```
> 2
```

Example of system response:

```
SC upgrade configuration
Enter new load file name:
```

b Enter the load file name for the Shelf Controller. Ensure that the configured load file name exists in the load server (CBM or SDM).

Load name format:

nn.n.n.nnnnnnnnnn

Example file name entry:

11.0.0.0409151320

Example of system response:

```
SC list

Enter the SC list (default: all):
```

c Enter the list of Shelf Controllers to be upgraded. The Shelf Controller contains node names to be upgraded in the same upgrade cycle with the same configured options. *Enter the node names without spaces between the entries.*

Example list entry:

SC1,SC2

The system displays the current input configuration values.

Example of system response:

```
Input values
NewLoadFileName      :      11.0.0.0409151320
SCList               :      SC0,SC1
Default values
LoadDiectory         :      /swd/sam21/
OldLoadName          :      ''(ignored)
UpgradeMode          :      bulk
PausePoint           :      0(none)
LoggingLevel         :      MAJ
MaxTime              :      0(no limitation)
AlarmLevel           :      MAJ
AlarmNumber          :      2

Do you want to use these values to configure? [Y|N]:
```

d Review all values displayed in the system response, including the default values, to ensure they are acceptable.

Note 1: If you have a CBM configuration, you must specify a new load directory. Therefore, you need to enter N in the next step to change the default value for LoadDirectory.

Note 2: By default, no pause points are defined. Pause points allow you to perform manual checks at selected intervals during the upgrade process. At each pause point, you are prompted to continue the upgrade. If you do not specify any pause points, you are not prompted at any point to continue the upgrade unless an error condition occurs. If you want to be prompted at certain points during the upgrade, enter N in the next step to change the default value for PausePoint.

e Refer to the following table to determine your next action.

If	Do
all the values, including the Default values, are acceptable	enter **Y** and go to step 4
one or more of the values are not acceptable and you want to change	enter **N** and continue to the next substep (f)

*Example of system response (after entering **> N**):*

```
Enter load directory (default: /swd/sam21/):
```

f Enter the load directory for the CBM or SDM. The load directory is different for the CBM and SDM..

If you want to configure for	Do
CBM	enter **/sam21**, and go to step g
SDM	enter **/swd/sam21,** and go to step g

Example of system response:

```
Enter old load name:
```

g Enter the old load name for the shelf controller, or press the Enter key to ignore this option.

Example of system response:

```
Upgrade mode selection
 1 - single  2 - bulk
 h - help

Enter selection (102,h),(default:2):
```

h Enter the number next to one of the following upgrade modes:

- single if you want to upgrade all specified shelf controller nodes one at a time
- bulk if you want to upgrade all specified shelf controller nodes simultaneously

Example of system response:

```
Pause points
 1) For the single mode SC pair.
      1, before lock the first upgrade unit of "seed" pair.
      2, before warm swact.
      3, after "seed" pair upgraded.
      4, pause on all above conditions.
 2) For bulk SC upgrade pairs.
      5, before warm-swact.

      0, no pause point. If 0 applied, ignore all other
         pause points.
 Example: 1,3
Enter pause point (default: 0):
```

i Enter the pause points for the upgrade. Pause points allow you to perform manual checks at selected intervals during the upgrade process. At each specified pause point, you will be prompted to continue the upgrade. If you do not specify any pause points, you will not be prompted at any point to continue the upgrade unless an error condition occurs.

Example pause point entry:

```
Enter pause point (default: 0): 1,3
```

*These selections allow pause points for a Shelf Controller pair in single mode to pause before the first upgrade unit of the "seed" pair is locked **(1)** and after the pair is upgraded **(3)**.*

Example of system response:

```
Logging level selection
1 - VRB 2 - MNR 3 - MAJ 4 - CRT

Enter selection (1-4),(default: 3):
```

j Enter one of the logging levels: VRB, MNR, MAJ or CRT (default: MAJ). Upgrade logs are stored in a file in upgrade.log under /opt/nortel/sam21em/logs/. Use the logs for troubleshooting.

Example of system response:

```
The max time limitation
 Note: 0 means no time limitation

Enter time limitation (mins), (default 0):
```

k Enter a time limitation (in minutes) for the upgrade. If the upgrade cannot complete on all shelf controller pairs in the specified time, the non-upgraded pairs remain un-upgraded and the process ends. The default value **0** disables the limitation check.

Example of system response:

```
Alarm level selection
1 - CRT 2 - MAJ

Enter selection, (default: 2):
```

l Enter the alarm level (CRT, MAJ).

Example of system response:

```
Enter the max allowed alarm number, (default: 2):
```

m Enter the maximum alarm level and number allowed during the upgrade. If the current alarm state has a higher priority than is defined in this entry, the upgrade process pauses and the system notifies the end user.

Command format:
-a <alarm_level> -an <alarm_number>

Example command:

```
Enter the max allowed alarm number,(default:2) -a MAJ-an 2
```

Alarm level (Major)

Alarm number

The entries in the previous example allow a maximum number of two Major (MAJ) alarms during the upgrade process. In this case, if three MAJ alarms occur in the element server for the pair, the upgrade tool pauses. If one MAJ alarm occurs, the upgrade tool ignores it and continues the upgrade process. If one Critical (CRT) alarm occurs, the upgrade tool pauses because CRT alarms have a higher priority than MAJ alarms.

Example of system response:

```
NewLoadFileName : 11.0.0.0409151320
SCList          : SC0,SC1
LoadDirectory   : /sam21
OldLoadName     :
UpgradeMode     : single
PausePoint      : 0
LoggingLevel    : CRT
MaxTime         : 0
AlarmLevel      : CRT
AlarmNumber     : 3

Is this information correct? [Y|N]:
```

n Review the values displayed in the system response and refer to the following table to determine your next action.

If	Do
you want to confirm the selections for configuration	enter **Y**. Note the following system response, and go to step o.
you do not want to confirm the selections for configuration	enter **N** and return to step b on page 1312, or go to step 13 to exit the upgrade tool

Example of system response:

```
Current configuration:
-------------------------------------------------------------
New load file name                        : 11.0.0.0409151320
Old load name                             :
Load directory name                       : /sam21
Upgrade mode                              : single
Check point                               : 0
log level                                 : CRT
LC lists                                  : SC0,SC1
Max time for doing upgrade                : No time limitation
Max parallel number when bulk upgrade     : 8
Allowed highest alarm level               : CRT
Allowed maximum alarm number              : 3
```

o The procedure for configuring upgrade-related options is completed. To continue the upgrade process, go to step 3.

3 Press **Enter** to return to the Main menu for the Shelf Controller upgrade tool.

Example of system response:

```
Main menu for SC upgrade tool
1  - Display all SC pairs
2  - Configure upgrade-related options
3  - List current upgrade configurations
4  - Enter Upgrade Menu

x  - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

4 Enter the Upgrade menu for the Shelf Controller tool. Enter:

> 4

Example of system response:

```
Upgrade menu for SC upgrade tool
1  - Prepare
2  - Pre-check
3  - Upgrade
4  - Query upgrade status
5  - Post-check

x  - Exit

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

5 Select the Prepare option. Enter:

> 1

Example of system response:

```
Upgrade menu for SC upgrade tool
1  - Prepare
2  - Pre-check
3  - Upgrade
4  - Query upgrade status
5  - Post-check

x  - Exit

Enter selection (1-5,x):
Configured load is available.
Invalid SC nodes: SC1

==============Upgrade Schedule==============
Group 1 :SC0
Estimated total time :660 seconds
```

Check to see if the load is available in the CBM or SDM (as the example shows). Make an upgrade plan for the Shelf Controller and calculate the estimated time (in seconds) for the upgrade. The example shows an estimated total time of 660 seconds.

If the load	Do
is not available, the system responds: `SC load file doesn't exist. Please check and try later.`	return to step b on page 1312
the load is available	step 6

6 Perform a pre-check. At the Upgrade menu, enter:

> 2

Example of system response:

```
SAM21EM is alive.
Configured load is available.

Checking SC nodes state...
Group 1
 SC0 is ready to upgrade.

Upgrade Status Report:
SC node                  : SC0
Upgrade status           : Upgrade not started
SCUnitUpgrade order      : slot7 (inactive), slot9 (active)
Estimated time left      : 11 minutes

SC0-0 slot7 ip: 47.142.128.182
 SCUnit Status:
   Administrative state  : Unlocked
   Operational state     : Enabled
   Activity state        : Active
   Card status           : None

 Total Alarms:
  Critical alarms        : 0
  Major alarms           : 0

 Load name               : 11.0.0.0410071440

SC0-1 slot9 ip: 47.142.128.183
 SCUnit status:
   Administrative state  : Unlocked
   Operational state     : Enabled
   Activity state        : Inactive
   Card status           : None

 Total Alarms:
  Critical alarms        : 0
  Major alarms           : 0

 Load name               : 11.0.0.0410071440
```

Review the information in the system response, and perform the following steps:

a Check the status of the SAM21 manager server (SAM21EM). If the manager is not alive, go to step 8 on page 1308 of the Prerequisites procedure.

b Verify that the load is available on the load server. If the load is not available, go to step 8 on page 1308 of the Prerequisites procedure.

c Clear any existing alarms.

d Verify that the two physical units of the shelf controller pair are in service.

If	Do
any of the pre-check conditions is not met	resolve the conditions and continue to step e to proceed with the upgrade process
all the pre-check conditions are met	step e

e The pre-check procedure is completed. The system automatically returns to the Upgrade menu for the SC upgrade tool.

Example of system response:

```
Upgrade menu for SC upgrade tool
1  - Prepare
2  - Pre-check
3  - Upgrade
4  - Query upgrade status
5  - Post-check

x  - Exit

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

To continue the upgrade process, go to step 7.

7

ATTENTION
The automatic upgrade tool does not allow provisioning activity on the system while the upgrade is in progress.

Upgrade the configured Shelf Controller nodes. When the upgrade starts, the system performs another pre-check and displays the upgrade status. If any of the problems or conditions in the following table occur, resolve the problem as indicated.

If	Do
pause points are enabled by the configuration step (step 2 on page 1312), when the tool pauses at the specified intervals during the upgrade	enter the desired value(s), and continue with this step
the Shelf Controller has an active ATM link	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. If all the connections are in the yellow state, then SWACT the SAM21 Shelf Controller at a period of low activity before proceeding. If some of the connections are in the green state and some are in the yellow state, 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. Then return to this procedure and continue with this step.

If	Do
the Communications Server LAN (CS LAN) is provided by 8000-series Ethernet Routing Switches (formerly known as 8000-series Passport router switches)	procedure “Reprovision Ethernet Routing Switch 8600 port to auto-negotiate” in *Upgrading the SAM21 Shelf Controller*, NN10067-461. *(This procedure is required only once.)* When the action is completed, return to this procedure and continue with this step.
the real alarms on the Shelf Controller card exceed the configured alarm state	perform the appropriate alarm clearing procedures. When the action is completed, return to this procedure and continue with this step.
the upgrade is in progress, and you want to query the overall status of the upgrade (for example, if the upgrade is taking longer than expected)	launch another telnet or SSH session to the server, and enter: **>/opt/nortel/sam21em/bin/ scuptool.sh -query**
you have an AAL1 solution, and the system displays the following message: “SWACT denied. The inactive shelf controller does not have a complete set of redundant ATM connections. A SWACT would isolate the affected gateways, resulting in an outage. Please resolve any issues with the ATM connections from the gateways before requesting a SWACT. Please select from the following: Retry Abort.”	wait two minutes and then retry
no problems exist	continue with the instructions in this step

To begin the upgrade, select the Upgrade option from the main menu. Enter:

> 3

The upgrade tool

- provisions the software load in the inactive shelf controller card
- prompts for confirmation that it can lock the inactive Shelf Controller card if pause points were configured in step 2i

Example of system response with pause points configured:

Note: The entire system response as shown below will not necessarily appear instantaneously. The system will display some output, then pause, then continue. Such pauses are normal.

```
==============Upgrade Schedule==============
Group 1 SC0

Start upgrade at 2004-11-10 02:35:07.152
Upgrading with no time limitation.
Group 1
Upgrade Status Report:
SC Node               :  SC0
Upgrade Status        :  Upgrade starting.

SCUnitUpgrade order   :  slot7 (inactive), slot9 (active)
Start time            :  2004-11-10 02:35:07.542
Estimated time left   :  10 minutes

Provision software load on the inactive (first) unit.

Provisioning in progress...

Provision completed successfully.

Lock inactive (first) SC unit started.

Message received from the server:

Locking the inactive shelf controller will cause the shelf
controllers to operate in simplex mode. Do you wish to
proceed?
Please select from the following:
Continue

Answer:
```

8 If prompted to proceed (configured pause point), type

Continue

and press the Enter key.

The upgrade tool

- locks the inactive Shelf Controller card
- unlocks the inactive Shelf Controller card
- swacts the current active Shelf Controller card
- prompts for confirmation that it can lock the second inactive Shelf Controller card if pause points were configured in step 2i

Example of system response with pause points configured:

Note: The entire system response as shown below will not necessarily appear instantaneously. The system will display some output, then pause, then continue. Such pauses are normal.

```
Locking in progress...

Lock completed successfully.

Unlock the inactive (first) unit started.

Unlock in progress...

Unlock completed successfully.

Swact the active (second) unit started.

Swacting in progress...

Swact completed successfully.

Lock second inactive unit started.

Locking the inactive shelf controller will cause the shelf
controllers to operate in simplex mode. Do you wish to
proceed?
Please select from the following:
Continue

Answer:
```

9 If prompted to proceed (configured pause point), type

Continue

and press the Enter key.

The upgrade tool

- locks the newly inactive Shelf Controller Card
- unlocks the newly inactive Shelf Controller Card.

Example of system response:

Note: The entire system response as shown below will not necessarily appear instantaneously. The system will display some output, then pause, then continue. Such pauses are normal.

```
Locking in progress...

Lock completed successfully.

Unlock the second unit started.

Unlocking in progress...

Unlock completed successfully.

Upgrade Status Report:
SC node                : SC0
Upgrade status         : Both SC units upgrade finished successfully

SCUnitUpgrade order    : slot7 (inactive), slot9 (active)
Start time             : 2004-11-10 02:35:07.542
Stop time              : 2004-11-10 02:47:25.305
Elapsed time           : 12 minutes 17 seconds

SC0-0 slo7 ip: 47.142.114.222
SCUnit status:
Administrative state   : Unlocked
Operational state      : Enabled
Activity state         : Active
Card status            : None

Total alarms:
Critical alarms        : 0
Major alarms           : 1

Load name              : 11.0.0.04.09151320

SC0-1 slot9 ip: 47.142.114.223
SCUnit status:
Administrative state   : Unlocked
Operational state      : Enabled
Activity state         : Inactive
Card status            : None

Total alarms:
Critical Alarms        : 0
Major alarms           : 1

Load name              : 11.0.0.0409151320

All SC pairs upgrade finished.
```

10 The upgrade is completed. The system automatically returns to the Upgrade menu for the SC upgrade tool.

Example of system response:

```
Upgrade menu for SC upgrade tool
1  - Prepare
2  - Pre-check
3  - Upgrade
4  - Query upgrade status
5  - Post-check

x  - Exit

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

To continue with the post-upgrade (post-check) process, go to step step 11.

11 Perform a post-check to ensure that the load, state, and alarm conditions are correct. To display the data, enter:

```
> 5
```

Example of system response:

```
Upgrade Status Report:
SC node                 : SC0
Upgrade status          : Both SC units upgrade finished successfully

SCUnitUpgrade order     : slot7 (inactive), slot9 (active)
Start time              : 2004-11-10 02:35:07.542
Stop time               : 2004-11-10 02:47:25.305
Elapsed time            : 12 minutes 17 seconds

SC0-0 slo7 ip: 47.142.114.222
SCUnit status:
Administrative state    : Unlocked
Operational state       : Enabled
Activity state          : Active
Card status             : None

Total alarms:
Critical alarms         : 0
Major alarms            : 1

Load name               : 11.0.0.04.09151320

SC0-1 slot9 ip: 47.142.114.223
SCUnit status:
Administrative state    : Unlocked
Operational state       : Enabled
Activity state          : Inactive
Card status             : None

Total alarms:
Critical Alarms         : 0
Major alarms            : 1

Load name               : 11.0.0.0409151320
```

If	Do
you want to continue upgrading other Shelf Controller nodes	return to step b on page 1312
you do not want to continue upgrading other Shelf Controller nodes	The post-check is completed. The system automatically returns to the Upgrade menu for the SC upgrade tool. Refer to the system response that follows this table.

Example of system response:

```
Upgrade menu for SC upgrade tool
1  - Prepare
2  - Pre-check
3  - Upgrade
4  - Query upgrade status
5  - Post-check

x  - Exit

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

To complete the process, go to step 12.

12 Exit the Upgrade menu for the Shelf Controller upgrade tool and return to the Main menu for the Shelf Controller upgrade tool. Enter:

```
> x
```

Example of system response:

```
Main menu for SC upgrade tool
1  - Display all SC pairs
2  - Configure upgrade-related options
3  - List current upgrade configurations
4  - Enter Upgrade Menu

x  - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

13 Stop the upgrade tool and exit the CLUI. Enter:

```
> x
```

Example of system response:

```
SC Upgrade Manager Stopped successfully at 2004-11-09
05:37:25.813
```

14 The procedure is completed.

Gateway Controller

Before upgrading the Gateway Controller

Perform the required prerequisite upgrade as follows:

Network	GWC applies to:	Previous Upgrade
ATM	UA-AAL1 and PT-AAL2	SAM21 Shelf Controller on page 1280
IP	PT-IP, UA-IP, IAC, IAW, and CHS[1]	SAM21 Shelf Controller on page 1280
Tri-Modal	all applications	SAM21 Shelf Controller on page 1280

1.Includes IP International: CHS, IAC, PT-IP, and UA-IP

After upgrading the Gateway Controller

Perform the next required upgrade as follows:

Network	GWC applies to:	Next Upgrade
ATM	UA-AAL1 and PT-AAL2	Media Server 2000 Series on page 1413
IP	CHS - North America, PT-IP, UA-IP, IAW, and IAC[1]	Media Server 2000 Series on page 1413
	CHS - International	Enhanced Network and Message Switch on page 1636
Tri-Modal	all applications	Media Server 2000 Series on page 1413

1.Includes IP International: IAC, PT-IP, and UA-IP

About the Gateway Controller

The Gateway Controller (GWC) is a network component in the Communication Server 2000 (CS 2000) and CS 2000 - Compact products. Its function is to manage and manipulate signaling and bearer paths on various types of media gateways. It receives instructions from the CS 2000 XA-Core or Call Agent (CS 2000 - Compact) to perform functions such as create or release a connection, collect in-band digits and provide echo cancellation.

A GWC is commonly used to manage signaling and data paths or virtual connections between endpoints from one network component to

another. A GWC mediates these virtual connections with other GWCs, inside or outside the network, through the internet or with local line or trunk access devices or other 3rd party peripherals. These devices are known as gateways or media gateways.

Prepare to upgrade the gateway controller

This section provides details on specific items that users must be aware of prior to upgrading gateway controller (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. See the supported upgrade paths in the SN08 upgrade document, *Upgrading a Carrier Voice over IP Network*, NN10440-450.
Upgrade order for all GWC card types		Applicable to all solutions. See section Upgrade order for all GWC card types on page 1333.
Verify the value in the PKTRATE field of Table MNIPPARM is the same value as packetization rate of the GWCs defined in the Call Server 2000 Management tools (Configuration->Configure Network->packetization rate).		See *GWC Configuration Management*, NN10205-511, for instructions on checking the Packetization Rate configured for the GWCs.
Upgrade and downgrade call service impact		Applicable to all solutions. See Upgrade and downgrade call service impact on page 1335.
Ensure compliant characters in RMGC application domain name		Applicable to IP solutions (Integrated Access Wireline, Cable, IP). See Ensuring compliant characters in RMGC application domain name on page 1336.
Allocate time for a GWC upgrade		Applicable to all solutions. See Allocating time for a GWC upgrade on page 1336.

GWC upgrade preparation list

Item	√	Details
Impact of an upgrade on GWC configuration		Applicable to all solutions. See Impact of an upgrade on GWC configuration on page 1337.
Provision all of the ALGs required for the network.		See Provisioning ALGs in SN08 on page 1337
Review network firewall configuration.		See Network firewall configurations on page 1338

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 new GWC Upgrade Tool automatically upgrades the card types in the correct order.

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 *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Upgrade GWC card pairs from SN06.2 or SN07 to SN08 in the following order of card type:

Note: For definitions of the terminology in the list, refer to the Glossary of terms in *Gateway Controller Basics*, 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, SN07 to SN08 and SN08 to SN08 upgrades only) - see Note 1
5	SIP-T/APG/RA - see Note 2

GWC card type upgrade order

Order	GWC card type
6	APG/RA - see Note 2
7	SIP-T/APG - see Note 2
8	APG - see Note 2
9	SIP-T
10	Trunk
11	H.323
12	V5.2 trunk
13	Lines - includes CICM

Note 1: The Session Server (SS) was 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 *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Note 2: The APG functionality was removed in the SN07 release. All GWC service profiles and gateway profiles that were required to support the APG functionality (all profiles with “APG” in their names, such as, SIP_T_APG) are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles. It is recommended that the existing DPT GWCs that still use these profiles migrate to SIP-T or SIP_TINTL profile to optimize resource utilization (resources previously reserved for APG are released for other tasks). The Packet Media Anchor (in IP network solutions) is the replacement device for the APG functionality.

Note 3: The manual upgrade process does not support parallel upgrades. 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 it 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 *Upgrading a Carrier Voice over IP Network*, NN10440-450 for a complete migration strategy for this feature.

It is assumed that an existing Audio Controller GWC is used to host the RMGC application. If commissioning a new GWC for RMGC in SN08, refer to appropriate procedures in *Gateway Controller Configuration Management*, 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.

Upgrade and downgrade call service impact (Sheet 1 of 2)

GWC type	SN06.2/07 -> SN08 Upgrade	SN08 -> SN08 Maintenance (patching)	SN08 -> SN07 Downgrade	SN08 -> SN06.2 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.
VRDN	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	ALL calls survive.	ALL calls 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.
MG 15000 Trunk	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	SOME calls may 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.

Upgrade and downgrade call service impact (Sheet 2 of 2)

GWC type	SN06.2/07 -> SN08 Upgrade	SN08 -> SN08 Maintenance (patching)	SN08 -> SN07 Downgrade	SN08 -> SN06.2 Downgrade
Line or H.323	Stable 2-party calls survive. Possible limited functionality after the swact. For SN07 to SN08 upgrade, H.323 gateway calls survive (except Cisco gateway). For unstable dialing, ringing, clearing or multi-party calls the behavior is unpredictable.	Stable 2-party calls survive. Possible limited functionality after the swact. For unstable dialing, ringing, clearing or multi-party calls the behavior is unpredictable.	SOME calls may survive. H.323 gateway calls survive (except Cisco gateway). Billing records may not be produced when calls go on-hook.	SOME calls may survive. Billing records may not be produced when calls go on-hook. H.323 gateway-based calls do not survive.
Note: This table omits the SN06 to SN08 upgrade/downgrade, which is supported for AAL1 solutions only. The AAL1 solution does not include GWC.				

Ensuring compliant characters in RMGC application domain name

If you are upgrading to SN08 and intend to use the Redirecting Media Gateway Controller (RMGC) application, you must 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 SN08, refer to procedures in *Gateway Controller Configuration Management*, 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 the GWC load package to CS 2000 Core Manager or CBM is 5 minutes.
- Time to perform a GWC node warm SWACT is 1 minute.
- Time to carry out the post upgrade call processing check for each GWC node is 2 minutes.
- The total upgrade time for all GWCs depends on the upgrade mode used in the GWC Upgrade Tool (see section Configurable options on page 1363 of procedure Upgrade the GWC using the GWC Upgrade Tool) and the number of different GWC card types.

Impact of an upgrade on GWC configuration

Once the CS 2000 Core Manager or CBM is upgraded, you cannot provision GWCs until the CS 2000 Management software package is upgraded and configured on the CS 2000 Management Tools server.

Provisioning ALGs in SN08

There is a very limited set of provisioning that can be done in an SN08 SESM + SN07 GWC configuration provided that steps are taken prior to upgrading the SESM to SN08 to get ALG

datafill properly sent to the GWC.

New ALG creations and or changes to an existing ALG and subsequent gateway associations to the ALG while SESM is on SN08 and GWC is on SN07 with ALG patch is not supported. You must create all of the ALGs and associate each with at least 1 gateway in order for the data to get populated in the gwc before upgrading SESM to SN08, for example, while SESM is on SN07 and GWC is on SN07 with their respective ALG patches activated. Provisioning the ALGs alone without a gateway association is not sufficient for proper behavior during the interim period.

Provision all of the ALGs required for the network. Associate at least 1 gateway(mta) even if its a dummy gateway to every provisioned ALG in the network. This will populate the gwc with the ALG data. Proceed with associating as many gateways as required. Type the following command:

SESM - SN07 + ALG patch, GWC -SN07 + ALG patch

Upgrade SESM to SN08.Continue associating gateways to existing ALGs. if required. Do not create or change existing ALG data. Type the following command:

```
SESM - SN08 + GWC -SN07 + ALG patch:
```

ew ALGs or changes to existing ALGs can be made. New associations or changes to existing associations can be made. Type the following command:

```
SESM - SN08 + GWC -SN08:
```

Network firewall configurations

Prior to (I)SN07 upgrade, review network firewall configurations to ensure that rules are not in place that would block fragmented UDP packets on IP port 2427.

Refer to RFC 3435 at URLhttp://www.ietf.org or PKT-SP-EC MGCP-I10-040402 at URL http://www.cablelabs.org for more details on UDP transmission.

CS 2000 call agent identifier

When upgrading from a pre-SN07 load to an SN08, 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 network zone ID (previously referred to as middlebox ID) for each network address translator (NAT) provisioned in your network. When provisioning a NAT, the system generates a zone ID. Starting in SN07, the Call Agent ID is incorporated in this automatically generated number. This ensures the uniqueness of all NAT zone 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 zone 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, the following IDs are also automatically generated using the CS 2000 call agent ID:

- zone IDs for limited bandwidth links (LBL) and composite NAT and LBL zones
- middlebox IDs for policy enforcement points (PEP) servers and application layer gateways (ALG)

Upgrading GWCs containing NATs or PEP servers

During an upgrade from pre-SN07 to SN08, the need to upgrade the zone 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 zone 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 SN08, it is recommended that you perform one of the following procedures:

- Upgrade without soak test
- Upgrade with soak test on page 1341

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 1343.

   The CS 2000 Management Tools software generates new IDs for the following items that have already been provisioned:

   - network address translators (NAT)
   - policy enforcement point (PEP) servers

2. Upgrade all GWC cards that will support internet transparency media endpoints in SN08.

   To upgrade a GWC card, refer to Overall GWC upgrade process - automated on page 1356.

   As part of this upgrade, the new zone 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 zone IDs on the CICM Element Manager must also be upgraded to reflect the new zone IDs.

   This must be done before the CICM is upgraded to SN08.

   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 SN08.

   To upgrade a GWC card, refer to Overall GWC upgrade process - automated on page 1356.

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 IDs for the following items that have already been provisioned.

   - network address translators (NAT)
   - 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 zone 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 SN08.

   To upgrade a GWC card, refer to Overall GWC upgrade process - automated on page 1356.

   As part of this upgrade, the new zone 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 zone IDs on the CICM Element Manager must also be upgraded to reflect the new zone IDs.

   This must be done before the CICM is upgraded to SN08.

   For information on working with the CICM, refer to your CICM customer documentation.

7. Repeat steps 1 through 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 zone ID (previously referred to as middlebox ID) for each network address translator (NAT) provisioned in your network. When provisioning a NAT, the system generates a zone ID. Starting in SN07, the Call Agent ID is incorporated in this automatically generated number. This ensures the uniqueness of all NAT zone 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 zone 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, the following IDs are also automatically generated using the CS 2000 call agent ID:

- zone IDs for limited bandwidth links (LBL) and composite NAT and LBL zones
- middlebox IDs for policy enforcement points (PEP) servers and application layer gateways (ALG)

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 from pre-SN07 to an SN08 load.

Note: For additional information on when and how to set the call agent ID as part of an SN08 upgrade, refer to CS 2000 call agent identifier on page 1339.

The call agent ID value must be set before you can provision any of the following:

- NAT devices
- PEP servers
- LBLs
- composite NAT and LBL zones
- ALGs

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 SN08. Specifically, the CS 2000 GWC Manager and Nodes Configuration applications must be upgraded.

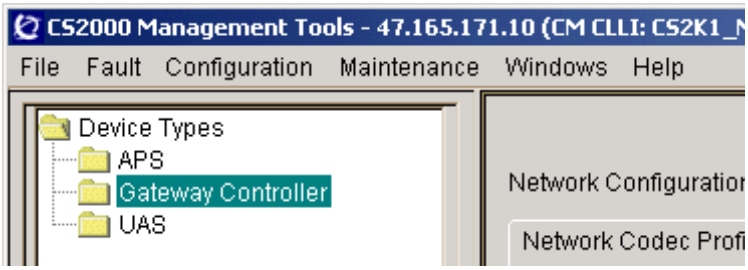
For details, refer to the upgrades NTP for your solution.

Note: For additional information on when and how to set the call agent ID as part of an SN00 upgrade, refer to CS 2000 call agent identifier on page 1339.

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.

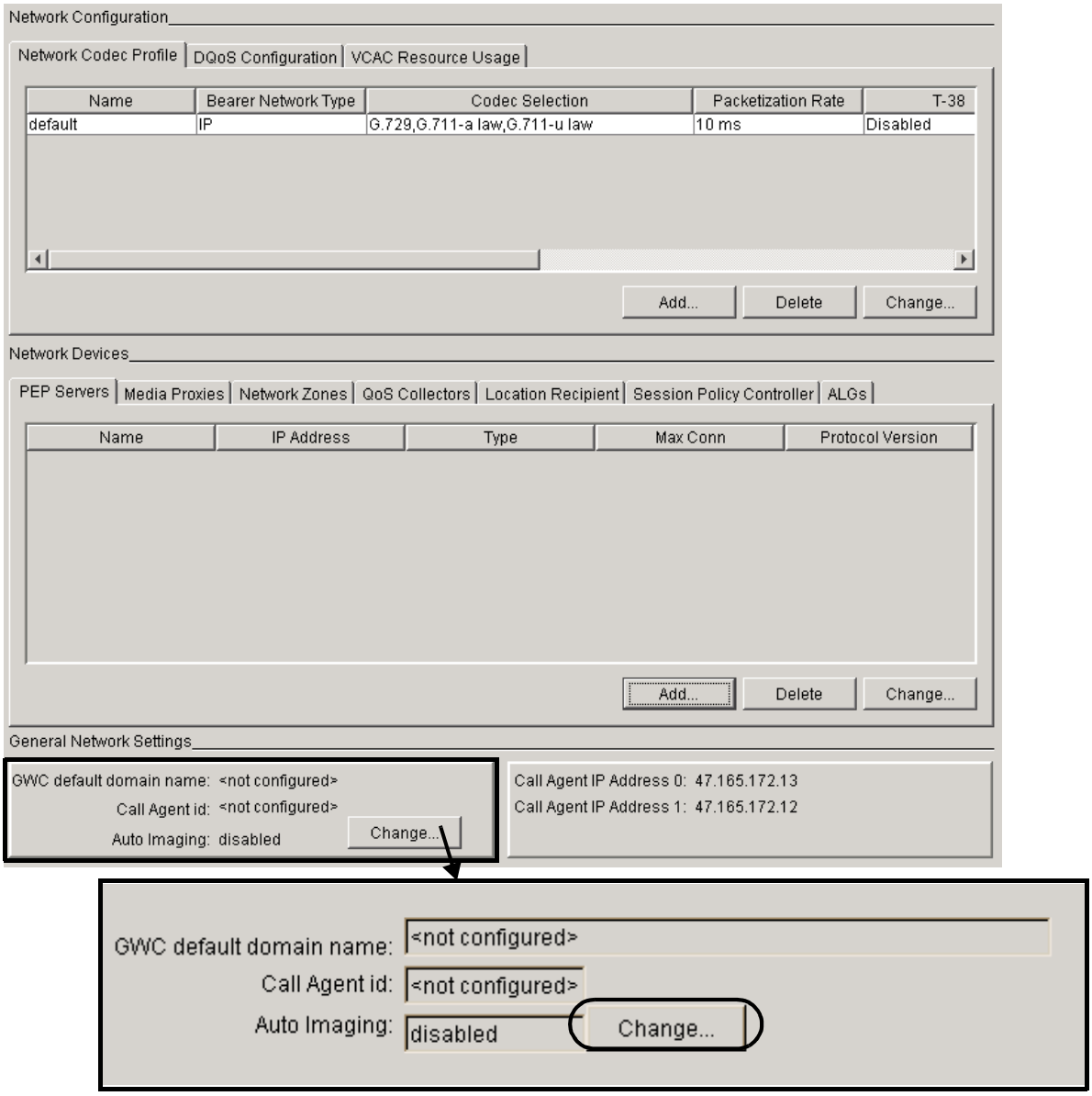


2 Note the current setting for Call Agent id at the bottom of the screen.

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.

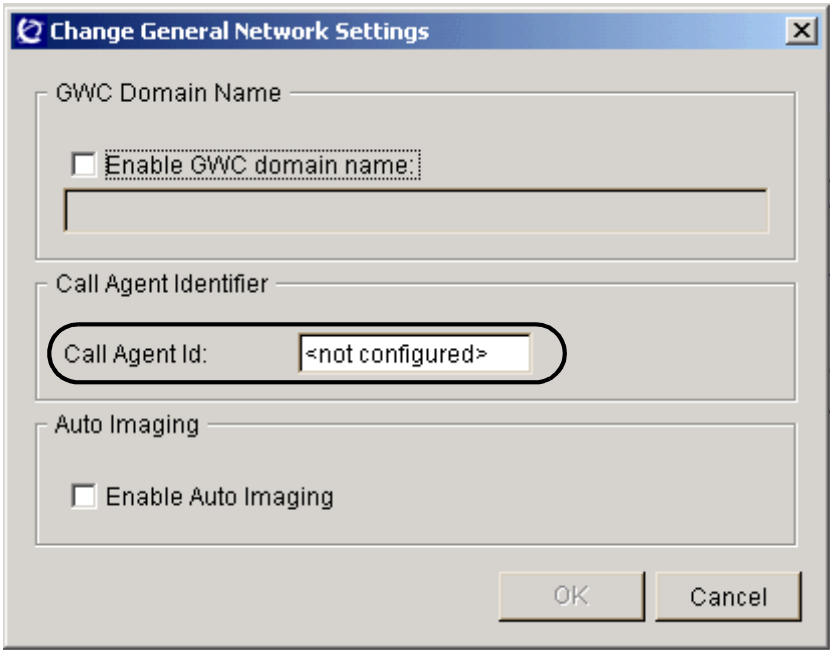


3 Determine your next step using the following table:

If you wish to	Do
set the call agent ID for the first time	step 4
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.



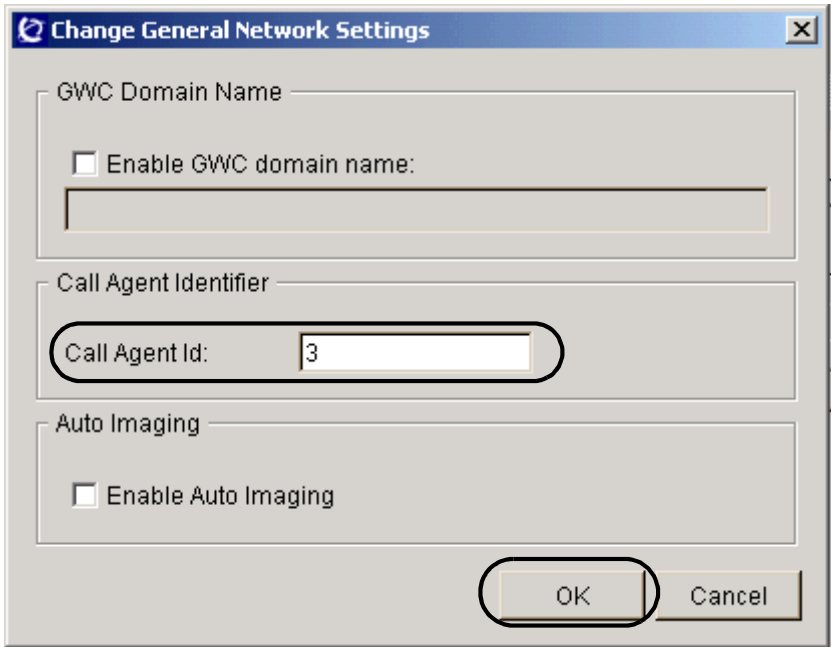
b Click in the Call Agent id field and assign a call agent ID value.

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 zones which have already been provisioned to incorporate the newly provisioned call agent ID into the NAT zone 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.

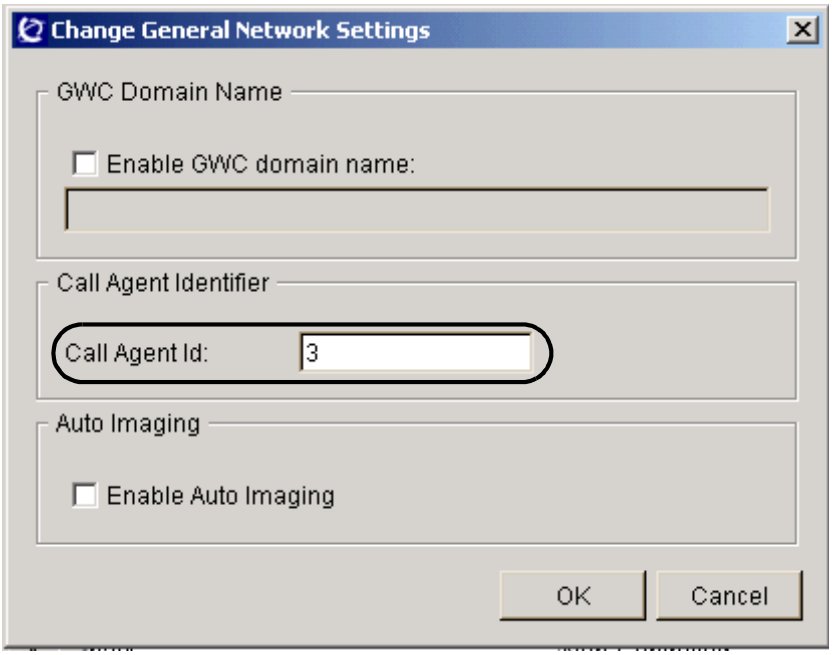
5

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.

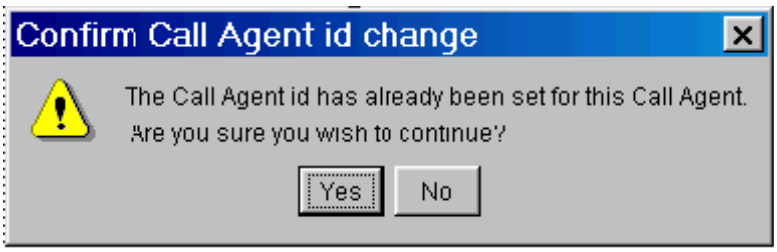
The range of valid values is between 1 and 255 inclusive. Contact your site system administrator to determine the call agent ID you should be using.

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 zone ID for NATs provisioned after the change has been made. The zone 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.

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 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 Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671.

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/gwcConFig.sh
/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 Type the root password for the CS 2000 Core Manager or the CBM and press the Enter key.

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, type 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, type the hostname of the SAM21 EM server and press the Enter key. Otherwise, continue with step 14.

13 If prompted, type 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.

Overall GWC upgrade process - automated

This section outlines the new automated process using the GWC Upgrade Tool for upgrading selected GWCs and applying patches.

Note 1: Starting in SN08, the automated process is the recommended process for upgrading the GWC. However, if you wish to use the original manual process, refer to procedure Overall GWC upgrade process - manual in *Upgrading the Gateway Controller*, NN10196-461.

Note 2: Before you begin, make sure that you have researched and addressed all the preparatory items described in procedure Prepare to upgrade the gateway controller in *Upgrading the Gateway Controller*, NN10196-461.

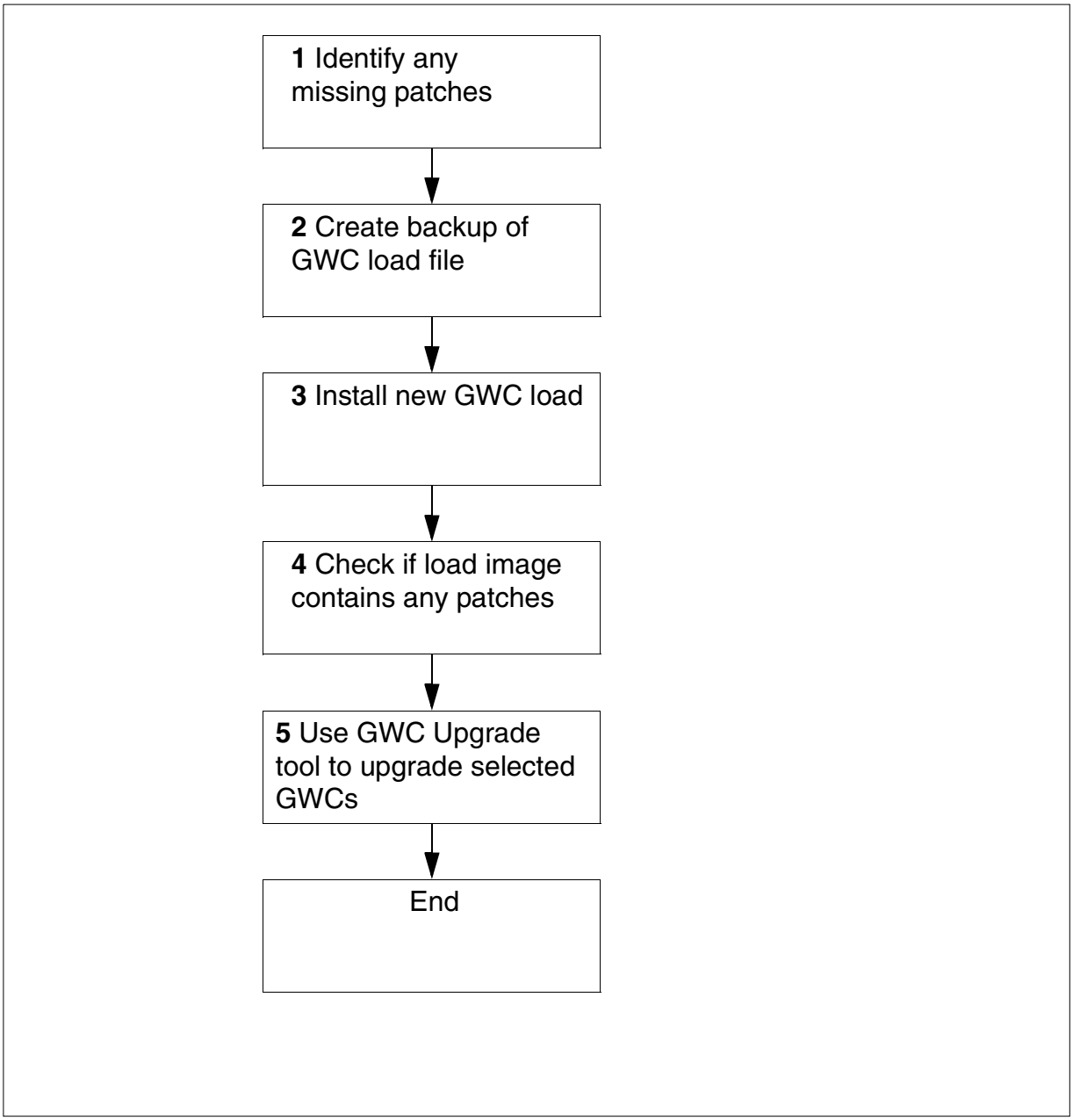
ATTENTION

For IP network solutions only (starting in SN07), the call agent identifier (ID) must be set for the CS 2000. This should typically be done prior to upgrading the GWC cards. For details, refer to section “CS 2000 call agent identifier” in *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Summary flowchart

The following flowchart summarizes the overall GWC upgrade process. The numbers relate to the steps of the detailed procedure in section Overall GWC upgrade procedure on page 1358 following the flowchart.

Summary of the overall GWC upgrade procedure



Overall GWC upgrade procedure

1 If necessary, complete the sub-steps (a) and (b) using one of the tools available at www.nortelnetworks.com.

Note: These steps may not be needed if you have obtained the soaked load from Nortel Networks GNPS (with all the necessary patches applied).

To obtain the tools:

- Under Support & Training, select Software Downloads.
- Select the Browse Product Support tab (this is usually the default choice).
- Follow the three steps displayed on the page:
  Step 1 - Product Families: select Succession or Succession Communication Server 2000.
  Step 2 - Product menu: select Communication Server 2000.
  Step 3 - Content menu: select Tools, then press 'Go'.
- 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 tool Pre Upgrade Patch Calculator. Download these patches (if any) to the site and retrieve the patch files for the NPM to process using the NPM CLUI **getpatch** command.

b Perform a site-specific audit to identify any missing patches - use the tool Patch Audit.

2 For security, back up your existing software load using procedure Create a backup of the GWC load file on page 1402.

3 Install the new load using one of the following methods:

- from CD-ROM - use procedure Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 1351 in *Upgrading the Gateway Controller*, NN10196-461
- using ESD - use procedure Transfer and mount an ISO image delivered through ESD onto an SSPFS-based server on page 671 in *Upgrading the Gateway Controller*, NN10196-461

4 Check whether the load image contains any patches using procedure View the contents of a load file image on page 1404. If so, add the patches to NPM as described in step 1a.

5 Upgrade the GWCs:

a If a day or more has passed between completing step 1a and performing the upgrade, repeat step 1b, then continue to step 5b.

b Use the GWC Upgrade Tool to upgrade the GWCs. Refer to procedure Upgrade the GWC using the GWC Upgrade Tool on page 1360. The tool upgrades all selected GWCs to the given new load, and applies all available patches in NPM.

Note: Nortel Networks recommends that you apply all patches with status Released (R) and Propagated (P), take the image, and then apply the patches with status Verification (V). The GWC Upgrade Tool attempts to apply all available patches to all the GWCs. It is preferable not to have V status patches in a saved image, as these patches are normally applied to only one GWC.

If V status patches are found during the upgrade process, the GWC Upgrade Tool pauses to allow you to apply these patches manually.

GWC Upgrade Tool

The Main Menu contains all the options necessary for configuring and performing the automated GWC upgrade process.

```
Main Menu for GWC upgrade tool
1 -  Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

Upgrade the GWC using the GWC Upgrade Tool

Purpose of this procedure

This procedure describes how to upgrade the software load from which the GWC cards boot, located on the CS 2000 Core Manager 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 CS 2000 Core Manager or CBM. This procedure upgrades all selected GWC nodes 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 CS 2000 Core Manager 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 1351 in *Upgrading the Gateway Controller*, NN10196-461
- Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server on page 671 in *Upgrading the Gateway Controller*, NN10196-461

All the necessary patches must be loaded into NPM. Refer to procedure Overall GWC upgrade process - automated (step 1 on page 1358).

The NPM automated processes must be disabled. Refer to step 29 of this procedure.

If the Communication Server LAN (CS LAN) is provided by Nortel Networks Ethernet Routing Switch 8600 routers, the port on the CS LAN router must be set to “auto-negotiate”. The port is normally configured that way. However, if the setting is incorrect, the port must be reconfigured before launching the GWC Upgrade Tool. Refer to procedure Re-provision the Ethernet Routing Switch 8600 port to auto-negotiate on page 1400.

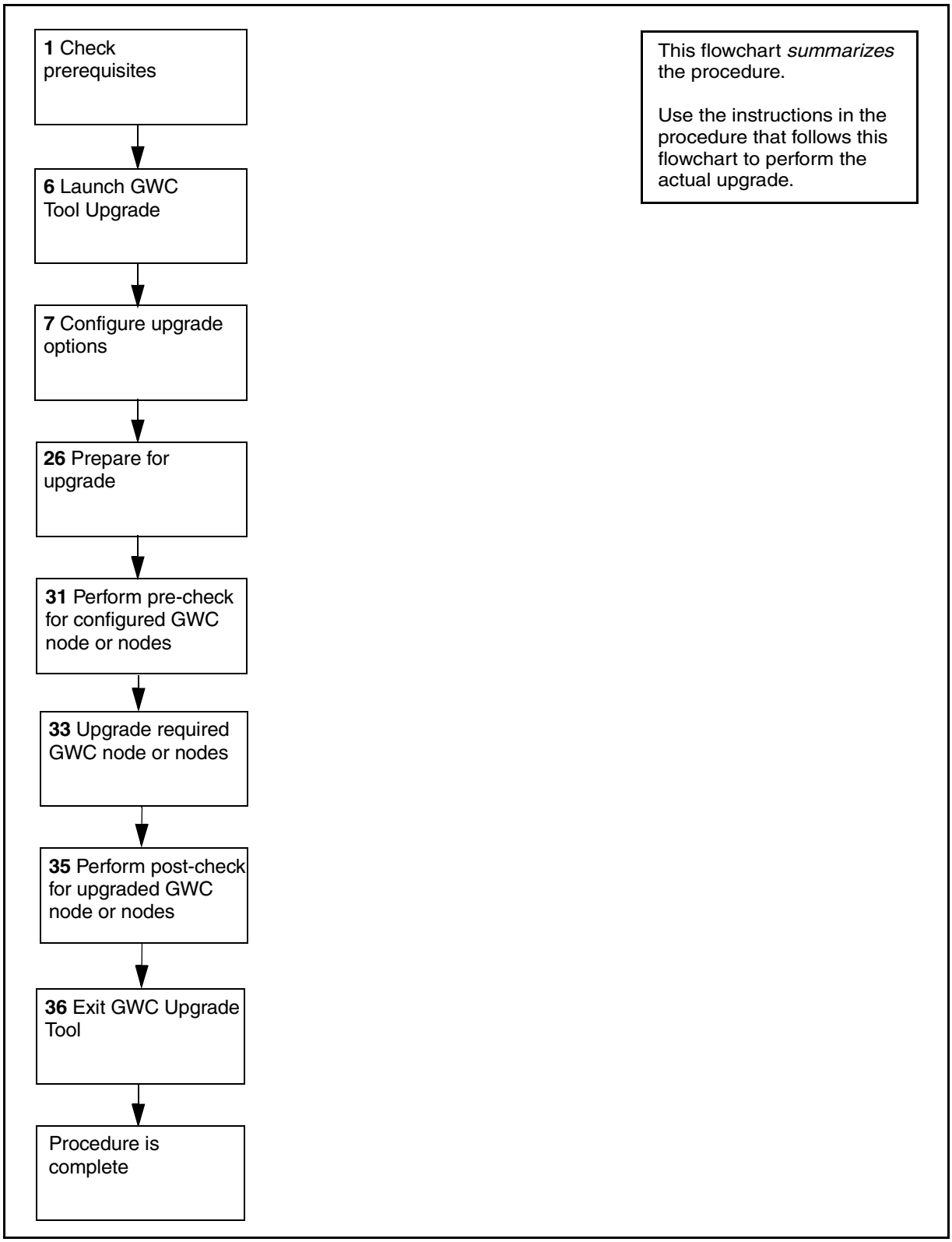
Overview

The GWC Upgrade Tool is distributed with the CS 2000 SESM package. The tool supports GWC upgrades via a command line user interface (CLUI). The tool is recommended as an alternative to the manual procedures (see procedure Upgrade a standby GWC card software load in *Upgrading the Gateway Controller*, NN10196-461), and automatically performs the following GWC upgrade operations:

- locks the inactive unit of the first selected GWC node (‘seed’ node), provisions it with a new load, and unlocks the unit
- busies the upgraded inactive unit, carries out a device audit, applies all available patches, returns the unit to service and swacts the ‘seed’ node
- locks the newly inactive unit of the ‘seed’ node, provisions it with the new soaked load, and unlocks the unit
- for all the other selected GWC nodes in turn (‘non-seed’ nodes) locks the inactive unit, provisions it with the new soaked load, unlocks the unit, and swacts the node
- locks the newly inactive unit of the ‘non-seed’ node, provisions it with the new soaked load, and unlocks the unit

The following flowchart provides an overview of the automated upgrade procedure. The numbers relate to the steps of the procedure in section Upgrade procedure on page 1366 following the flowchart.

Automatic upgrade overview



Configurable options

The user can configure 11 options in the GWC Upgrade Tool. Two options are mandatory, and one of them must be given a specific value. For the optional items, the user can just press the Enter key to accept the default values.

Option name	Mandatory (M) or optional (O)	Description	Default value
New Load File	M	The name of the new GWC load file. The user must specify a name. Refer to procedure Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 1351.	
GWC List	M	The GWCs to be upgraded. By default, all GWC nodes managed by the CS 2000 Manager and SAM21 Manager are selected.	All
Load Directory	O	The GWC load directory configured in CS 2000 SAM21 Manage. The default value is '/swd/gwc'. If CS 2000 Core and Billing Manager (CBM) was used, the user must change the load directory to '/gwc'.	current configured load path
New Load Name	O	The target load name of the given GWC load file. If the file name does not contain the GWC load name, the user must specify a valid GWC load name here. The new load name is used to query the patch list from NPM. By default, the new load file name should be LOAD_NAME.imag, for example, gn070ch.imag, gn070ch.	new load file name (excluding '.imag')
Old Load Name	O	The load upgraded from. The default value is ' ' (null). If the user ignores this option (the default), the upgrade manager server bypasses old load checking and all selected GWC nodes are upgraded automatically.	old load file name (excluding '.imag')

Option name	Mandatory (M) or optional (O)	Description	Default value
Upgrade Mode	O	Defines whether GWCs are upgraded singly or together. Three modes are available: **single** - All GWC nodes are upgraded one by one, ordered by GWC profile type and GWC ID. **bulk** - All GWC nodes within the same service group (for example, TRUNK, LINE) are upgraded at the same time. If patching is needed, the first selected 'seed' GWC node which is used to create the soak image uses single mode, and the other nodes that do not need patching use bulk mode. **mix** - In the same GWC profile group (for example, Trunk GWCs, Line GWCs), one GWC node is upgraded first. This enables the user to verify a specific type of GWC. After the first node is upgraded successfully, all the other GWC nodes within the same profile group are upgraded together.	bulk
Pause Point	O	Specifies the points at which the upgrade process pauses to allow the user to make manual checks. Seven options are available: **0** - No pause points; if 0 is selected, all other pause points are ignored. **1** - Pause before locking the first unit of the 'seed' GWC node. **2** - Pause after patches are applied to the 'seed' node. **3** - Pause before warm swact of the 'seed' node. **4** - Pause after warm swact of the 'seed' node. **5** - Pause after the 'seed' node is upgraded. **6** - Pause before warm swact of 'non-seed' nodes. Pause points 1 to 5 apply only to the 'seed' GWC node; pause point 6 applies to all other bulk upgrade GWC nodes.	0
Logging Level	O	Defines the default logging level of the GWC Upgrade Tool.	MAJ
Max Time	O	Defines the time limit (in minutes) for the upgrade. If the upgrade cannot complete all the GWC nodes in the specified time, the non-upgraded GWCs remain un-upgraded and the process ends. The default value **0** disables the time limit check.	0 (no time limit)

Option name	Mandatory (M) or optional (O)	Description	Default value
Alarm Level	O	Defines the alarm level of the in-service GWC unit that the GWC Upgrade Tool reports to the user. Values are: **MAJ** - major **CRT** - critical	MAJ
Alarm Number	O	Defines the acceptable alarm count, that is, the number of in-service GWC alarms of the specified alarm level at which the GWC Upgrade Tool reports to the user (see section Alarm checking on page 1365 for details).	2

Alarm checking

During the upgrade only the in-service GWC unit is checked for alarms, and only the critical and major alarms are checked. When the actual GWC alarms reach the defined alarm state, the upgrade pauses and the system displays a message to the user.

For example, if the alarm checking is set to the default values ‘MAJ 2’, the following table shows how the GWC Upgrade Tool behaves when different numbers of in-service GWC alarms occur:

In-service GWC alarms	Upgrade pauses?
CRT 0, MAJ 1	N
CRT 0, MAJ 2	N
CRT 0, MAJ 3	Y
CRT 1, MAJ 0	Y
CRT 1, MAJ 1	Y
CRT 2, MAJ 0	Y
CRT 2, MAJ 1	Y
CRT 2, MAJ 2	Y

For a further example, if the alarm checking is set to the values ‘CRT 2’, the following table shows how the tool behaves when different numbers of in-service GWC alarms occur:

In-service GWC alarms	Upgrade pauses?
CRT 0, MAJ 1	N
CRT 0, MAJ 2	N
CRT 0, MAJ 3	N
CRT 1, MAJ 0	N
CRT 1, MAJ 1	N
CRT1, MAJ 2	N
CRT 2, MAJ 0	N
CRT 2, MAJ 1	N
CRT 2, MAJ 2	N
CRT 3, MAJ 0	Y

Upgrade procedure

At the CS 2000 Management Tool interface

1 **Check prerequisites**
Check the prerequisites as described in section Prerequisites and guidelines on page 1360. Return to this procedure and carry out the additional prerequisite actions in steps 2, 3, and 5.

2 Ensure that you have a valid user ID and password to access the GWC Upgrade Tool.

a Telnet or SSH to the Sun server. Type:

```
> telnet <server>
```
or
```
> ssh -1 <user_ID> <server>
```
where <server> is the IP address or host name of the Sun server where CS 2000 SESM server resides.

and press the Enter key.

b When prompted, type your user ID and password, and press the Enter key.

3 Ensure that the operator belongs to one of the following groups authorized to launch the GWC Upgrade Tool: mgcmtc, mgcadm, emsmtc or emsadm. If necessary, refer to procedure "Setting up local user accounts on an SSPFS-based server" in *ATM/IP Solution-level Security and Administration*, NN10402-600. Type:

```
> id -a
```

and press the Enter key.

System response:

```
$ id -a
uid=104(ptm)  gid=105(succssn)
groups=105(succssn),1001(trkadm),1006(lnadm),
1011(mgcadm),1016(mgadm),1021(emsadm)
$
```

Group names

Note 1: CS 2000 SAM21 Manager must be installed in the same server as the GWC Upgrade Tool. CORBA, SESMService, NPM, and SAM21 Manager must be running in this server, otherwise the GWC Upgrade Tool cannot be launched.

Note 2: If NPM server is configured within the same server, it must be configured and running correctly. If NPM server is running with the Integrated EMS server, the PSE package within the same server must be configured and running correctly (and NPM may not appear in the system response below).

4 Refer to the following table to determine your next action.

If you are	Do
logged in as root	go to step 5
not logged in as root	change to the root user: type **su - root** , press the Enter key and continue at step 5

5 Check the status of the SAM21 element server and CORBA server to ensure they are running properly. Type:

```
> servquery -status all
```

and press the Enter key.

System response:

```
$ servquery -status all
APP NAME                STATUS
========                ======
DATABASE                RUNNING
CINOTIFIER              RUNNING
BACKUP_MANAGER          Group Started. Current status unavailable
BOOTP                   RUNNING
WEBSERVER               RUNNING
CORBA                   RUNNING
OMPUSH                  RUNNING
SESMService             RUNNING
WEBSERVICES             RUNNING
DDMSPROXY               RUNNING
ORA_AUTO_BACKUP         RUNNING
DELEGATE                RUNNING
ORA_ARCHIVE_ROTATOR     RUNNING
NPM                     RUNNING
PROP_SRV                RUNNING
SAM21EM                 RUNNING
SNMP_POLLER             Group Started. Current status unavailable
QCA                     RUNNING
```

Server states

6 Launch GWC Upgrade Tool

Exit from root and start the GWC Upgrade Tool CLUI. Type:

```
> exit
> cd /opt/nortel/NTsesm/gwcuptool/bin
> ./gwcuptool.sh
```

and press the Enter key.

System response:

```
cd /opt/nortel/NTsesn/gwcuptool/bin
./gwcuptool.sh
Starting ....

Main Menu for GWC upgrade tool
1 -  Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

Within the GWC Upgrade Tool, after typing a menu option or other input value, press the Enter key. Details of the Main Menu options are as follows:

1 - Display all GWC nodes
This option is to query the name and card type for all GWC nodes.

Example system response:

```
Enter selection (1-4,x): 1

------------------------------------------------------------
GWC-7   TRUNKNA
GWC-0   SMALL_LINENA
GWC-2   SMALL_LINENA
GWC-3   LARGE_LINENA
GWC-4   SMALL_LINENA
GWC-5   SMALL_LINENA
GWC-6   SMALL_LINENA
------------------------------------------------------------
Total: 7
```

2 - Configure upgrade-related options
This option is to configure upgrade options manually. The CLUI prompts the user to input the necessary information step by step. These configuration options are then effective throughout the whole upgrade process.

3 - List current configuration values
This option lists all the configuration options currently applied.

4 - Enter Upgrade Menu
This option is to enter the upgrade submenu.

x - Stop upgrade tool and exit CLUI
This option stops the GWC Upgrade Tool and exits the CLUI.

7 Configure upgrade options

From the Main Menu, enter:

> 2

System response:

```
Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 2

GWC upgrade configuration
[Step 1 - LOAD FILE NAME]
Enter the new load file name (Example: gn070bv.imag):
```

8 Enter the new GWC load file name. Ensure that the configured load file name exists in the load server (CS 2000 Core Manager or CBM).

Load name format:

nnnnnnn.nnnn

Example file name entry:

gn080bv.imag

System response:

```
Enter the new load file name (Example: gn070bv.imag): gn080bf.imag

[Step 2 - GWC LIST]
GWC list
Separate GWC names with commas, for example: GWC-1,GWC-2,GWC-3,GWC-5.

Enter the GWC list (Default: all):
```

9 Enter the GWC nodes to be upgraded. To select all available GWCs, just press the Enter key. To select specific GWCs, enter the names of those required (with no spaces between the names).

Note: If you select all available GWCs, the GWC Upgrade Tool automatically upgrades the card types in the correct order (see GWC card type upgrade order on page 1333).

Example list entry:

GWC-1,GWC-2,GWC-3,GWC-5

The system displays the current input configuration values.

Example system response:

```
Enter the GWC list (Default: all): GWC-2,GWC-4

[Step 3 - INPUT VALUES]
New Load File Name    : gn080bf.imag
GWC List              : GWC-2,GWC-4
Default values
Load Directory        : /swd/gwc/
New Load Name         : ""(ignored)
Old Load Name         : ""(ignored)
Upgrade Mode          : bulk
Pause Point           : 0(none)
Logging Level         : MAJ
Max Time              : 0 (no limitation)
Alarm Level           : MAJ
Alarm Number          : 2

Do you want to use these configuration values? [Y|N] (Default: N):
```

10 Review the values displayed in the system response and refer to the following table to determine your next action.

If you want to	Do
use the values	enter **Y** and go to step 26
change the values	enter **N** and continue at step 12

Note: In the downgrade procedure, you must enter **N** to reject the default values, otherwise you cannot continue with step 12 and the rest of the downgrade steps.

11 *System response (after entering **N**):*

```
Do you want to use these configuration values? [Y|N] (Default: N): n

Do not use default values
[Step 4 - LOAD DIRECTORY]
Default load directory formats are different for SDM and CBM.
If SDM is used, it should be "/swd/gwc".
If CBM is used, it should be "/gwc".
Enter the load directory. (Default: "/swd/gwc"):
```

12 Enter the load directory for CS 2000 Core Manager or CBM. The load directory formats are different, as listed below.

Note: The load directory must be as same as the “Load Info --> Path” value.

If you want to configure for	Do
CS 2000 Core Manager	enter **/swd/gwc**
CBM	enter **/gwc**

13 *System response (after pressing Enter):*

```
Enter the load directory. (Default: "/swd/gwc"): /swd/gwc

[Step 5 - NEW LOAD NAME]
Enter the new load name (Default: ""):
```

14 Enter the name of the new GWC load file. The load file name is used to query the patch list from NPM. If the file name does not contain the GWC load name, you must specify a valid GWC load name here, otherwise the GWC Upgrade Tool cannot retrieve the available patch list.

System response (after pressing Enter):

```
Enter the new load name (Default: ""):

[Step 6 - OLD LOAD NAME]
Enter the old load name (Default: ""):
```

15 Optionally, enter the name of the old GWC load file, that is, the file from which the load was upgraded. This is not normally needed; if you ignore this option, the upgrade manager server bypasses old load checking.

If you want to	Do
carry out a restricted upgrade, involving only GWCs running with a special load	enter the old GWC load file name
ignore this option ***Note:*** This is the recommended action.	press the Enter key

16 *System response (after pressing Enter):*

```
Enter the old load name (Default: ""):

[Step 7 - UPGRADE MODE]
Values:
1 - single
2 - bulk
3 - mix
h - help

Enter the upgrade mode (1-3,h) (Default: 2):
```

17 Enter the upgrade mode (see section Configurable options on page 1363.

If you want to	Do
upgrade all configured GWC nodes one at a time (*single*)	enter **1**
upgrade all configured GWC nodes in the same service group simultaneously (*bulk*)	enter **2**
upgrade all configured GWC nodes in the same profile group simultaneously (*mix*)	enter **3**
accept the default (*bulk*)	press the Enter key

18 *System response (after pressing Enter):*

```
Enter the upgrade mode (1-3,h) (Default: 2):

[Step 8 - PAUSE POINTS]
Values:
0 - no pause points

(1) For the first GWC node within the same GWC group.
1 - before locking first upgrade unit of "seed" node
2 - after patch applied to the "seed" unit
3 - before warm-swact
4 - after warm-swact
5 - after "seed" node upgraded

(2) For bulk upgrade of GWC nodes with the same GWC service type.
6 - before warm-swact

Separate numbers with comma, for example: 1,3,4
Enter the pause points (Default: 0):
```

19 Enter the pause points for the upgrade (see section Configurable options on page 1363). Pause points allow you to carry out manual checks at selected intervals during the upgrade process. Pause points 1 to 5 (see above screen) apply only to the patched 'seed' GWC node; pause point 6 applies to all other bulk upgrade GWC nodes.

To accept the default value (0), just press the Enter key.

Example pause point entry:

```
Enter the pause points (Default: 0): 1,3
```

These entries allow two pause points:
before the first upgrade unit of the "seed" pair is locked ***(1)***
and before a warm SwAct ***(3)****.*

System response (after pressing Enter):

```
Enter the pause points (Default: 0):

[Step 9 - LOGGING LEVEL]
Values:
1 - Verbose
2 - Minor
3 - Major
4 - Critical

Enter the logging level (1-4) (Default: 3):
```

20 Enter the required logging level: VRB, MNR, MAJ or CRT (default: MAJ). Upgrade logs are stored in a file in upgrade.log under /opt/nortel/sam21em/logs/. Use the logs for troubleshooting.

To accept the default value (MAJ), just press the Enter key.

System response (after pressing Enter):

```
Enter the logging level (1-4) (Default: 3):

[Step 10 - TIME LIMIT]
Note: 0 means no time limit

Enter the time limit in minutes (Default: 0):
```

21 Enter a time limit (in minutes) for the upgrade. If the upgrade cannot complete all the GWC nodes in the specified time, the non-upgraded GWCs remain un-upgraded and the process ends.

The default value (0) disables the time limit check.To accept the default value, just press the Enter key.

In the Prepare step (see step 26), this value is compared with the estimated time for the upgrade. If the upgrade cannot be completed within the given time limit, the Prepare step fails.

System response (after pressing Enter):

```
Enter the time limit in minutes (Default: 0):

[Step 11 - ALARM LEVEL]
Values:
1 - Critical
2 - Major

Enter the alarm level (Default: 2):
```

22 Enter the required alarm level: CRT or MAJ. For details, refer to section Alarm checking on page 1365.

To accept the default value (MAJ), just press the Enter key.

System response (after pressing Enter):

```
Enter the alarm level (Default: 2):

[Step 12 - ALARM NUMBER]

Enter the maximum allowed alarm number (Default: 2):
```

23 Enter the maximum number of alarms allowed during the upgrade. For details, refer to section Alarm checking on page 1365. If the current alarm state has a higher priority than the alarm number defined in this entry, the upgrade process pauses and the system notifies the user.

To accept the default value (2), just press the Enter key.

The entries in the example allow a maximum of two Major alarms during the upgrade process. In this case, if three Major alarms occur during the upgrade, the GWC Upgrade Tool pauses. If one Major alarm occurs, the tool ignores it and continues the upgrade process. If one Critical alarm occurs, the tool also pauses, because Critical alarms have a higher priority than Major alarms.

System response (after pressing Enter):

```
Enter the maximum allowed alarm number, (Default: 2):

New Load File Name    : gn080bf.imag
GWC List              : GWC-2,GWC-4
Load Directory        : /swd/gwc
New Load Name         :
Old Load Name         :
Upgrade Mode          : bulk
Pause Point           : 0
Logging Level         : MAJ
Max Time              : 0
Alarm Level           : MAJ
Alarm Number          : 2

Is this information correct? [Y|N] (Default: N):
```

24 Check the upgrade configuration options. Review the values displayed in the system response (see above screen) and decide whether or not to proceed with the upgrade.

If	Do
you want to confirm the upgrade configuration options	enter **Y**. Note the following system response, and go to step 26
you do not want to confirm the upgrade configuration options	enter **N** , then return to step 7 to re-enter the options, or go to step 36 to exit the GWC Upgrade Tool

25 *System response (after entering **Y**):*

```
Is this information correct? [Y|N] (Default: N): y

Current configuration values:
 GWC load file: gn080bf.imag
 New load name: GN080BF
Load directory: /swd/gwc
  Working mode: bulk
 Selcted nodes: GWC-2,GWC-4
  Pause points: 0
      Max time: unlimited
Ignored alarms: MAJ 2
 Logging level: MAJ

Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

Note: After confirming the configuration, you can display the current configuration settings at any time by selecting option 3 from the Main Menu.

Example system response:

```
Enter selection (1-4,x): 3

Current configuration values:
 GWC load file: gn080bf.imag
 New load name: GN080BF
Load directory: /swd/gwc
  Working mode: bulk
 Selcted nodes: GWC-2,GWC-4
  Pause points: 0
      Max time: unlimited
Ignored alarms: MAJ 2
 Logging level: MAJ

Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

26 **Prepare for upgrade**

On completion of the configuration steps, you must select the Upgrade Menu to carry out the actual upgrade. From the Main Menu, enter:

> 4

System response:

```
Enter selection (1-4,x): 4

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

27 In the Upgrade Menu, select the Prepare option. Enter:

> 1

Example system response:

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

[1 Prepare step]

The following patches are available in NPM.
  1, NBF00G08
  2, NBF01G08
  3, NBF02G08
  4, NBF03G08
  5, NBF04G08
  6, NBF05G08
  7, NBF06G08
  8, NBF07G08
  9, NBF08G08
  10, NBF09G08
  11, NBF11G08
  12, NBF12G08
  13, NBF13G08
  14, NBF14G08
  15, NBF15G08
  16, NBF17G08
Please disable the NPM automated processes.
```

28 Check that the load is available in CS 2000 Core Manager or CBM.

If the load	Do
is not available, the system displays the following message: `GWC load file doesn't exist. Please check and try later.` (see GWC load not available on page 1392)	return to step 8
is available	continue at step 29

29 Disable the NPM automated processes.

a Log in to the NPM GUI:
- Select "System" from the tool bar.
- Select "Plans..." from the menu.
- Click on the "Plan List" tab.
- If any of the plans in the list have "Enabled" checked, they must be disabled. For each plan that is enabled, highlight the plan in the menu and click on the "Disable" button at the bottom.

OR

Log in to the NPM CLUI:
- Execute the command: getplan
- If any of the plans in the list have "Enabled" set to "Y", they must be disabled. For each plan that is enabled, execute the following to disable it:
enableplan <planname> OFF

b Keep a record of the plans that were disabled. These plans must be re-enabled at the end of the upgrade process.

30 Display and confirm the patch list.

Note: You must be assigned to user group "emsadm" to perform patching activities using the NPM.

a If patches were delivered on CD, insert the CD that contains the patches into the CD drive of the Sun server where NPM resides.

b Telnet to the Sun server where the NPM resides.

c When prompted, type your user ID and password, and press the Enter key.

d Change to the root user. Type **su - root** and press the Enter key.

e When prompted, type the root password and press the Enter key.

f If patches were delivered electronically, go to step l; otherwise continue at step g.

g Patches on CD:
Make a temporary directory for the patchlist file.
Type **mkdir /data/npm/tmp** and press the Enter key.

h Change the permissions on the temporary directory.
Type **chmod 777 /data/npm/tmp** and press the Enter key.

i In the temporary directory, create the .patchlist file for all the patches on the CD. Type **find /cdrom -name '*.patch' > /data/npm/tmp/current.patchlist** and press the Enter key.

j Access the directory you just created.
Type **cd /data/npm/tmp** and press the Enter key.

k Go to step v.

l Patches delivered electronically:
Make a directory for the patch files you want to install.
Type **mkdir /data/npm/patch_upgrade** and press the Enter key.

m Change the permissions on the newly created directory.
Type **chmod 777 /data/npm/patch_upgrade** and press the Enter key.

n Access the newly created directory.
Type **cd /data/npm/patch_upgrade** and press the Enter key.

o FTP to the ESD server. Type **ftp** <ESD_server> and press the Enter key.

p When prompted, type your user ID and password for the ESD server,.and press the Enter key.

q Set the transfer mode to binary. Type **ftp> bin** and press the Enter key.

r Transfer all the patches from the ESD server to the NPM.
Type **ftp> mget *.patch** and press the Enter key.

s Exit FTP. Type **ftp> quit** and press the Enter key.

t Verify that the patches are in the temporary directory on the Sun server. Type **ls** and press the Enter key.

u Change the permissions for the patch files in the directory. Type **chmod 777 *** and press the Enter key.

v Retrieve the patch files:
Verify that the NPM server application is running.
Type **servquery -status -group NPM** and press the Enter key.

Note: The NPM can be started by typing **servstart NPM**.

w Access the NPM command line user interface (CLUI).
Type **npm** and press the Enter key.

x When prompted, type your user ID and password, and press the Enter key.

y Retrieve the patch files for the NPM to process as follows:

- For patches from CD-ROM, type **npm> getpatch current.patchlist** and press the Enter key.

- For patches from ESD, type **npm> getpatch** <patch_filename> and press the Enter key,
where <patch_filename> is the name of the file that contains the names of the patch files to retrieve (name must end with ".patchlist"), or is an actual patch file.

z Exit the NPM CLUI. Type **npm> quit** and press the Enter key.

aa Change directory. Type **cd** and press the Enter key.

Note: You must change directory from the cdrom directory for the next command (eject cdrom) to execute successfully.

ab Eject the CD from the drive. Type **eject cdrom** and press the Enter key.

Example system response:

```
--{ Group-1 }-------------------------------------------------------
  GWC-2 SMALL_LINENA

--{ Group-2 }-------------------------------------------------------
  GWC-4 SMALL_LINENA
-------------------------------------------------------------------------
Estimated Time:  1 hour 5 minutes 30 seconds

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

The system displays the GWC upgrade plan and estimated upgrade time, then returns to the Upgrade Menu.

31 Perform pre-check

In the Upgrade Menu, select the Pre-check option. Enter:

> 2

Example system response:

```
Enter selection (1-5,x): 2

[2 Pre-check step]

--{ Group-1 }-------------------------------------------------------
  GWC-2 SMALL_LINENA ... passed

--{ Group-2 }-------------------------------------------------------
  GWC-4 SMALL_LINENA ... passed
-------------------------------------------------------------------------
Total:  1 hour 5 minutes 30 seconds

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

32 Check the pre-check conditions. Review the information in the system response (see above screen) as follows:

a Check that the CS 2000 GWC Manager, SAM21 Manager, and NPM servers are running.

b Check that neither GWC card has a hardware alarm.

c Verify that one GWC card is in service, and the other card is hot-standby.

If	Do
any of the pre-check conditions is not met (see Pre-check failure on page 1392)	resolve the error conditions (go to step 4 to activate the servers, clear any hardware alarms, correct the status of the GWC cards), then continue the upgrade process at step 33
all the pre-check conditions are met (the screen displays "`passed`")	continue the upgrade process at step 33

33 **Upgrade GWC nodes**

In the Upgrade Menu, select the Upgrade option. Enter:

```
> 3
```

Internal procedures

At the start of the upgrade, the GWC Upgrade Tool performs the pre-check again. During the upgrade, the system displays a continuous log of the upgrade status (the log freezing may indicate a problem with one of the internal upgrade procedures). You can also use the query option (see Query upgrade status on page 1387) to display the upgrade status. If any unexpected problems occur, the system normally prompts you for a response or confirmation before continuing.

If pause points were enabled during configuration (see step 19), the tool pauses at the specified points and waits for you to carry out the required manual checks. When you have finished, enter **Continue** to continue the upgrade.

During the upgrade, the GWC firmware flash is enabled automatically.

There are two different internal upgrade procedures:

- For the 'seed' GWC node there are 16 steps. The 'seed' node is based on the upgrade order of the GWC card types, and GWC node ID. The GWC Upgrade Tool automatically selects

the ‘seed’ node from the GWC list entered by the user (see step 9).

- For all other (‘non-seed’) nodes there are 11 steps. The tool automatically upgrades the other nodes when the ‘seed’ is upgraded successfully.

Example system response - ‘seed’ node:

```
Enter selection (1-5,x): 3

[3 Upgrade step]

--{ Group-1 }------------------------------------------------------
  GWC-2 SMALL_LINENA

--{ Group-2 }------------------------------------------------------
  GWC-4 SMALL_LINENA
------------------------------------------------------------------
Estimated Time:  1 hour 5 minutes 30 seconds

--{ Group-1 }------------------------------------------------------
  GWC-2 SMALL_LINENA ... passed

--{ Group-2 }------------------------------------------------------
  GWC-4 SMALL_LINENA ... passed
------------------------------------------------------------------
Total:  1 hour 5 minutes 30 seconds

Group-1 started
GWC-2: Upgrade task is started.
GWC-2 [1/16]  Busy the hot-standby first unit.(GWC-2-UNIT-1)
GWC-2 [2/16]  Lock the inactive first unit. (GWC-2-UNIT-1)
GWC-2 [3/16]  Change the load of locked first unit. (GWC-2-UNIT-1)
GWC-2 [4/16]  Unlock the first unit. (GWC-2-UNIT-1)
GWC-2 [5/16]  Waiting for the first unit to be hot-standby. (GWC-2-UNIT-1)
GWC-2 [6/16]  Upgraded first unit is hot-standby. (GWC-2-UNIT-1)
GWC-2 [7/16]  Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Apply request was attempted by the NPM server.
GWC-2 [8/16]  Patches are applied with the upgraded first unit (GWC-2-UNIT-1)
GWC-2 [9/16]  Waiting for the patched unit to be hot-standby (GWC-2-UNIT-1)
GWC-2 [10/16] Patched unit is hot-standby, load imaging is started(GWC-2-UNIT-1)
GWC-2 [11/16] GWC load imaging is finished. Perform the warm-swact(GWC-2-UNIT-0)
GWC-2 [12/16]  Warm-swact is finished, busy the second unit. (GWC-2-UNIT-0)
GWC-2 [13/16]  Locking the second unit. (GWC-2-UNIT-0)
GWC-2 [14/16]  Second unit is locked. (GWC-2-UNIT-0)
GWC-2 [15/16]  Change load of the locked second unit. (GWC-2-UNIT-0)
GWC-2 [16/16]  Second unit is booted up with the soaked load. (GWC-2-UNIT-0)
GWC-2 Upgrade finished successfully.
Group-1 finished
 Elapsed Time: 16 minutes 25 seconds
Remaining Time: 24 minutes 15 seconds
```

Upgrade steps for the ‘seed’ GWC node

This section assumes that GWC-2 is the ‘seed’ node, GWC-2 UNIT-0 is in service, GWC-2 UNIT-1 is hot-standby, the new load file name is gn080as.imag, and the load version is GN080AS.

The GWC Upgrade Tool automatically performs the following actions:

1. Busies the inactive unit GWC-2 UNIT-1 in the GWC EM.
2. Locks the inactive unit GWC-2 UNIT-1 in the SAM21 EM.
3. Provisions GWC-2 UNIT-1 with the new load gn080as.imag in the SAM21 EM.
4. Unlocks GWC-2 UNIT-1 in the SAM21 EM.
5. Waits for the inactive/upgraded GWC-2 UNIT-1 to become hot-standby.
6. Busies the upgraded GWC-2 UNIT-1 in the GWC EM.
7. Carries out a device audit against GWC-2 UNIT-1 in NPM.
8. Applies all available patches to GWC-2 UNIT-1 in NPM.
9. Returns To Service the patched GWC-2 UNIT-1 in the GWC EM.
10. Waits for GWC-2 UNIT-1 to become hot-standby.
11. Saves the soaked GWC image into CS 2000 Core Manager or CBM in the GWC EM.

    Note: The gn080as.imag is now a soaked load which contains all applicable patches for the GN080AS load.

12. Warm swacts the GWC-2 nodes: GWC-2 UNIT-1 provides service, and GWC-2 UNIT-0 is hot-standby.
13. Locks the inactive second unit GWC-2 UNIT-0 in the SAM21 EM.
14. Provisions GWC-2 UNIT-0 with the new soaked load gn080as.imag in the SAM21 EM.
15. Unlocks GWC-2 UNIT-0 in the SAM21 EM.
16. Waits for the inactive/upgraded GWC-2 UNIT-0 to become hot-standby.

Example system response - 'non-seed' nodes:

```
Group-2 started
GWC-4: Upgrade task is started.
GWC-4 [1/11]  Busy the hot-standby first unit. (GWC-4-UNIT-0)
GWC-4 [2/11]  Lock the inactive first unit. (GWC-4-UNIT-0)
GWC-4 [3/11]  Change the load of locked first unit. (GWC-4-UNIT-0)
GWC-4 [4/11]  Unlock the first unit. (GWC-4-UNIT-0)
GWC-4 [5/11]  Waiting for the first unit to be hot-standby. (GWC-4-UNIT-0)
GWC-4 [6/11]  First unit is hot-standby. Perform the warm-swact. (GWC-4-UNIT-1)
GWC-4 [7/11]  Warm-swact is finished, busy the second unit. (GWC-4-UNIT-1)
GWC-4 [8/11]  Locking the second unit. (GWC-4-UNIT-1)
GWC-4 [9/11]  Second unit is locked. (GWC-4-UNIT-1)
GWC-4 [10/11]  Change load of the locked second unit. (GWC-4-UNIT-1)
GWC-4 [11/11]  Second unit is booted up with the soaked load. (GWC-4-UNIT-1)
GWC-4 Upgrade finished successfully.
Group-2 finished
 Elapsed Time: 26 minutes 2 seconds
```

Upgrade steps for the 'non-seed' GWC nodes

This section assumes that GWC-4 is a 'non-seed' node, GWC-4 UNIT-1 is in service, GWC-4 UNIT-0 is hot-standby, the new load file name is gn080as.imag, and it is a soaked load which contains all applicable patches for the GN080AS load.

The GWC Upgrade Tool automatically performs the following actions:

1. Busies the inactive unit GWC-4 UNIT-0 in the GWC EM.
2. Locks the inactive unit GWC-4 UNIT-0 in the SAM21 EM.
3. Provisions GWC-4 UNIT-0 with the new soaked load gn080as.imag in the SAM21 EM.
4. Unlocks GWC-4 UNIT-0 in the SAM21 EM.
5. Waits for the inactive/upgraded GWC-4 UNIT-0 to become hot-standby.
6. Warm swacts the GWC-4 nodes: GWC-4 UNIT-0 provides service, and GWC-4 UNIT-1 is hot-standby.
7. Busies the hot-standby GWC-4 UNIT-1 in the GWC EM.
8. Locks the inactive second unit GWC-4 UNIT-1 in the SAM21 EM.
9. Provisions GWC-4 UNIT-1 with the new soaked load gn080as.imag in the SAM21 EM.
10. Unlocks GWC-4 UNIT-1 in the SAM21 EM.
11. Waits for the inactive/upgraded GWC-4 UNIT-1 to become hot-standby.

Pause conditions

During upgrade, the system may pause, because manual actions are needed, or an operation has failed. The table below shows the various pause conditions and the user action required:

If	Do
the current upgrade state is a pause point that you configured (see step 19) (see Pause points on page 1394)	carry out the required manual check, then enter **Continue** to continue the upgrade
NPM requires manual actions to be taken during the patching step (see Patch problem on page 1395)	launch the NPM GUI or CLUI to perform the required actions, then return to the GWC Upgrade Tool and enter **Continue** to continue the upgrade
the GWC alarms (in the in-service unit) exceed the configured alarm level (see steps 22 and 23) (see Alarm level exceeded on page 1396)	refer to section Alarm checking on page 1365
an operation failed when the tool invoked the GWC EM, SAM21 EM or NPM functions (e.g. the GWC EM cannot save the GWC load image to CS 2000 Core Manager or CBM)	check and rectify the failed operation manually, then enter **Retry** to continue the upgrade
an operation timeout occurs (e.g. the upgraded inactive unit is not hot-standby; see Operation timeout on page 1397)	carry out the timed-out operation manually, then enter **Retry** to continue the upgrade

Query upgrade status

While the upgrade in progress, you can launch another telnet or SSH session to the server, and use the following command to query the overall status of the upgrade:

/opt/nortel/NTsesm/gwcuptool/bin/gwcuptool.sh -query

34 When the upgrade finishes, the system reports the final service status of the upgraded GWC nodes and returns to the Upgrade Menu.

System response:

```
--{ Group-1 }-------------------------------------------------------------------
               GWC Node: GWC-2
                Profile: SMALL_LINENA
                 Status: Upgrade finished successfully.
.
.
.
--{ Group-2 }-------------------------------------------------------------------
               GWC Node: GWC-4
                Profile: SMALL_LINENA
                 Status: Upgrade finished successfully.
.
.
.
States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

35 Perform post-check

In the Upgrade Menu, select the Post-check option. Enter:

> 5

Example system response:

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

[5 Post-check step]

--{ Group-1 }-------------------------------------------------------------------
              GWC Node: GWC-2
               Profile: SMALL_LINENA
                Status:  Upgrade is finished successfully.
            Start time: Mon Dec 13 05:36:12 EST 2004
             Stop time: Mon Dec 13 05:52:36 EST 2004
          Elapsed time: 16 minutes 23 seconds
    GWC-2-UNIT-1: 47.142.128.51
     States from GWCEM:
     Current load name: GN080BF
  Administrative state: unlocked(1)
     Operational state: enabled(1)
        Stand by state: providingService(3)
           Fault state: none(0)
           Alarm state: 00 00 00 00
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0
    GWC-2-UNIT-0: 47.142.128.50
     States from GWCEM:
     Current load name: GN080BF
  Administrative state: unlocked(1)
     Operational state: enabled(1)
        Stand by state: hotStandby(1)
           Fault state: none(0)
           Alarm state: 00 00 00 00
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0

--{ Group-2 }-------------------------------------------------------------------
              GWC Node: GWC-4...
```

The screen display repeats the service status of the upgraded GWC nodes. The post-check checks the status of all the upgraded nodes, to ensure that:

- there is no alarm for the in-service GWC unit
- one unit is in service, and the other unit is hot-standby

36 **Exit GWC Upgrade Tool**

When the post-check finishes, press the Enter key to return to the Upgrade Menu.

System response:

```
Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

37 Exit the Upgrade Menu and return to the Main Menu. Enter:

> x

System response:

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

Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

38 Use the following table to determine your next step.

If	Do
you want to upgrade further GWC nodes	go back to step 7
all the required GWCs have been upgraded	continue at step 39

39

CAUTION

Do not exit the GWC Upgrade Tool before the upgrade finishes successfully. Do not press 'Ctrl+C' or close the TERM. If you do so and then start the GWC Upgrade Tool again, the system displays the message:

```
Warning!!! One Upgrade Manager is
running already. It is not recommended
to start a new server. Start a new one
to override it? (default N) Y/N):
```

Stop the GWC Upgrade Tool and exit the CLUI. Enter:

> x

Example system response:

```
Enter selection (1-4,x): x
GWC Upgrade Manager server stopped.
comp5iems-unit0(active):/export/home/ptm>
```

40 This procedure is complete.

Example screens

GWC load not available

If the GWC load is not available, the Prepare step fails. You must verify that the GWC load file is installed correctly, then return to the Configuration step to re-input the file name.

```
Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 2

GWC upgrade configuration
[Step 1 - LOAD FILE NAME]
Enter new load file name(Example: gn070bv.imag): gn080be.imag
.
.
.
Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x): 1
 GWC load file doesn't exist.
Available GWC loads in the given directory in SDM/CBM:
  - GwcConfig.sh
  - gn080bf.imag
  - gn080bf_jg.imag
  - gn080bg1.imag
```

Pre-check failure

There are several conditions which may cause the Pre-check step to fail, for example, servers not running, GWC cards with incorrect status. You must correct the problem, then repeat the Pre-check step.

```
Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x): 2

--{ Group-1 }------------------------------------------------------------
  GWC-10        LARGE_LINENA ... failed
              GWC Node: GWC-10
               Profile: LARGE_LINENA
                Status:  Auto discovery in progress.
        Estimated time: 41 minutes 15 seconds
                Paused: Invalid GWC status, unable to perform the upgrade.
    GWC-10-UNIT-0: 47.142.128.158
     States from GWCEM:
     Current load name: GN080BF
  Administrative state: locked(2)
     Operational state: disabled(2)
        Stand by state: coldStandby(2)
           Fault state: none(0)
           Alarm state: minor(3) , alarmOutstanding(4)
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0
    GWC-10-UNIT-1: 47.142.128.159
     States from GWCEM:
     Current load name: GN080BF
  Administrative state: unlocked(1)
     Operational state: enabled(1)
        Stand by state: providingService(3)
           Fault state: none(0)
           Alarm state: major(2) , alarmOutstanding(4)
            - Critical: 0
               - Major: 1
    1, Communication with a gateway is down. (MG10/00/5)
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0
```

Pause points

Pause points occur during the upgrade process wherever you specified them in the Configuration step. You must carry out the required manual checks, then enter **Continue** to allow the upgrade process to continue.

```
[Step 8 - PAUSE POINTS]
Values:
0 - no pause points

(1) For the first GWC node within the same GWC group.
1 - before locking the first upgrade unit of "seed" node
2 - after patch applied to "seed" unit
3 - before warm-swact
4 - after warm-swact
5 - after "seed" node upgraded

(2) For bulk upgrade GWC nodes with same GWC service type.
6 - before warm-swact

Separate numbers with comma, for example: 1,3,4
Enter the pause points (Default: 0):1,2,3,4,5

[Step 9 - LOGGING LEVEL]
.
.
.
Group-1 started
Upgrade task started
GWC-10 [1/16]  Busy the hot-standby first unit. (GWC-10-UNIT-1)
GWC-10 [2/16]  Lock the inactive first unit. (GWC-10-UNIT-1)

Message received from the server:

GWC-10 CHECK-POINT: before lock the first upgrade unit.
Please select from following:
Continue

Answer: continue
GWC-10 [3/16]  Change the load of locked first unit. (GWC-10-UNIT-1)
GWC-10 [4/16]  Unlock the first unit. (GWC-10-UNIT-1)
GWC-10 [5/16]  Waiting for the first unit to be hot-standby. (GWC-10-UNIT-1)
GWC-10 [6/16]  Upgraded first unit is hot-standby. (GWC-10-UNIT-1)
GWC-10 [7/16]  Apply patch to the upgraded first unit. (GWC-10-UNIT-1)
Apply request was attempted by the NPM server.
GWC-10 [8/16]  Patches are applied with the upgraded first unit. (GWC-10-UNIT-1)

Message received from the server:

GWC-10 CHECK-POINT: patches are applied for the "seed" unit.
Please select from following:
Continue
Answer: Continue
GWC-10 [9/16]  Waiting for the patched unit to be hot-standby (GWC-10-UNIT-1)
. . .
```

Patch problem

To ignore the error and allow the upgrade process to continue, you can simply enter **Continue**. If some manual action is needed (for example, launching the NPM CLUI/GUI), carry out the required action, then enter **Continue**. To invoke the NPM to attempt to apply the patch again, enter **Retry**. To abort the upgrade for the current GWC node, enter **Abort**.

```
Group-1 started
GWC-2: Upgrade task is started.
GWC-2 [1/16]  Busy the hot-standby first unit. (GWC-2-UNIT-1)
GWC-2 [2/16]  Lock the inactive first unit. (GWC-2-UNIT-1)
GWC-2 [3/16]  Change the load of locked first unit. (GWC-2-UNIT-1)
GWC-2 [4/16]  Unlock the first unit. (GWC-2-UNIT-1)
GWC-2 [5/16]  Waiting for the first unit to be hot-standby. (GWC-2-UNIT-1)
GWC-2 [6/16]  Upgraded first unit is hot-standby. (GWC-2-UNIT-1)
GWC-2 [7/16]  Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Patch NBF01G08 requires special attention:
  Ftp Error command
Patch NBF02G08 requires special attention:
  ERROR: Patch NBF01G08 needs to be applied in GWC-2-UNIT-1 before NBF02G08 can be
applied.
Patch NBF03G08 requires special attention:
  ERROR: Patch NBF01G08 needs to be applied in GWC-2-UNIT-1 before NBF03G08 can be
applied.
.
.
.
Message received from the server:

GWC-2 Warning: NPM can't apply all patches to GWC unit. GWC-2-UNIT-1
Please select from following:
Continue Retry Abort

Answer: retry
GWC-2 [7/16]  Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Apply request was attempted by the NPM server.
GWC-2 [8/16]  Patches are applied with the upgraded first unit. (GWC-2-UNIT-1)
GWC-2 [9/16]  Waiting for the patched unit to be hot-standby (GWC-2-UNIT-1)
GWC-2 [10/16]  Patched unit is hot-standby, load imaging is started.
(GWC-2-UNIT-1)
.
.
.
```

Alarm level exceeded

If the actual GWC alarms reach the alarm level defined in the Configuration step, the upgrade pauses. To ignore the alarms and allow the upgrade process to continue, you can simply enter **Continue**. Otherwise you must enter **Abort** to stop the upgrade, and correct the problem before continuing.

```
Group-1 started
Upgrade task started
GWC-10 [1/16]  Busy the hot-standby first unit. (GWC-10-UNIT-1)
    GWC-10-UNIT-0: 47.142.128.158
     States from GWCEM:
     Current load name: GN080BE
  Administrative state: unlocked(1)
     Operational state: enabled(1)
        Stand by state: providingService(3)
           Fault state: none(0)
           Alarm state: major(2) , alarmOutstanding(4)
            - Critical: 0
               - Major: 1
    1, Communication with a gateway is down. (MG10/00/5)
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0

Message received from the server:

GWC-10 In service unit has more alarms in GWCEM than configured. GWC-10-UNIT-0
Please select from following:
Continue Abort

Answer: Continue
GWC-10 Ignore the alarm states, and continue the upgrade task
```

Operation timeout

If an operation timeout occurs, the upgrade does not necessarily fail. You can use the CMT client and SAM21EM client to check the status of the GWC card. After performing the timed-out operation manually (for example, locking the GWC card), you can enter **Retry** to allow the upgrade process to continue.

```
Group-1 started
GWC-10: Upgrade task is started.
GWC-10 [1/16]  Busy the hot-standby first unit. (GWC-10-UNIT-0)
GWC-10 [2/16]  Lock the inactive first unit. (GWC-10-UNIT-0)

Message received from the server:

GWC-10 Timeout: SAM21EM can't lock the inactive GWC unit. GWC-10-UNIT-0
Please select from following:
Retry Abort

Answer: retry
GWC-10 [3/16]  Change the load of locked first unit. (GWC-10-UNIT-0)
.
.
.
```

Downgrade procedure

In SN08, the GWC Upgrade Tool (Phase 1) does not support an automated rollback procedure. However, as long as the upgraded GWC has not been provisioned with new data (for example, gateways, carriers, lines), the tool can be used to switch between the old and new loads, as described below.

At the CS 2000 Management Tool interface

1 Perform steps 1 to 10 of Upgrade procedure on page 1366.

Note: At step 10 you must enter **N** to reject the default values, otherwise you cannot continue with step 12 and the rest of the downgrade procedure.

System response:

```
.
.
.
Do you want to use these configuration values? [Y|N] (Default: N): n

Do not use default values
[Step 4 - LOAD DIRECTORY]
Default load directory formats are different for SDM and CBM.
If SDM is used, it should be "/swd/gwc".
If CBM is used, it should be "/gwc".
Enter the load directory. (Default: "/swd/gwc"): /swd/gwc

[Step 5 - NEW LOAD NAME]
Enter the new load name (Default: ""):
```

2 Enter the name of the old GWC load image file, that is, the original load that existed before the automatic upgrade started. The load name is used to query the patch list from NPM. If the load name does not contain the GWC load name, you must specify a valid GWC load name here, otherwise the GWC Upgrade Tool cannot retrieve the available patch list.

System response:

```
[Step 5 - NEW LOAD NAME]
Enter the new load name (Default: ""): G1070CH

[Step 6 - OLD LOAD NAME]
Enter the old load name: (Default: "")
```

3 Enter the name of the new GWC load image file, that is, the load that was used in error during the automatic upgrade.

System response:

```
[Step 6 - OLD LOAD NAME]
Enter the old load name (Default: ""): G1080BH

[Step 7 - UPGRADE MODE]
Values:
1 - single
2 - bulk
3 - mix
h - help

Enter the upgrade mode (1-3,h) (Default: 2):
```

4 Perform steps 17 to 40 of the Upgrade procedure starting on page 1373. The GWC Upgrade Tool reboots the GWC cards using the old load.

Re-provision the Ethernet Routing Switch 8600 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 Ethernet Routing Switch 8600.

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 Ethernet Routing Switch 8600 documentation and choose Getting Started.

At the CLI for the Ethernet Routing Switch 8600

1 Determine the slot and port on the router that connects to the device. Type:

> show ip arp info <ip_address>

and press the Enter key

where **<ip_address>**
is the physical IP address of the GWC card.

Example system 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 the slot and port number; you will need this information in the next step of this procedure.

Note: If the response indicates MLT instead of the slot and port, perform this operation from the mate unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.

2 Use the numbers recorded in step 1 on page 1400 to set the slot and port to auto-negotiate. Type:

> config ethernet <slot>/<port> auto-negotiate enable

and press the Enter key.

System response:

```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

The system configures the slot and port to auto-negotiate, and the prompt returns.

3 Verify the port configuration. Type:

> show ports info config <slot>/<port>

and press the Enter key.

System response:

```
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
```

The system displays the slot and port configuration.

4 Commit the change. Type:

> save config

and press the Enter key.

5 Go to step 6 on page 1368 to continue with the procedure "Upgrading the GWC using the GWC Upgrade Tool".

Create a backup of the GWC load file

Purpose of this procedure

This procedure is used to log onto the CS 2000 Core Manager or Core and Billing Manager (CBM) and manually make a copy of one or more existing GWC load images stored on the CS 2000 Core Manager or CBM.

When to use this procedure

Use this procedure prior to saving an image of a GWC load if you wish to save a backup of the original GWC load stored on the CS 2000 Core Manager or CBM.

Note: If a backup is not created, then the process of taking a GWC load image overwrites the existing image stored on the CS 2000 Core Manager or CBM.

Prerequisites

There are no prerequisites to this procedure.

Action

At the CS 2000 Core Manager or CBM console

1 Log in to the CS 2000 Core Manager or CBM as the root user.

```
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

2 Change directory to the GWC software directory by typing

 # cd /swd/gwc

and pressing the Enter key.

3 Type **ls** and press the Enter key to list the contents of the directory.

4 Locate the load file name that corresponds to the load you wish to back up.

Note: There are likely to be multiple load file names. Ensure that you select the correct load filename. If you are saving the load file of a specific GWC card or node, refer to procedure "View the operational status of a GWC" in *Gateway Controller Configuration Management*, NN10205-511, to locate the load filename associated with a specific GWC card.

5

CAUTION

Be sure to use the command **cp** in this step.

Failure to use the **cp** command can cause problems with the general upgrade process.

Make a copy of the existing GWC software load file by typing

 # cp <load_filename>.imag <load_filename>.imag.bak

and pressing the Enter key.

where

<load_filename>
is the GWC load filename that you want to copy

Note: You can use any name for the backup file name. You can also include the date in this filename, for example: <load_filename>.imag.031201

6 Change the permissions for the image file by typing

 # chmod 755 <load_filename>.imag.bak

and pressing the Enter key.

where

<load_filename>
is the GWC load filename

7 This procedure is complete.

Note: To return to the procedure that sent you here, refer to "Overall GWC upgrade procedure" (automated or manual) in *Upgrading the Gateway Controller*, NN10196-461.

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 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

Note: In the above command, insert a space after the "gwclfinfo" character string. Do not insert any other spaces.

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 procedure that sent you here, refer to "Overall GWC upgrade procedure" (automated or manual) in *Upgrading the Gateway Controller*, NN10196-461.

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 procedure that sent you here, refer to “Overall GWC upgrade procedure“ (manual or automated) in *Upgrading the Gateway Controller*, NN10196-461.

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**.

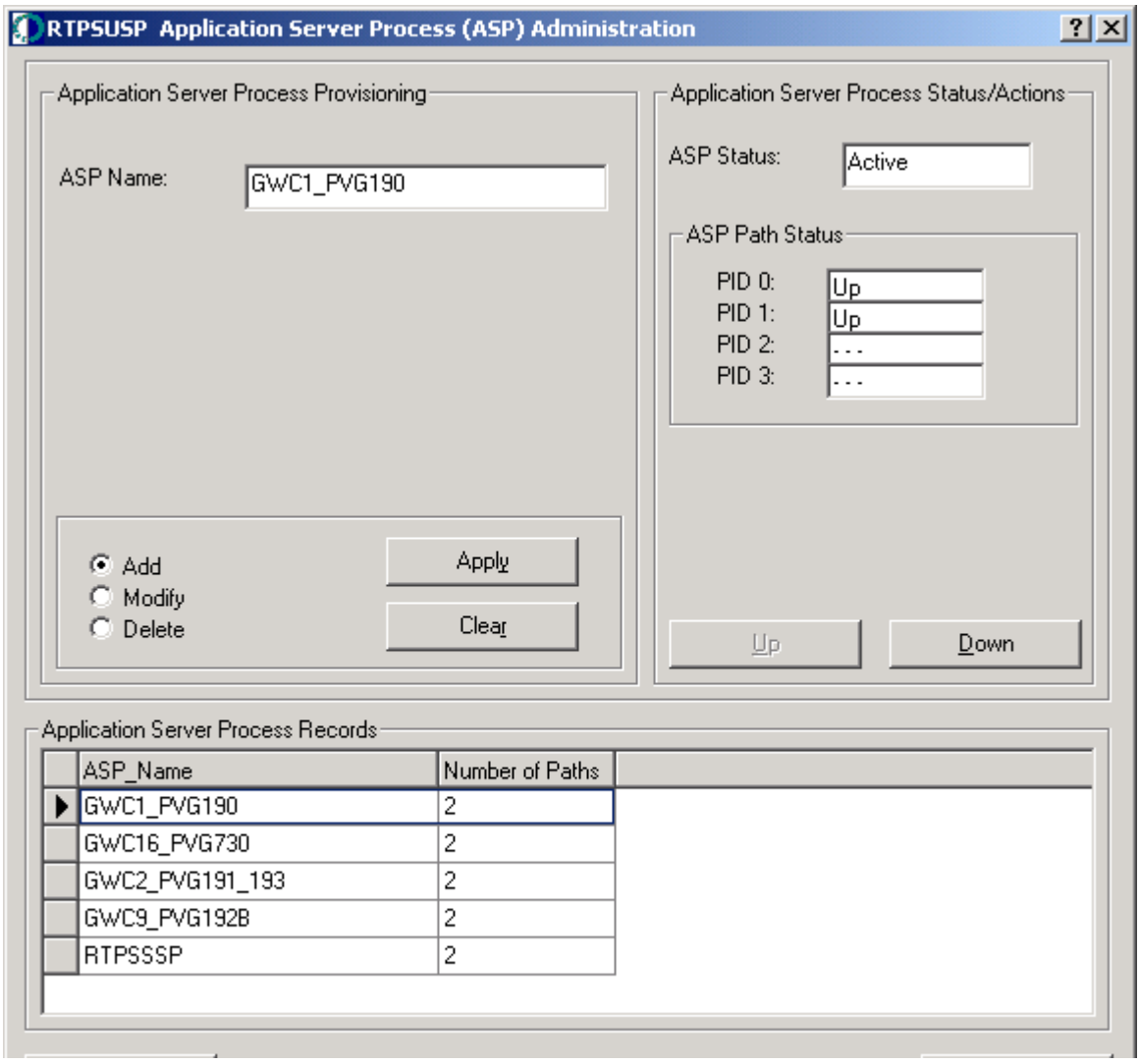
3 In the **IPS7** window, click **ASP**.

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).

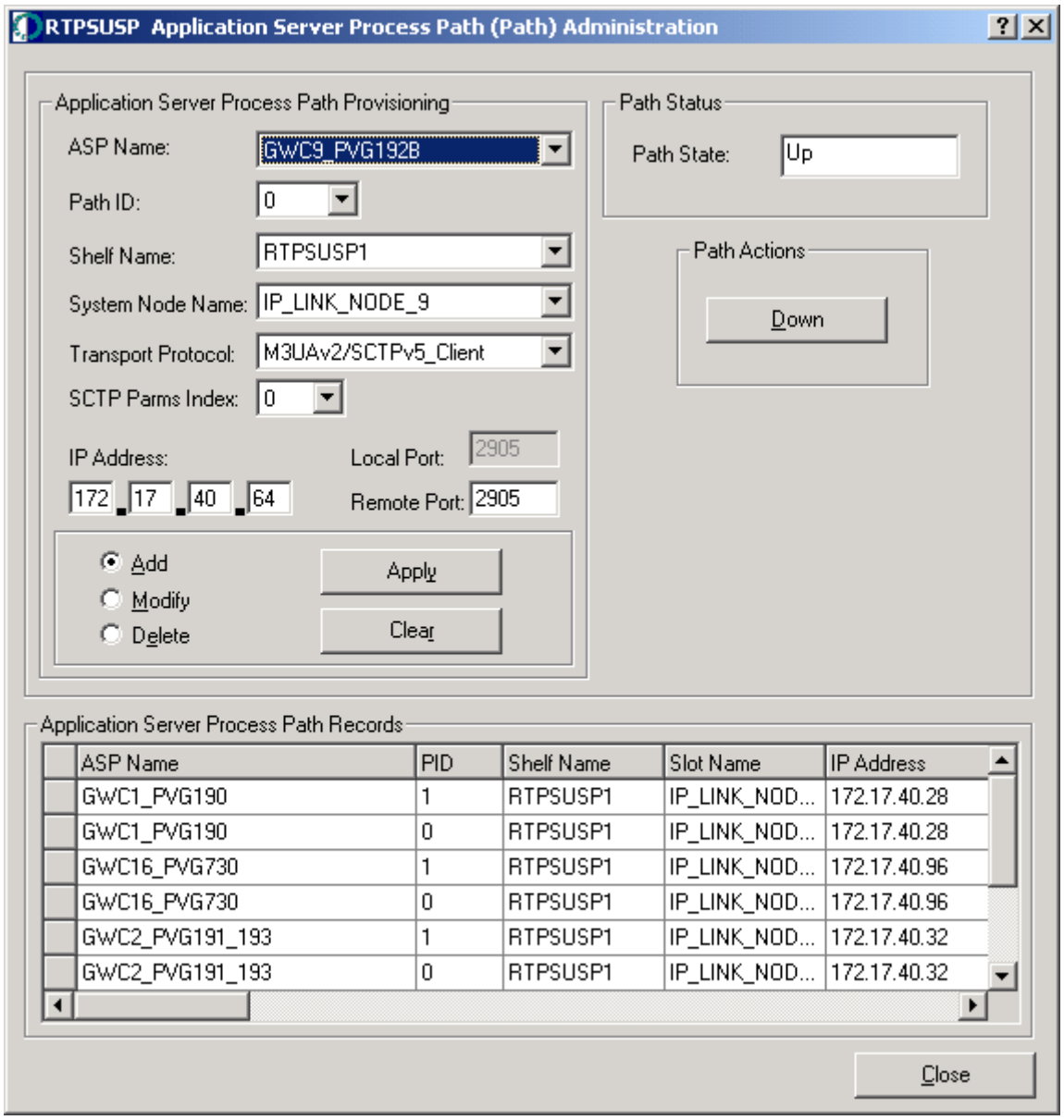
d Click **Apply** to add the IP Path.

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.

Media Server 2000 Series

IP applications use Media Server 2010 and ATM applications use Media Server 2020. The ATM Media Server 2020 was introduced in the SN07 software release.

WARNING

The SN08 software release introduces an IEMS Graphical User Interface (GUI) Media Server 2000 series configuration interface that replaces the Command Line User Interface (CLUI) used in SN07. An IEMS must be commissioned in the office and at an SN08 release before upgrading a Media Server 2000 node.

Before upgrading the Media Server 2000 Series

Perform the required prerequisite upgrade as follows:

Network	Media Server 2000 applies to:	Previous Upgrade
ATM	UA-AAL1 and PT-AAL2	Gateway Controller on page 1330
IP	PT-IP, UA-IP, IAC, IAW[1], and CHS[2]	Gateway Controller on page 1330
Tri-Modal	all applications	Gateway Controller on page 1330

1.Includes IP International: PT-IP, IAC, and UA-IP
2.Applies to CHS North America only

After upgrading the Media Server 2000 Series

Perform the next required upgrade as follows:

Network	Media Server 2000 applies to:	Next Upgrade
ATM	UA-AAL1	Media Gateway (MG) 9000 on page 1440
	PT-AAL2	Universal Signaling Point on page 1490
IP	UA-IP[1]	Media Gateway (MG) 9000 on page 1440

Network	Media Server 2000 applies to:	Next Upgrade
	PT-IP, IAW, and IAC [2]	Universal Signaling Point on page 1490
	CHS[3]	Enhanced Network and Message Switch on page 1636
Tri-Modal	all applications	one of above based on configuration

1.Includes IP International: UA-IP
2.Includes IP International:PT-IP and IAC
3.Applies to CHS North America only

About the Media Server 2000 Series

The Nortel Media Server 2000 Series (MS 2000 Series) servers offer audio service applications providing an interface for caller interactive features that require user input collection and prompt playback.The MS 2000 Series consist of:

- MS 2010 for IP networks
- MS 2020 for ATM networks

Upgrading the Media Server 2000 Series

This document contains the procedures for upgrading the Media Server 2000 Series software (Media Server 2010 and Media Server 2020).

Note: For downgrading the Media Server 2000 refer to the *Downgrading a Media Server 2000 node* procedure in document *NN10335-461*.

Integrated EMS GUI

The SN08 software release introduces an Integrated Element Management System (IEMS) Graphical User Interface (GUI) Media Server 2000 series configuration interface that replaces the Command Line User Interface (CLUI) used in SN07. An IEMS must be commissioned in the office and at an SN08 release before upgrading a Media Server 2000 node.

The Integrated EMS GUI is the human interface to the Succession Operations and Maintenance Center Platform. To access the Integrated EMS GUI, refer to the *Integrated EMS Basics document* (NN10329-111).

Media Server 2000 Series upgrade

The Media Server 2000 Series upgrade procedure enables you to apply a maintenance release or “patch” to a Media Server 2000 Series node, or upgrade the node as part of a network-wide upgrade to a new release.

Beginning in SN08, the Media Server 2000 series is configured through the CS 2000 Management Tools GUI. In SN07, the Media Server 2000 series was configured through a command line User Interface (CLUI). This procedure covers the steps necessary to migrate from SN07 to SN08.

CAUTION

Backing up the current load files and completing the pre-migration section of this document must be performed prior to upgrading the server. These steps use the CLUI interface that is not available once the server is upgraded.

The following table lists the procedures used in upgrading the Media Server 2010 or Media Server 2020.

Media Server 2000 Series upgrade procedures

Procedure and page
Backing up Media Server 2000 Series files on page 77
Updating the Media Server 2000 Series trusted manager table on page 80
Upgrading a Media Server 2000 Node on page 1417
Migration of Media Server 2000 nodes into an Integrated EMS on page 1418
Procedure to upgrade a Media Server 2000 on page 1433

Upgrading a Media Server 2000 Node

This procedure enables you to upgrade a Media Server 2000 node as part of a network-wide upgrade to a new release.

Office impact

Upgrading a Media Server 2000 node 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 2000 node 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 2000 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 2000 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!

CAUTION

If you must apply a patch and perform an upgrade, only apply the patch after the upgrade, or the patch will be overwritten in the upgrade process.

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

Prerequisites

If your software is being delivered through ESD, the image file must be uncompressed and available on your ESD repository server.

Migration of Media Server 2000 nodes into an Integrated EMS

In SN06.2 and SN07, configuration and maintenance of the Media Server 2000 nodes (IP Media Server 2010 and the ATM Media Server 2020) was handled through a command line tool running on the SESM application. With the SN08 software release, Media Server 2000 node configuration and maintenance is handled under the IEMS software using a GUI client. To access the IEMS GUI, refer to the IEMS Basics document (NN10329-111).

In SN06.2 the Media Server 2000 CLUI (Command Line User Interface) provided the user with the ability to set a single web server user name and password that would be used by all devices. In SN07, the Media Server 2000 CLUI (Command Line User Interface) provided the user with the ability to set the community string and web server passwords on the Media Server 2000 nodes. The tool stored these encrypted passwords to use when communicating with the node.

In SN08, the Media Server 2000 Configuration and Maintenance GUI will also need to use these passwords for communication with the nodes. Because of this, any password changes that were made to the Media Server 2000 nodes will need to be manually entered into the IEMS Media Server 2000 node properties.

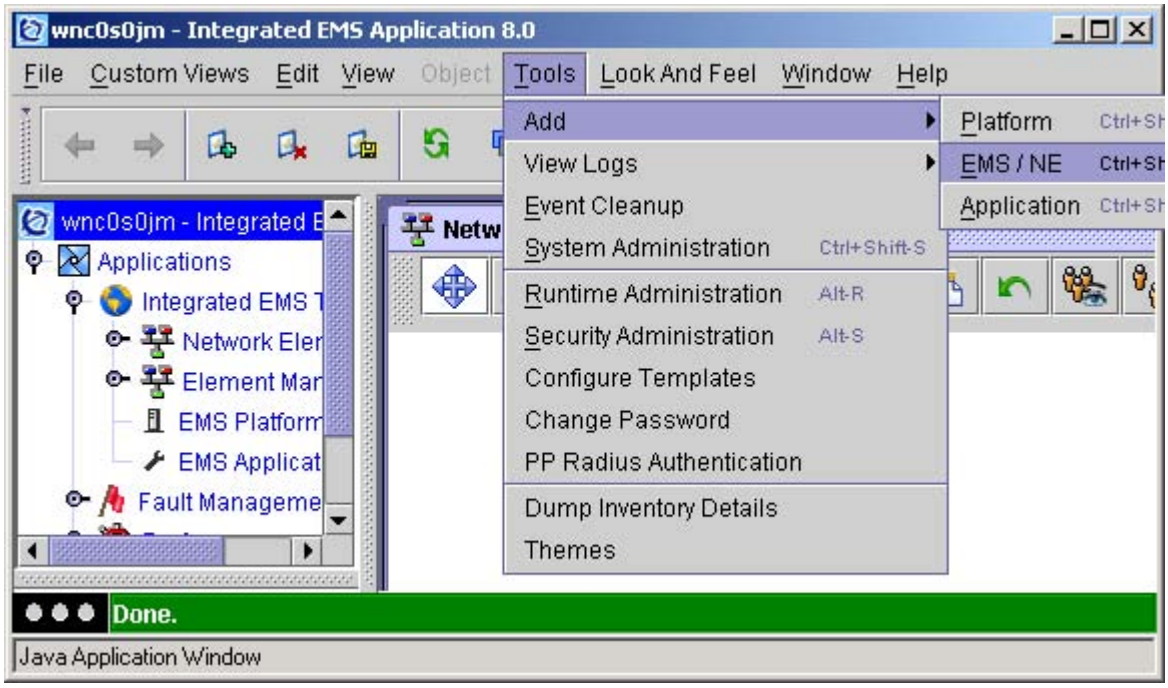
There are three scenarios for migrating or upgrading an SN06.2 or SN07 Media Server 2000 node into an SN08 IEMS.

- Scenario 1 - SN06.2 or SN07 Media Server 2000 node existed in the network but was not previously managed by IEMS (refer to Procedure for Scenario 1).
- Scenario 2 - SN07 Media Server 2000 node existed in IEMS and used default settings for web server and SNMP community strings (refer to Procedure for Scenario 2).
- Scenario 3 - SN07 Media Server 2000 node existed in IEMS with modified settings for web server and SNMP community strings (refer to Procedure for Scenario 3).

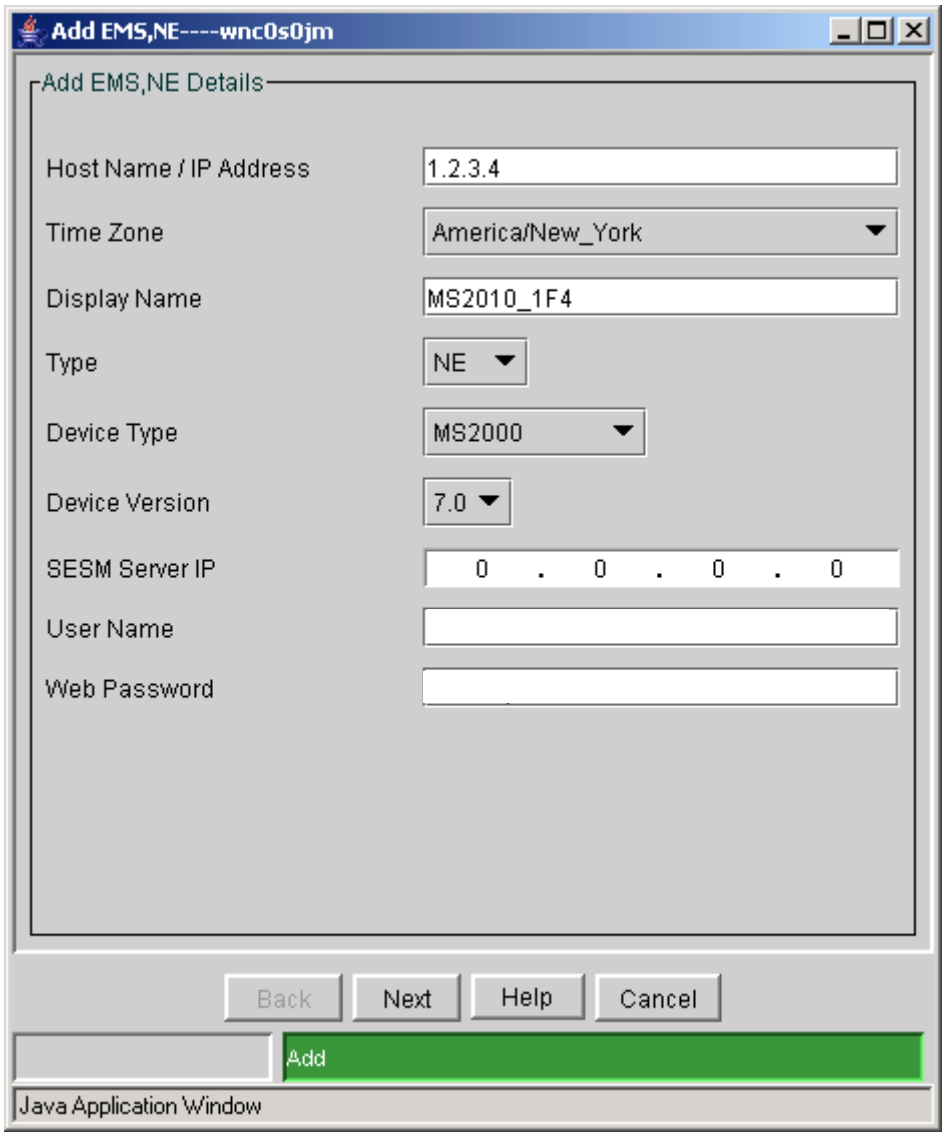
Procedure for Scenario 1

A Media Server 2000 node was present in SN06.2 or SN07 network but did not exist in IEMS.

1 Add the Media Server 2000 node to the IEMS by selecting the Add NE menu item under Tools menu.



The add EMS/NE wizard opens.



2 Select a type of “NE”, Device Type of “MS2000”, and Device Version.

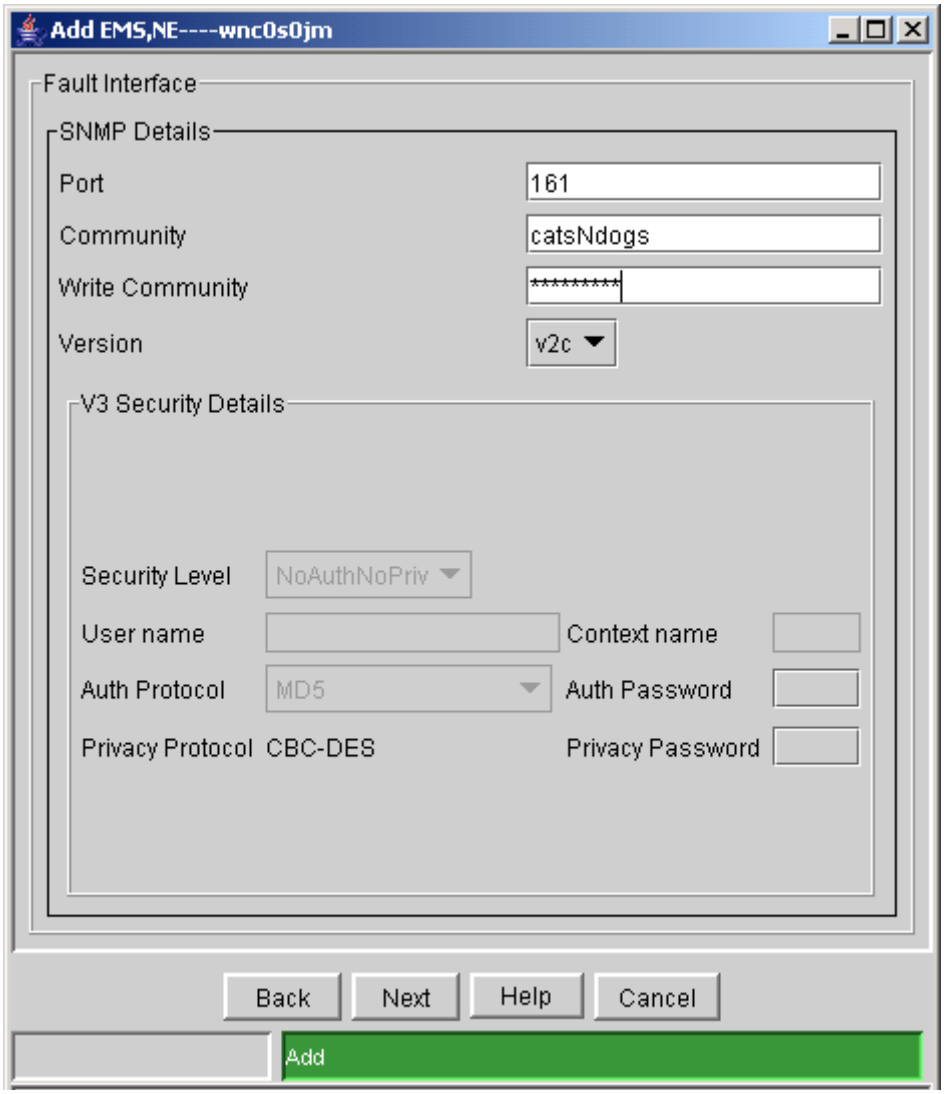
Note: If you are upgrading from SN06.2, the IEMS does not support management of an SN06.2 Media Server 2000 node. However, you can add the node into the IEMS as an "8.0" Device version in order to upgrade it. Because the IEMS cannot collect alarms or performance metrics from the SN06.2 node, the node will have some alarms registered against it until it is upgraded to the SN08 load.

The panel adds the fields to enter the web server “User Name” and “Web Password”.

3 If the web user name and password were modified in SN06.2 or SN07, enter the modified values in the NE properties for the Media Server 2000 node. If the web server user name and password are still the node default values, enter a user name of “Admin” and a password of ”Admin”.

Note: Failure to put the correct values here will cause the Maintenance and Configuration tool to fail when it attempts to perform file transfers to and from the node.

The next figure panel illustrates setting up the Fault Interface. The SNMP Read and Write Community Strings will be setup for the node.



4 If the node has previously had its community strings changed from the default values then the new values need to be entered here. If the default values for the node are still being used then enter a read community of “public” and write community of “private”.

Note 1: If the community strings were changed by the Media Server 2000 CLUI in SN07, then both the read and write community string will be the same value. These can be changed after this procedure is completed by using the Media Server 2000 Configuration and Maintenance tool from the Media Server 2000 device menu.

Note 2: Failure to put the correct read community string for the node here will prevent the Media Server 2000 Configuration and Maintenance tool from communicating with the node. When the tool is launched for this node a “Request Timeout” will occur while trying to retrieve the node information. If the write community string is not correct then the tool will fail whenever any configuration or maintenance activity attempts to change settings on the node. Again this will appear as a “Request Timeout” to the node.

5 Fill in the appropriate community strings for the node.

Procedure for Scenario 2

A Media Server 2000 node was present in an SN07 IEMS and used the default file transfer / web server password and SNMP community string.

There is *No* action required. When a Media Server 2000 node in an SN07 IEMS is upgraded it is assigned the default values used by the node for web server user name (“Admin”) and password (“Admin”) and the default SNMP read (“public”) and write (“private”) community strings.

Procedure for Scenario 3

A Media Server 2000 node was present in an SN07 IEMS and the file transfer / web server password or SNMP community string was changed.

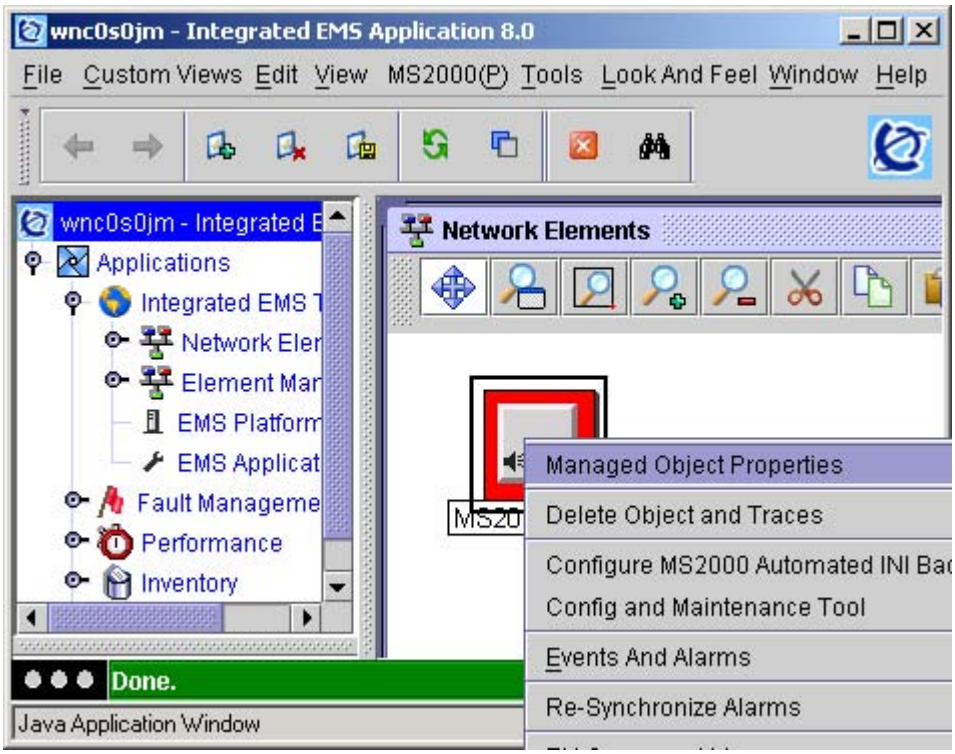
1 Once the IEMS is running on an SN08 load you can modify the properties of the existing Media Server 2000 node and change the settings of the web user name and password as well as the SNMP community strings if necessary.

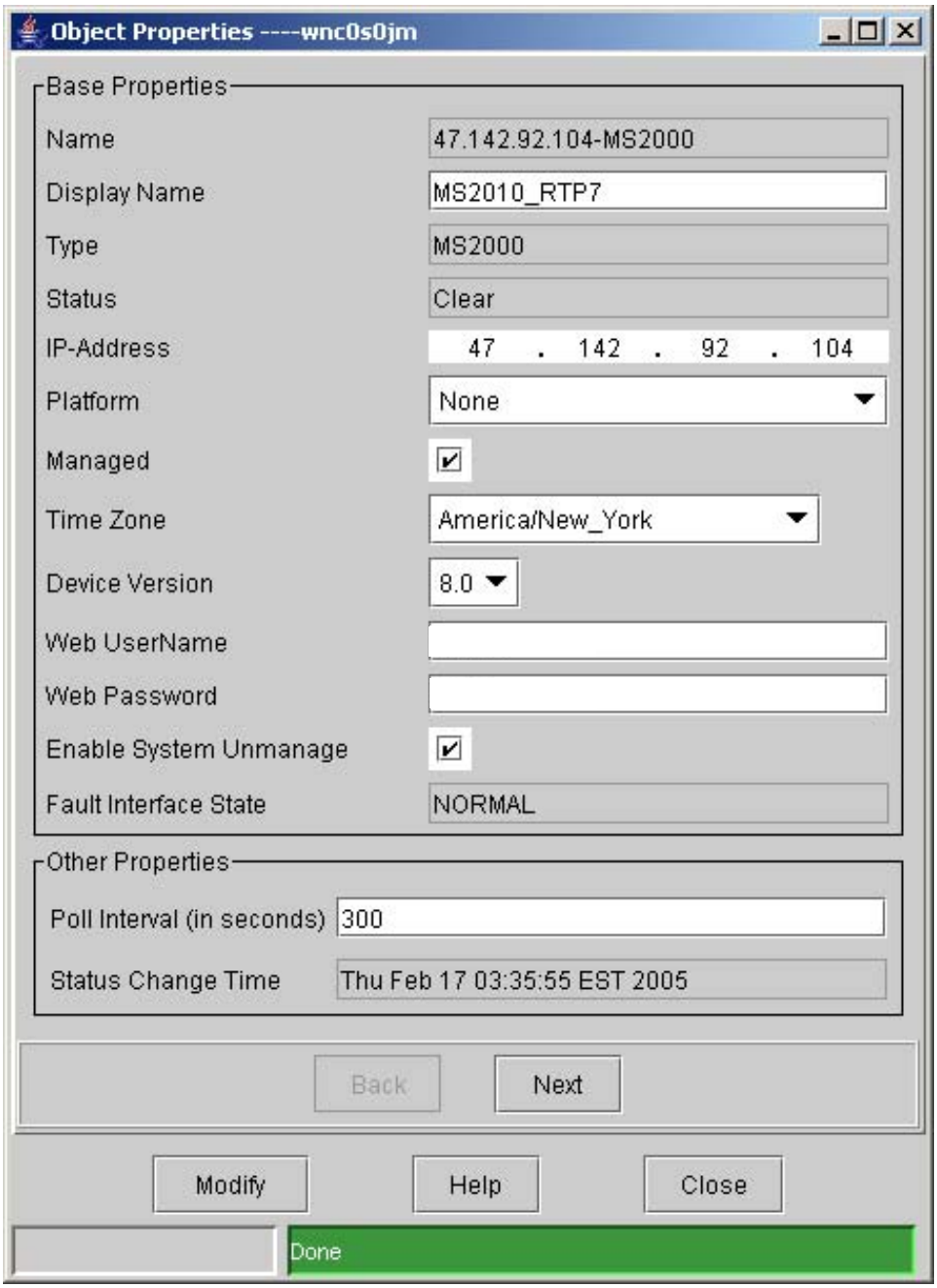
2 From the Media Server 2000 network element icon right-click on the node and select the “Managed Object Properties” menu item.

This brings up the “Object Properties” for this node. On the first panel there are entries for the webserver User and Password. After upgrading from SN07 these will be set to the default values for the node. Namely the web user and password will be set to “Admin”.

3 If the web server username or password was previously changed in an SN06.2 or SN07 release, they will need to be updated here to the correct values.

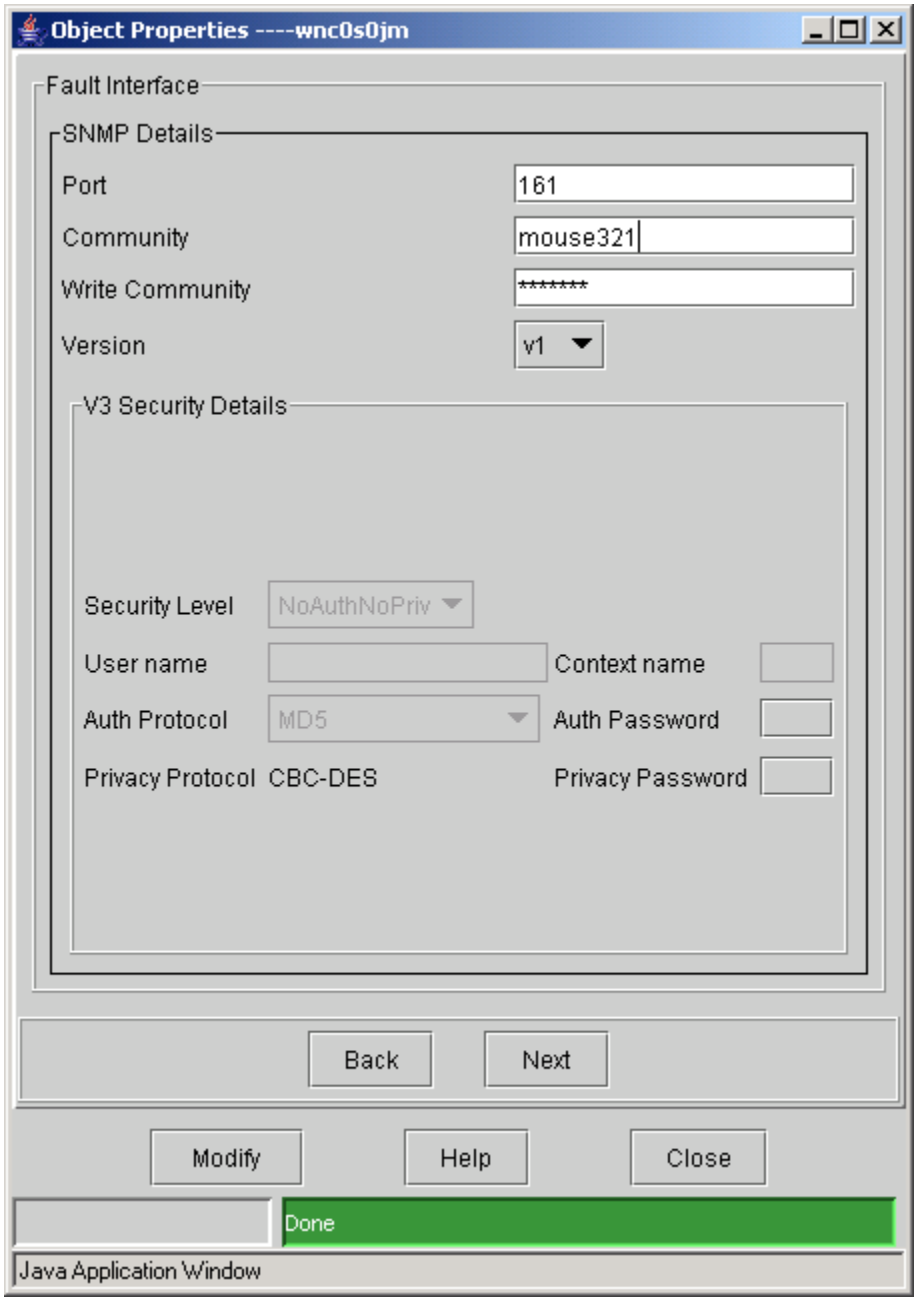
Note: Failure to put the correct values here will cause the Maintenance and Configuration tool to fail when it attempts to perform file transfers to and from the node.





The object properties for the fault interface displays. Here the SNMP Read and Write Community Strings will be setup for the node. After an upgrade the node will be set with the default values.

4 If the SN07 node has previously had its community strings changed from the default values of read community “public” and write community of “private”, enter the new values.



Note 1: If the community strings were changed by the Media Server 2000 CLUI in SN07, both the read and write community string will be the same value. These can be changed after this procedure is completed by using the Media Server 2000 Configuration and Maintenance tool from the Media Server 2000 device menu.

Note 2: Failure to have the correct read community string for the node will prevent the Media Server 2000 Configuration and Maintenance tool from communicating with the node. When the tool is launched for this node a “Request Timeout” will occur while trying to retrieve the node information. If the write community string is not correct then the tool will fail whenever any configuration or maintenance activity attempts to change settings on the node. This will appear as a “Request Timeout” to the node.

Copying the files to the audiocodes directory

At the Windows desktop interface

1 Determine the source for the software upgrade files.

If	Do
the software upgrade files are delivered through ESD	step 2
the software upgrade files are on CD	step 14

2 Log in to the server by typing

```
> telnet <server>
```

where

server
is the IP address or host name of the SSPFS-based server to which you want to transfer the software load

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

5 When prompted, enter the root password.

6 Make a temporary directory to store the ESD software by typing

```
# mkdir /data/iso_esd
```

and pressing the Enter key.

7 Change directory by typing

 # cd /data/iso_esd

and pressing the Enter key.

8 Display the available disk space in the directory by typing

df -k

and pressing the Enter key.

Example response

```
# df -k
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2         3082223  144125 2876454    5%    /data/iso_esd
```

9 Record the amount of available disk space, which is provided in kilobytes. You will need the information later in this procedure.

Note: Recommended minimum disk space is 2.3 GBytes.

10 Transfer the ESD software load from the drop box on the repository server to the server as follows:

a Access the repository server through FTP by typing

 # ftp <repository_server>

where

<repository_server>
is the machine owned by the operating company that was selected to be the destination for ESD software.

b Log in and change directory to the drop box location on the repository server.

c Change the transfer mode to binary by typing

ftp> bin

d List the contents of the drop box by typing

ftp> ls

e Transfer the ESD software load onto the SSPFS-based server by typing

ftp> get <iso_image>

where

<iso_image>
is the CS2M ISO image filename

for the software load.

f End the FTP session by typing

```
ftp> bye
```

g Uncompress the software load file.

```
# gunzip -d
CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar.gz
```

h Untar the software load file.

```
# tar -xvf
CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar
```

i Remove the .tar file by typing

```
# rm CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar
```

j Access the directory that contains the software load file by typing

```
# cd CS2M0080.80.P.NCL.NAP.VAULT.1.D
```

and list the file in the directory.

k Change the name of the file in the directory by typing

```
# mv CS2M0080_load.iso.tape
CS2M0080_load.iso
```

11 Mount the ISO image as follows:

a Access the command line interface by typing

```
# cli
```

Example response

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

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)
 X - exit
```

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

If the response is	Do
`ISO Image Already Mounted`	substep d
`Enter the full path of the ISO image`	substep e

d Enter the number next to the “umount_image” option in the menu and retry substep c.

Note: If the umount_image or mount-image command is unsuccessful a second time, contact your next level of support.

e When prompted, enter the full path name of the ISO image on the server from the root.

Example

`/MS2000X0.X0.V.NCL.NAP.VAULT.X.D/MS2000X0_load.iso`

Or

`/MS2A00X0.X0.V.NCL.NAP.VAULT.X.D/MS2A00X0_load.iso`

The contents of the ESD software file are placed in directory /tmpmnt.

The following message displays.

```
=== "mount_image" completed successfully
```

Note: Do not attempt to access the /tmpmnt directory until the mount command is complete.

If the response is	Do
`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`	step f
`Provided full path to ISO image does not exist`	Verify the location and name of the ISO 9660 image.
`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 your next level of support.
`ERROR MOUNTING <ESD_filename>`	This response indicates that either the ISO 9660 file is corrupt, or the `/tmpmnt` directory has been deleted. Repeat this procedure, and if it fails a second time, contact your next level of support.

f Exit each menu level of the command line interface to return to the root level prompt, by typing **x** and pressing Enter.

12 Enter the following commands.

```
cd /tmpmnt
ls
```

Verify the content of the /tmpmnt directory 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). There may also be some documentation or a README.file.

13 Proceed to step 17.

14 Insert the CD into the active CS 2000 Management Tool CD drive.

15 Enter the following command.

```
cd /cdrom/cdrom0
```

16 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.

17 Copy the files to the audiocodes directory by entering the following commands.

```
cp -r * /data/loads/audiocodes
```

```
cp * /data/loads/audiocodes
```

18 Enter the following commands.

```
cd /data/loads/audiocodes
```

```
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.

19 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 Login as root.

c Change to the audiocodes tools directory by entering the following command.

```
cd /data/loads/audiocodes/Tools
```

Note 1: Check the /data/loads/audiocodes/(IP address) directory for the .DAT and .INI files. If you do not find the files, check the /data/loads/ams/(IP address) directory.

Note 2: If the SESM and IEMS are on the different boxes, FTP the .ini file from the /data/loads/ams/(IP address)

directory on SESM to /data/loads/audiocodes/(IP address) directory on the IEMS.

d Perform an upgrade to the .ini file by entering the following command.

perl iniupgrade.pl /data/loads/audiocodes/AMS_DefaultConfig_<.ini file from audiocodes> /data/loads/audiocodes/<SN06.2 .ini or SN07 .ini file from step c **of the** Backing up Media Server 2000 Series files **procedure > <SN08 .ini filename>**

Note: SN06.2 and SN07 use different directories as shown in the examples below.

Example for SN06.2

perl iniupgrade.pl /data/loads/audiocodes/AMS_DefaultConfig_IP_v204.ini /data/loads/ams/10.69.33.1/2005-03-04_10:56:33.Board.ini SN08_new.ini

Example for SN07

perl iniupgrade.pl /data/loads/audiocodes/AMS_DefaultConfig_IP_v204.ini /data/loads/audiocodes/10.69.33.1/2005-03-04_10:56:33.Board.ini SN08_new.ini

20 Make a note of the .DAT and .INI file names for use later in this procedure.

21 Copy the INI file you created in step 19d above to the proper directory on the IEMS server. This allows the INI file to appear in the Media Server 2000 Configuration and Maintenance GUI during the node upgrade.

a Enter the following commands to change directories.

> cd /data/loads/audiocodes

> cd <ip address of the Media Server 2000 node>

b If the directory does not exist, create the directory for this node by entering the following command.

>mkdir <ip address of the MS2000 node>

c Copy the upgraded INI file to this directory as shown below.

```
>cp /data/loads/audiocodes/Tools/<ini file
created in step 19d>
/data/loads/audiocodes/<ip address of
node>/.
```

22 If you acquired the the software upgrade files from CD, eject the CDRom and store in a secure location. Eject the CDRom by entering the following commands.

```
# cd /

# eject cdrom
```

23 If you acquired the software upgrade files through ESD, remove the directory and files created in the Copying the files to the audiocodes directory procedure.

Example

```
cd /

rm -r /MS2000X0.X0.V.NCL.NAP.VAULT.X.D
```

Or

```
rm -r /MS2A00X0.X0.V.NCL.NAP.VAULT.X.D
```

Procedure to upgrade a Media Server 2000

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, are equipped with login timeouts. If at any point the procedure 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.

At the Windows desktop interface

1 Enter the following commands.

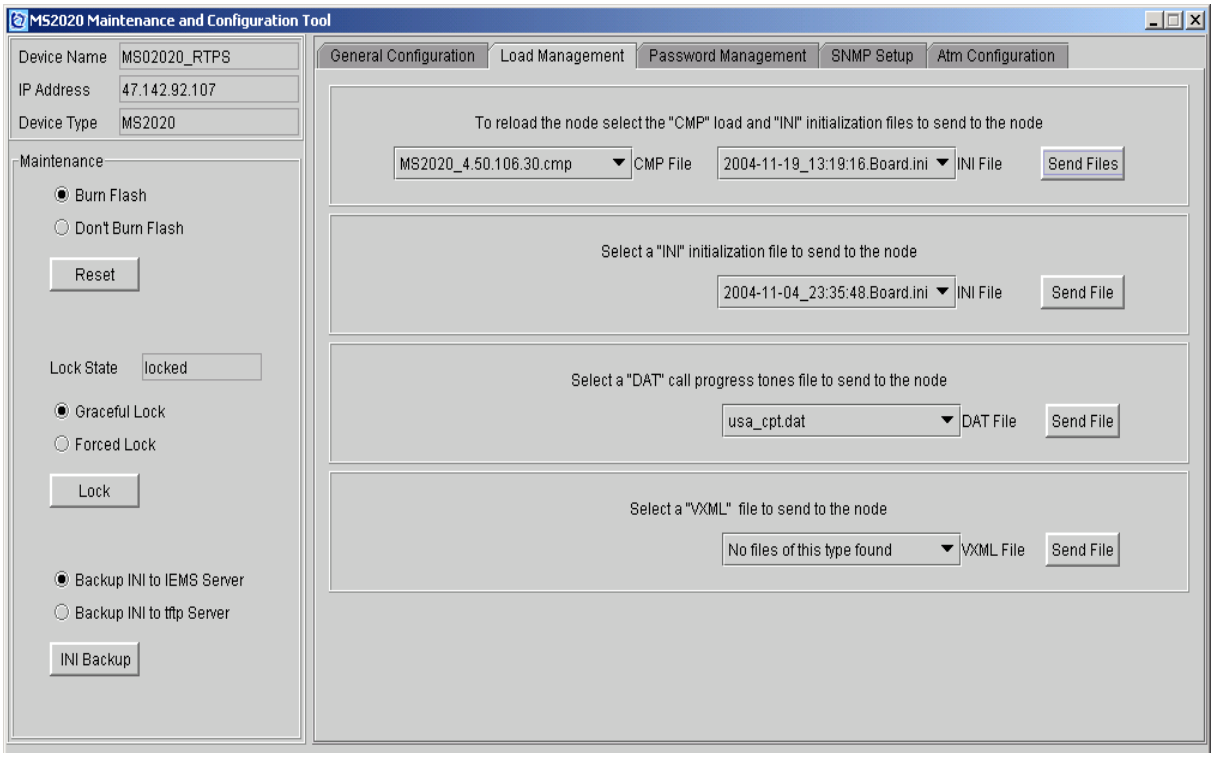
```
cd /data/loads/audiocodes

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.

2 From the IEMS client, launch the MS2000 Configuration and Maintenance GUI. Consult your system administrator for instructions about how to do access the GUI.

3 Select the Media Server 2000 node to upgrade and then select the Load Management tab as shown in the following figure.



4 On the left side of the window, choose the Graceful Lock or the Forced Lock radio button to lock the node. (You will actually initiate the lock in the next step.)

CAUTION

Performing a *Graceful Lock* on the node will take it out of service after any active calls have completed.

CAUTION

Performing a *Forced Lock* on the node will take it out of service immediately. Active calls will be dropped.

5 Select *Lock* to lock the node.

6 Select the *CMP* and *INI* files to upload from the pull down menus at the top of the Load Management page.

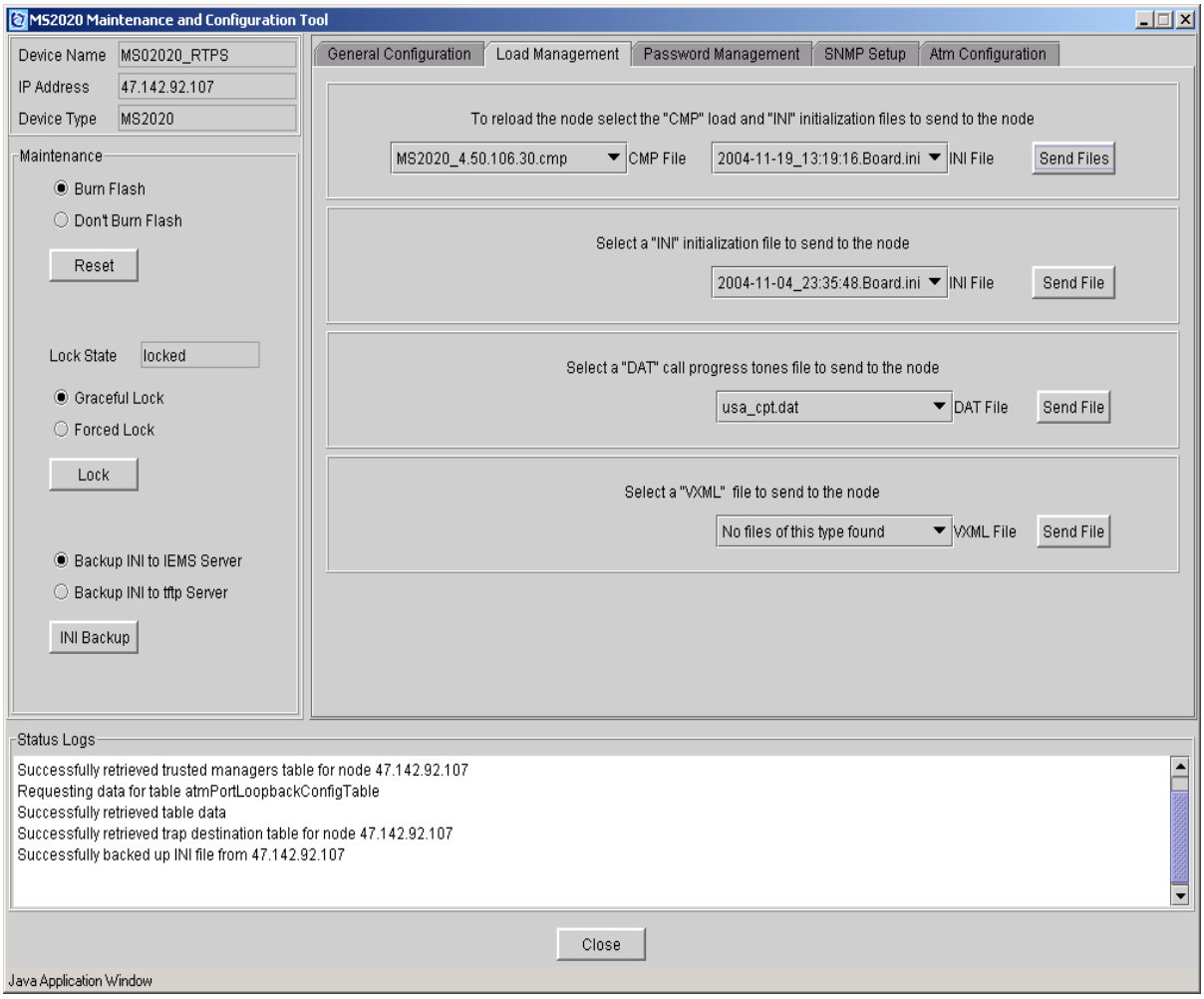
Note 1: The *CMP* and *INI* files associated with the new software load must be installed on the Media Server 2000 nodes. These are the files you copied in step 19 on page 1431.

Note 2: If you upgraded the INI file in step 19 on page 1431, you will see the upgraded file in the pull down list. Select this upraded INI file to upload to the Media Server 2000 node.

7 Select the *DAT* file to upload from the pull down menus in the middle of the Load Management page.

Note: The *DAT* file is the .dat file you copied in the step 8 on page 79 of the Backing up Media Server 2000 Series files section above.

8 Select the *Send Files* button to start the upgrade (load the files to the node).



The status logs section at the bottom of the Load Management window displays the load that is being sent. Also, periodic updates display information on how long the burn process has been progressing.

Example

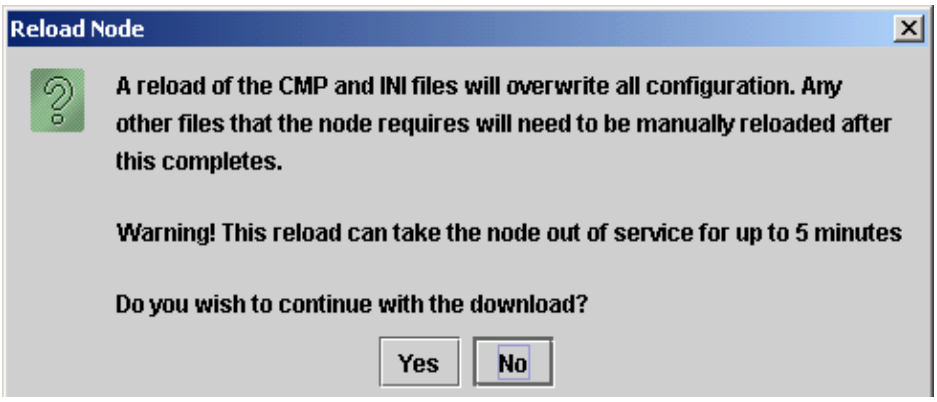
Waiting for load to be burned into flash. Time from burn start is 2 minutes 1 secs

Waiting for load to be burned into flash. Time from burn start is 2 minutes 21 secs

Download of 2004-11-19_13:19:16.Board.ini starting.

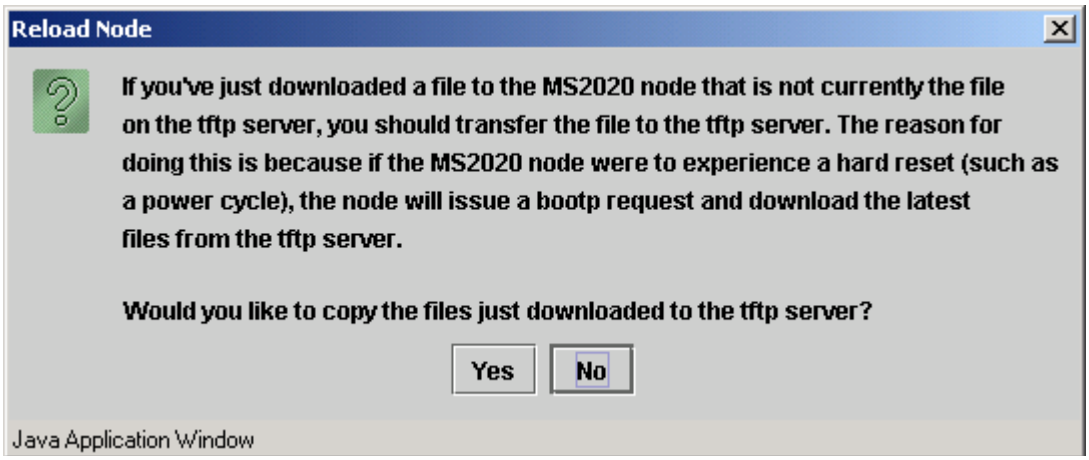
Download of 2004-11-19_13:19:16.Board.ini completed.

While executing the upgrade, the following message displays.



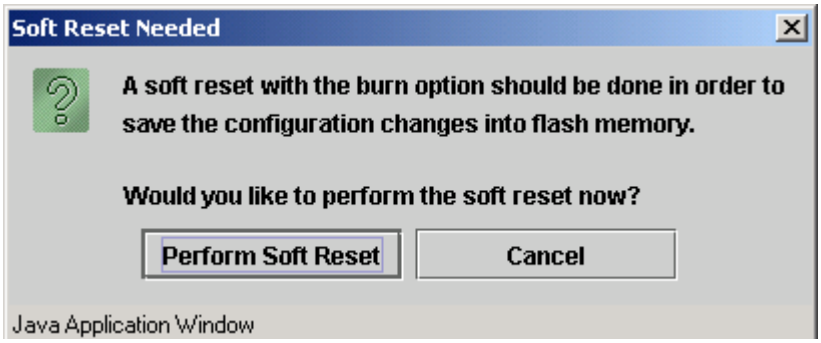
9 Select *Yes* to proceed with the upgrade.

Once the loads have been sent the following screen displays prompting you to save the file to the tftp server if it is different than the file already there. Because this is an upgrade, the file you just loaded is not yet on the tftp server.



10 Select *Yes* to save the file to the tftp server.

11 After the upgrade completes, the following screen displays.



CAUTION

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! Make sure both Media Servers are locked before proceeding.

12 Select *Perform Soft Reset*.

13 On the left side of the Configuration and Maintenance GUI window, select *Unlock* to unlock the node.

14 To upgrade additional Media Server 2000 nodes, do the following:

a complete step 19d, step 20 and step 21 of Copying the files to the audiocodes directory on page 1426

b complete Procedure to upgrade a Media Server 2000 on page 1433

15 Edit the object properties in the IEMS for the MS2000 network element you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the Device Version field.

- Editing and viewing object properties using Java Web Client on page 1841
- Editing and viewing object properties using Web Client on page 1846

16 You have completed this procedure.

Media Server Series 2000 patches

Media Server 2010 and 2020 patches and maintenance releases are available through Nortel web delivery, Electronic Software Delivery (ESD), or CD-ROM. Patches must be applied after the upgrade. When applying a patch always refer to either the .txt file for installation instructions.

The following procedure documents applying Media Server Series 2000 patches, and should be followed after the Procedure to upgrade a Media Server 2000 if patching is done following an upgrade to a higher release.

Applying Media Server 2010 and 2020 patches

From your web browser:

1. Go to http://www.nortel.com.
2. Select Support & Training.
3. Select Software Downloads.
4. Select Browse Product Support.
5. Select Product Categories.
6. Select Voice & IP Communications.
7. Select Software from the appropriate product; either Media Server 2010 or Media Server 2020.
8. Select the desired patch. Patches are indicated by applicable release level and status. Every customer should be at the released level status, verification offices should apply pre-released patches if posted. If you are not sure which patch to apply, please contact your next level of

   support.
9. Logon to the software repository site if prompted.
10. Select and download the documentation file.
11. Select and download the Download file.
12. Apply the patch as instructed in the associated documentation file into EVERY MS20x0 device in the office.
13. You have completed this procedure.

Media Gateway (MG) 9000

Before upgrading the MG 9000

Perform the required prerequisite upgrade as follows:

Network	MG 9000 applies to:	Previous Upgrade
ATM	UA-AAL1	Media Server 2000 Series on page 1413
IP	UA-IP[1]	Media Server 2000 Series on page 1413
Tri-Modal	configuration specific	Media Server 2000 Series on page 1413

1.Includes IP International UA-IP

After upgrading the MG 9000

Perform the next required upgrade as follows:

Network	MG 9000 applies to:	Next Upgrade
ATM	UA-AAL1	Universal Signaling Point on page 1490
IP	UA-IP[1]	Universal Signaling Point on page 1490
Tri-Modal	configuration specific	Universal Signaling Point on page 1490

1.Includes IP International UA-IP

About the MG 9000

The Nortel Networks Media Gateway 9000 (MG 9000) is an access gateway positioned at the edge of the Succession Network, offering a wide range of voice, data, and video services.

Universal Access-AAL1 (UA-AAL1) applications provide voice, DSL, and private lines services over a unified ATM network in the North American market. The UA-AAL1 solution uses the ATM transport network to carry packetized voice, call control signaling, OAM and data traffic.

Universal Access IP (UA-IP) applications use the IP network to carry packetized voice, call control signaling, OAM and data traffic to provide end office plain old telephone service (POTS), P-Phone, and Coin lines services, trunking services, and DSL services in International and North American markets.

Upgrading the MG 9000 network element

This section contains upgrade information and procedures for the MG 9000 network element (NE).

When to use this document

Use this document to upgrade the MG 9000 network element from SN06.2 or SN07 to SN08.

When upgrading the MG 9000 network element from SN06.2 to SN08 or SN07 to SN08, the following activities take place in the following order:

- follow the procedure Upgrading MG 9000 Manager software from SN06.2 or SN07 to SN08 on page 1123
- install the GUI client application
- provision userids
- upgrade software in MG 9000 cards

For a high level MG 9000 NE upgrade summary, refer to either the MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (one-server) on page 1448 or the MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (two-server) on page 1454, depending on the appropriate upgrade path. These checklists reference detailed procedures that are provided later in the document.

Refer to *Upgrading the MG 9000*, NN10048-461for the following related procedures:

- downgrading the MG 9000 software
- upgrading the MG 9000 cards individually, by card type, or all cards

Upgrade strategy

The following high-level strategy summarizes network upgrade procedures required when upgrading the MG 9000 NE:

1. Upgrade the Communication Server 2000 (CS2000) Management Tools software to ensure node and line provisioning applications are updated (CS 2000 Management Tools and Clients (CMT) on page 523).
2. Remove the existing SN06.2 or SN07 software packages. Perform this activity just prior to upgrading the Succession Server Platform Foundation Software (SSPFS). SN06.2 or SN07 SSPFS software does not operate with SN08 SSPFS software.

3. Upgrade the SSPFS software (Upgrading SSPFS software on page 666). This includes the SSPFS on the MG 9000 Manager master and mid-tier servers.

   Note: The CS2000 Management Tools and the SSPFS platform software must be upgraded to SN08 before upgrading the MG 9000 Manager server and mid-tier software (step 4).

4. Upgrade the MG 9000 Manager software in the following order: server, mid-tier.
5. Upgrade all of the MG 9000 intelligent cards and the MTA and xDSL cards to SN08 from an image received on CD or through electronic software delivery (ESD) using the mg9kuptool accessible from the command line interface (CLI) on the MG 9000 master server.

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 can be performed during upgrades. During the upgrade of a given NE, the MG 9000 Manager blocks any attempt to change data for that NE. The MG 9000 Manager displays a minor warning indicating provisioning is halted and the database is unavailable for that NE.
  - — PM collection cannot be performed during the time between stopping the mid-tier server and when the OM Collector starts.
  - — OC3 carriers must not be in split-mode. For details, refer to the procedure “Recovery from APS Split-mode” in *MG 9000 Fault Management*, NN10074-911.
  - — Refer to the following table to identify the PEC codes for SN07-SN08 cards.

SN08 upgrade PEC codes

Card type	Pre-SN07 PEC codes	SN07 new hardware PEC codes	SN08 new hardware PEC codes
ITP	NTNY30AA or NTNY30BA (IP)	NTNY30BA or NTNY30CB	
ITX	NTNY41AA	NTNY41BA	
DS-512 ABI	NTNY43AA	NTNY43BA or NTNY43BB	NTNY43xx?

SN08 upgrade PEC codes

Card type	Pre-SN07 PEC codes	SN07 new hardware PEC codes	SN08 new hardware PEC codes
DCC-OC3 (SCO)	NTNY45AA	NTNY45CA	
Hybrid DCC-OC3 (OC3)	NTNY45AA		
DCC-DS1IMA (SCI hybrid)	NTNY45BA	NTNY45BA	
DCC-GigE			NTNY45FA
MTA			NTNY42AB

- Recommendations for limiting service impact: none

Tools and utilities

The MG 9000 supports software upgrades and downgrades. Procedures in this document reference these activities. For MG 9000 Manager software downgrade procedures, refer to *Upgrading the MG 9000*, NN10048-461.

The MG 9000 Manager supports patching through the network patch manager (NPM). Patching procedures and information are located in Carrier Voice over IP Network patching on page 1850.

The command line interface (CLI) mg9kuptool provides an automated software upgrade for the MG 9000 cards, including the MTA and xDSL cards. The mg9kuptool can upgrade multiple MG 9000 NE devices. The mg9kuptool automates device patching after the upgrade. Although the mg9kuptool does not provide upgrade process status messages, those messages can be obtained by performing a telnet to the server and enter the mg9kuptool -query command. The mg9kuptool upgrade procedure is Upgrading the MG 9000 to SN08 using the CLI mg9kuptool on page 1474.

Pre-upgrade requirements

Ensure the CS 2000 Manager has been upgraded to SN08 before upgrading any MG 9000s to SN08.

The MG 9000 Manager must be upgraded to SN08 before the MG 9000 cards are upgraded to SN08. An MG 9000 Manager at software level

SN08 is capable of managing an MG 9000 NE operating at SN06.2, SN07, or, SN08.

Note: All alarms on the MG 9000 Manager and MG 9000 network element must be cleared prior to proceeding with the SN06.2 or SN07 to SN08 upgrade process.

Do not provision any new data to the NEs during upgrade activities.

Entry criteria

The following are the criteria for entering the SN06.2 or SN07 to SN08 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 SN06.2 or SN07 with all patches applied
  - MG 9000 Manager software must be at SN06.2 or SN07 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 SN08 (Upgrading SSPFS software on page 666).
  - CS 2000 Management Tools must be upgraded to SN08 prior to upgrading the MG 9000 Manager to SN08.

— MG 9000 card upgrades are addressed in Upgrading the MG 9000 to SN08 using the CLI mg9kuptool on page 1474.

— ensure MG 9000 PSEs are configured correctly before the upgrade starts as described in the MG 9000 Manager upgrade procedures Upgrade interdependencies on page 1110.

- if this is an SN06.2 or SN07 to SN08 Sun Netra cluster (two-server) upgrade, run a getpatch to retrieve all SN08 patches before the upgrade starts. Refer to Transferring patches delivered on CD to the NPM database on page 1884 for more information

Exit criteria

The following are the criteria for exiting from the SN06.2 or SN07 to SN08 upgrade process:

- The upgrade was successful
  — after the MG 9000 NE is successfully discovered in SN08
- 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 procedure “Upgrading the MG 9000 Manager software to a maintenance release” in *Upgrading the MG 9000*, NN10048-461.
- The MG 9000 uses the Network Patching Manager (NPM) patching system. Any device requiring patching must first be audited to

determine the load name compatibility with the patch before applying the patch

For more information on patching refer to Carrier Voice over IP Network patching on page 1850.

MG 9000 SN08 upgrade checklists

SN06.2 or SN07 to SN08 t1400/N240 one-server (simplex) upgrade checklist

Use the following table as a checklist for upgrading the MG 9000 network element from SN06.2 or SN07 to SN08 in a t1400/N240 single-server (simplex) configuration. Enter a check mark (√) in the √ column as each step or procedure is completed.

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (one-server)

	Activity	Procedure	√
For each network element in SN06.2			
1	Ensure all MG 9000 Patch Image (PI) load files have been copied to the CS2000 Core Manager (SDM) to support upgrade / downgrade activity from CD-ROM or Electronic Software Delivery.	Refer to "*Upgrading the CS 2000 Core Manager*, NN10060-461." Refer to Installing MG 9000 loads into CS 2000 Core Mgr from CDROM on page 1460 or Deliver and install MG 9000 loads using Electronic Software Delivery on page 1463.	
2	Provisioning a floating IP address, if one has not already been provisioned.	Refer to Provisioning a floating IP address on page 1471.	

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (one-server)

	Activity	Procedure	√
3	If this is an SN06.2 to SN08 upgrade, 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: • ITXBITS - if syncing to the ITX card • DCCBITS - if syncing to the DCC cards and the cable is connected to the DCC card BITS connector • Network - if syncing to the upstream network connection Refer to *MG 9000 Configuration Management*, NN10096-511.	
4	If the SDM is freshly installed, remove the SSH keys on all cards in the gateway (or gateways).	Go to the LCI on the active DCC card. Select maintenance. Select the shelf with the active DCC card. Select the active DCC card. Select Debug Cmds. Enter command number 6 (/keymgmt/clrsshclientkeys) to remove all the SSH client keys.	
5	Perform a card upgrade on the following cards on the NE: all DS1s, ABIs, ITPs, ITXs, DCCs, MTA, and xDSLs.	Perform the procedure Upgrading the MG 9000 to SN08 using the CLI mg9kuptool on page 1474.	
	Note: This is a safe stopping point.		

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (one-server)

	Activity	Procedure	√
6	Configure Preshared Keys between the MG 9000 and the MG 9000 Manager	Perform the following to configure Preshared Keys. ***Note 1:*** If Preshared Keys are not configured, certain functions such as software upgrade or ESA data download will not run. ***Note 2:*** Preshared Keys must be configured at this time. If it becomes necessary to downgrade the MG 9000, the downgrade cannot proceed until the Preshared Keys are configured. 1. From the MG 9000 Manager Subnet View, select the NE just upgraded and select Configuration->View/Modify NE Properties. The Properties View appears. 2. In the NE Encryption Key field, enter a 20-65 alphanumeric key and record this key for entry later. 3. Click Apply. 4. From the LCI for the same NE, select Connections. 5. Select OAMP Connection from the menu bar at the left. The OAMP Connection screen appears. 6. In the Preshared Key field, enter the same 20-65 alphanumeric key that was entered in step 2 above. ***Note:*** This value must match what was entered in the Properties View in step 2 to ensure important MG 9000 functions work properly. 7. Click Submit.	

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (one-server)

	Activity	Procedure	√
7	Create patched images of all MG 9000 loads, only if patches were applied during upgrade	1. After the MG 9000 cards have been upgraded to SN08 and all other MG 9000 Manager workstations have been upgraded to SN08, perform the following procedure to image the network element (NE) cards for use in upgrading the cards in other NEs. ***Note 1:*** Perform the following steps after the following conditions are met: • the NPM is at SN08 • the suite of MG 9000 Manager servers are running SSPFS08 ***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-DS1-IMA MG 9000). Ensure the NEs selected include all MG 9000 intelligent card types in the office. First the user will upgrade all the intelligent cards and the MTA and xDSL cards on a DCC-OC3 MG 9000 using the latest available PI loads. During the upgrade, any available patches that were not included on the PI load are applied. After patching is complete, the user will take an image of the DCC-OC3 MG 9000 using the NPM. Next, the user will upgrade a DCC-IMA MG 9000 using the PI loads just created. During the upgrade, any available patches for any remaining intelligent card types (including the DCC-DS1-IMA) that were not patched during the DCC-OC3 MG 9000 upgrade are applied. After upgrading is complete, the user will take an image of the DCC-DS1-IMA MG 9000 using the NPM. a. Use the following to determine the next step. • if there were additional patches added to the pre-patched image loadfile, go to step c • if there were no additional patches added to the pre-patched image loadfile, go to step b	

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (one-server)

	Activity	Procedure	√
	Create patched images of all MG 9000 loads (contd)	b. Apply remaining SN08 patches to all cards on this NE with DCC OC3 cards. Information on remaining patches is obtained by using the mg9kuptool -postcheck command from the CLI. c. Take an image of the inactive cards on this NE with DCC-OC3. Refer to the "Performing a device image using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450 for steps on performing a device image. Select SmartImage->MG9KDEVICES. d. 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. e. Apply the remaining patches to all cards on this NE with DCC DS1-IMA cards. Information on remaining patches is obtained by using the mg9kuptool -postcheck command from the CLI. f. Take an image of the inactive cards on this NE with DCC DS1-IMA cards that were not imaged in step c above. Refer to the "Performing a device image using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450 for steps on performing a device image. Select SmartImage->MG9KDEVICES. g. Use the images created in the previous steps to upgrade all the of the cards on all the remaining NEs to be upgraded to SN08.	
8	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. Refer to procedure "Provisioning ESA" in *MG 9000 Configuration Management*, NN10096-511.	
	Note: This is a safe stopping point.		

After all NEs are at SN08 and there is no need to downgrade to SN06.2 or SN07 proceed to the next step:

Note: If it is necessary to downgrade the MG 9000 and MG 9000 Manager, perform procedure "Downgrading the MG 9000 Manager from SN08 to SN06.2 or SN07" in *Upgrading the MG 9000*, NN10048-461, otherwise proceed to the next step.

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (one-server)

	Activity	Procedure	√
	Note: After step 6 is performed, the MG 9000s cannot be downgraded to SN06.2 or SN07 without service data loss.		
	Note: Proceed to the next step only after the one night process (ONP) is complete.		
9	Clean up old data in the NPM database.	Perform the procedure Cleaning up old data in the NPM database on page 2014.	
10	This procedure is complete.		

SN06.2 or SN07 to SN08 N240 two-server (cluster) upgrade checklist

Use the following table as a checklist for upgrading the MG 9000 network element from SN06.2 or SN07 to SN08 in a two-server (cluster) configuration. Enter a check mark (√) in the √ column as each step or procedure is completed.

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (two-server)

	Activity	Procedure	√
On the Inactive node			
For each network element in SN06.2 or SN07			
1	Ensure all MG 9000 Patch Image (9PI) load files have been copied to the CS2000 Core Manager (SDM) to support upgrade / downgrade activity from CD-ROM or Electronic Software Delivery.	Refer to "*Upgrading the CS S2000 Core Manager*, NN10060-461." Refer to Installing MG 9000 loads into CS 2000 Core Mgr from CDROM on page 1460 or Deliver and install MG 9000 loads using Electronic Software Delivery on page 1463.	
2	Provisioning a floating IP address.	Refer to Provisioning a floating IP address on page 1471.	
3	If this is an SN06.2 to SN08 upgrade, 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: • ITXBITS - if syncing to the ITX card • DCCBITS - if syncing to the DCC cards and the cable is connected to the DCC card BITS connector • Network - if syncing to the upstream network connection Refer to *MG 9000 Configuration Management*, NN10096-511.	

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (two-server)

	Activity	Procedure	√
4	If the SDM is freshly installed, remove the SSH keys on all cards in the gateway (or gateways).	Go to the LCI on the active DCC card. Select maintenance. Select the shelf with the active DCC card. Select the active DCC card. Select Debug Cmds. Enter command number 6 (/keymgmt/clrsshclientkeys) to remove all the SSH client keys.	
5	Perform a card upgrade on the following cards on the NE: all MTA, xDSLs, DS1s, ABIs, ITPs, ITXs, and DCCs.	Perform the procedure Upgrading the MG 9000 to SN08 using the CLI mg9kuptool on page 1474.	
	Note: This is a safe stopping point.		

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (two-server)

	Activity	Procedure	√
6	Configure Preshared Keys between the MG 9000 and the MG 9000 Manager	Perform the following to configure Preshared Keys. ***Note 1:*** If Preshared Keys are not configured, certain functions such as software upgrade or ESA data download will not run. ***Note 2:*** Preshared Keys must be configured at this time. If it becomes necessary to downgrade the MG 9000, the downgrade cannot proceed until the Preshared Keys are configured. 1. From the MG 9000 Manager Subnet View, select the NE just upgraded and select Configuration->View/Modify NE Properties. The Properties View appears. 2. In the NE Encryption Key field, enter a 20-65 alphanumeric key and record this key for entry later. 3. Click Apply. 4. From the LCI for the same NE, select Connections. 5. Select OAMP Connection from the menu bar at the left. The OAMP Connection screen appears. 6. In the Preshared Key field, enter the same 20-65 alphanumeric key that was entered in step 2 above. ***Note:*** This value must match what was entered in the Properties View in step 2 to ensure important MG 9000 functions work properly. 7. Click Submit.	

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (two-server)

	Activity	Procedure	√
7	Create patched images of all MG 9000 loads, only if patches were applied during the upgrade	1. After the MG 9000 cards have been upgraded to SN08 and all other MG 9000 Manager workstations have been upgraded to SN08, perform the following procedure to image the network element (NE) cards for use in upgrading the cards in other NEs. ***Note 1:*** Perform the following steps after the following conditions are met: • the NPM is at SN08 • the suite of MG 9000 Manager servers are running SSPFS08 ***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-DS1-IMA MG 9000). Ensure the NEs selected include all MG 9000 intelligent card types in the office. First the user will upgrade all the intelligent cards on a DCC-OC3 MG 9000 using the latest available PI loads. During the upgrade, any available patches that were not included on the PI load are applied. After patching is complete, the user will take an image of the DCC-OC3 MG 9000 using the NPM. Next, the user will upgrade a DCC-IMA MG 9000 using the PI loads just created. During the upgrade, any available patches for any remaining intelligent card types (including the DCC-DS1-IMA) that were not patched during the DCC-OC3 MG 9000 upgrade are applied. After upgrading is complete, the user will take an image of the DCC-DS1-IMA MG 9000 using the NPM.	

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (two-server)

	Activity	Procedure	√
	Create patched images of all MG 9000 loads (contd)	a. Use the following to determine the next step. • if there were additional patches added to the pre-patched image loadfile, go to step c • if there were no additional patches added to the pre-patched image loadfile, go to step b b. Apply remaining SN08 patches to all cards on this NE with DCC OC3 cards. c. Take an image of the inactive cards on this NE with DCC OC3 cards. Refer to the "Performing a device image using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450 for steps on performing a device image. Select SmartImage->MG9KDEVICES. d. Upgrade one NE with DCC-DS1-IMA cards with the SN08 MG 9000 patched images just created in the previous step. Load all cards on this NE with the supplied image. e. Apply the remaining patches to all cards on this NE with DCC DS1-IMA cards. f. Take an image of the inactive cards on this NE with DCC DS1-IMA cards that were not imaged in step c above. Refer to the "Performing a device image using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450 for steps on performing a device image. Select SmartImage->MG9KDEVICES. g. 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	
8	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. Refer to the "Provisioning ESA" procedure in *MG 9000 Configuration Management*, NN10096-511.	
	Note: This is a safe stopping point.		

MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (two-server)

	Activity	Procedure	√
After all NEs are at SN08 and there is no need to downgrade to SN06.2 or SN07 proceed to the next step: ***Note:*** If it is necessary to downgrade the MG 9000 and MG 9000 Manager, perform procedure "Downgrading the MG 9000 Manager from SN08 to SN06.2 or SN07" in *Upgrading the MG 9000*, NN10048-461, otherwise proceed to the next step.			
	Note: Proceed to the next step only after the one night process (ONP) is complete.		
9	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 *Upgrading a Carrier Voice over IP Network*, NN10440-450.	
	Note: After step 9 is performed, the MG 9000s cannot be downgraded to SN06 without service data loss.		
10	Clean up old data in the NPM database.	Perform the procedure Cleaning up old data in the NPM database on page 2014.	
11	This procedure is complete.		

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 SN06.2 or SN07 to SN08, ensure the SN06.2 or SN07 loads are currently in the SDM/CBM in the event there is a need to perform a software downgrade from SN08 to SN06.2 or SN07.

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, MG9K0080, 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 Change the ownership of all files in the /swd/mg9k directory to imaging userid by performing the following steps:

a Login as root to the SDM/CBM as root.

b Change ownership recursively of the /swd/mg9k directory by typing

```
# chown -R <imaging userid>:<userid group>
/swd/mg9k
```

where

imaging user id is the user id for the image server

userid group is the group to which the userid belongs

c Log out of the SDM/CBM.

10 Remove the CDROM.

11 This procedure is complete.

Deliver and install MG 9000 loads using Electronic Software Delivery

Purpose of this procedure

This procedure describes how to transfer MG 9000 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.

Note: For information on how to install MG 9000 load from CD-ROM, refer to procedure Installing MG 9000 loads into the CS 2000 Management Tools Manager from CDROM on page 1460.

When to use this procedure

Use this procedure after receiving electronic notification for the following software loads:

- MG9KC0080.n.V.NCL.NAP.VAULT.nn.D.tar.gz - for standard NCL release
- MG9KW0080.n.V.NCL.NAP.VAULT.nn.D.tar.gz - for standard International NCL release
- MG9K0M080.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 Display the available disk space in the directory by typing

`# df -k`

and pressing the Enter key.

Example response

```
# df -k
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2         3082223  144125 2876454    5%    /data/iso_esd
```

4 Record the amount of available disk space, which is provided in kilobytes. You will need the information later in this procedure.

5 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.

6 Change the transfer mode to binary by typing

`ftp> bin`

and pressing the Enter key.

a List the contents of the drop box by typing

```
ftp> ls
```

7 Locate the uncompressed image file you want to transfer, and identify the size of the file, which is provided in bytes.

Note: Divide the number of bytes by 1024 to convert the size to kilobytes.

8 Compare the size of the uncompressed image file with the amount of available space you recorded in step 4.

9 Use the following table to determine your next step.

If	Do
the server has enough available disk space	step 11
otherwise	step 10

10 Clear additional disk space following local office policy, before you continue with this procedure. If necessary, contact your next level of support.

11 Retrieve the ESD software load by typing

`ftp> get <esd_filename>`

and pressing the Enter key.

where

<esd_filename>
is the ESD filename for the MG 9000 software load

12 Repeat steps 7 through 11 for all ESD software loads recorded in the notification from Nortel Networks.

13 End the FTP session by typing

`ftp> bye`

and pressing the Enter key.

14 Become the root user by typing

`$ su - root`

and pressing the Enter key.

15 When prompted, enter the root password.

16 Mount the ISO image 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)


 X - exit


select -
```

c Enter the number next to the "mount_image" option in the menu.

If the response is	Do
Enter the full path of the ISO image	substep e
ISO Image Already Mounted	substep d

d Enter the number next to the "mount_image" option in the menu and retry substep c.

Note: If the umount_image or mount_image command is unsuccessful a second time, contact your next level of support.

e When prompted, enter the full path name of the ISO image on the server from the root.

The contents of the ESD software file are placed in directory /tmpmnt

Note: Do not attempt to access the /tmpmnt directory until the mount command is complete.

If the response is	Do
It 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.	step f
Provided full path to ISO image does not exist	Verify the location and name of the ISO 9660 image.
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 your next level of support.
ERROR MOUNTING <ESD_filename>	This response indicates that either the ISO 9660 file is corrupt, or the /tmpmnt directory has been deleted. Repeat this procedure, and if it fails a second time, contact your next level of support.

f Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

```
select - x
```

and pressing the Enter key.

17 Use the following table to determine your next step.

If you want to install the software	Do
later	go to step 18

If you want to install the software	Do
now	go to step 19

18 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 19, but in sub-step e, specify the new location of the software instead of typing /tmpmnt/noarch.

Continue with step 20.

19 Complete the following steps to install the software on the CS 2000 Core Manager.

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.

After the load file is installed on the CS 2000 Core Manager, the transferred .rpm package is deleted from the CS 2000 Core Manager.

f Exit the installation program by typing

 # x

and pressing the Enter key.

20 Unmount the ISO image 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)


 X - exit


select -
```

c Enter the number next to the "umount_image" option in the menu.

d Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

`select - x`

and pressing the Enter key.

21 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

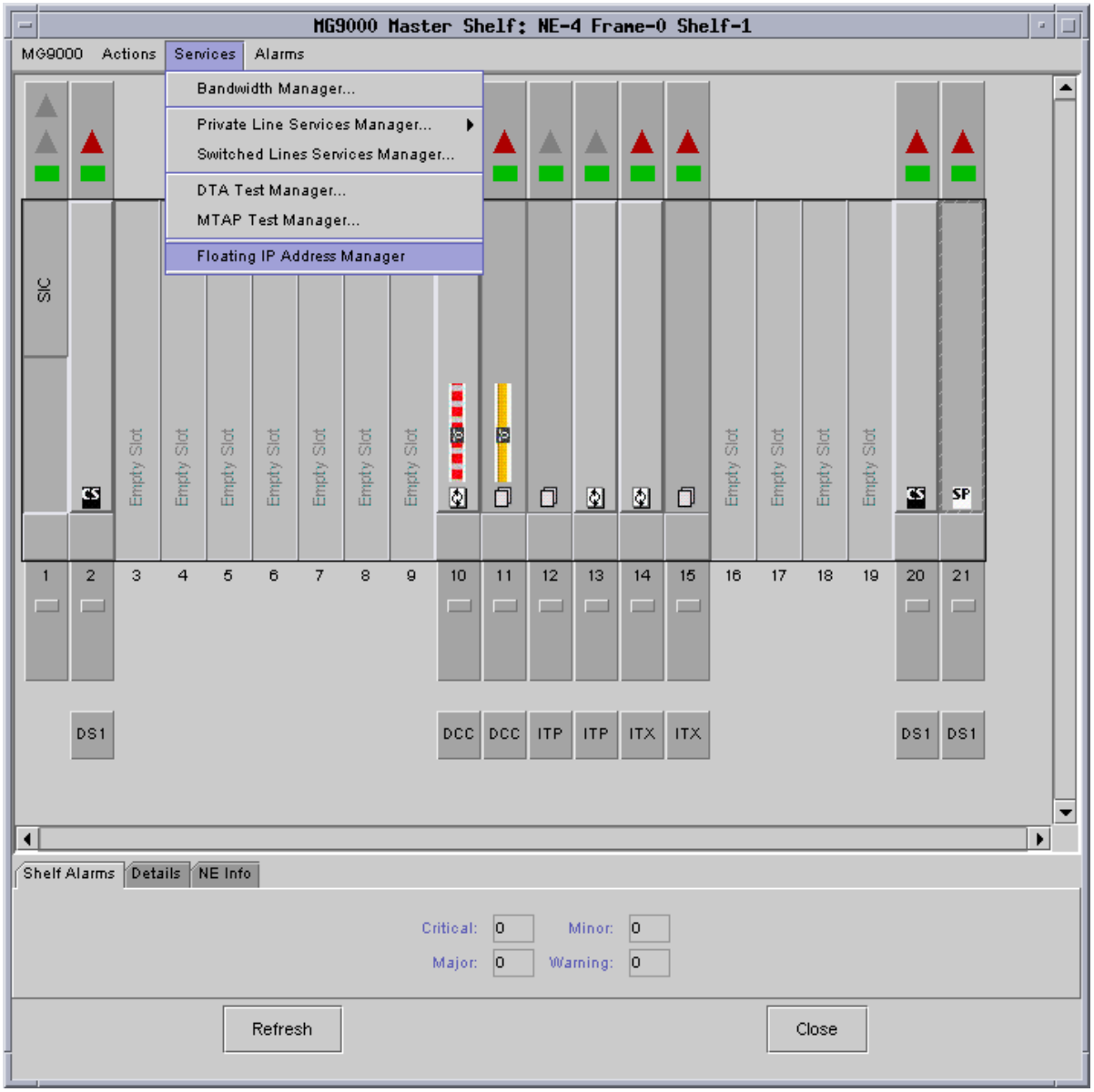
At the MG 9000 Manager

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.

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 the MG 9000 to SN08 using the CLI mg9kuptool

When to use this procedure

Use the following procedure when it is necessary to upgrade the MG 9000 to SN08. The upgrade is performed using the command line interface (CLI) mg9kuptool.

Note: Fix upgrade problems by using the "Software upgrade errors and problem resolution" in *Upgrading the MG 9000*, NN10048-461. Once the problem has been resolved, re-enter the command which failed for the single NE. After successfully completing the command for the single NE, continue with the next step in the mg9kuptool for all NEs being upgraded. For example, while downloading NE 1, 2, and 3, NE2 fails. Clear the download failure with NE2, open another mg9kuptool, and download NE2. Once NE 1, 2, and 3 have all completed the download step successfully, proceed with the precheck step for NEs 1, 2, and 3.

The mg9kuptool enables the upgrade process to be separated into the following two time frames, thereby using operating company personnel time more effectively.

- preparation phase which includes downloading of the card loads, that takes place outside of the maintenance window, with no service impact
- upgrade phase, which occurs within the maintenance window

The following table shows the command options used in the mg9kuptool.

mg9kuptool command options

Time frame	Command options	Description
Preparation phase - outside the maintenance window	-configure	Provides the configuration of the upgrade tool. This includes the list of NEs to upgrade, the name and location of the card loads.
	-prepare	Provides information to the user to determine if the system is prepared for the upgrade. It is executed for each node in the target list <-n>.
	-download	Downloads the card loads as defined in the upgrade plan. It is executed for each node in the target list <-n>.
	-precheck	Reviews the overall system health of each node in the target list <-n> in preparation for the upgrade. Any problems discovered are returned so that action can be taken to correct the issue before the upgrade begins.
Upgrade phase - inside the maintenance window	-upgrade	Executes the actual upgrade process defined in the upgrade plan. It is executed for each node in the target list <-n>. When the upgrade is complete, all available patches will be applied.
	-postcheck	Determines if any alarms were raised and reports any patches that were not applied. This command is executed for each node in the target list <-n>.
	-query	Provides status information regarding the upgrade process for each node in the target node list <-n>.
	-abort	Terminates the upgrade step being executed for each node in the target node list <-n>.
	-n	Describes the list of nodes on which to apply the operation. This is a comma separated list of NE numbers. If the list is specified as ALL then the operations is applied to all nodes in the plan. This option may be used on all commands except <configure> and <prepare>.

When the mg9kuptool is executed, with or without options, an MGEM714 log is output. The MGEM714 log is accessible from custlog.

For information on retrieving custlog, refer to "Retrieving MG 9000 logs" in *MG 9000 Fault Management*, NN10074-911.

Limitations and restrictions

The following limitations and restrictions apply to the use of the mg9kuptool.

- The mg9kuptool does not prevent two users from modifying the configuration data. However, this could produce unexpected results.
- Configure only the NEs which should be upgraded at the same time. However, the number of NEs that can be configured simultaneously is four.
- Minor and Warning alarms on the NEs are not indicated as an error since the MG 9000 will allow upgrades on the cards.
- The maximum number of mg9kuptool sessions that can be launched is five.
- When the user performs the download command, the MG 9000 will download the specified load, even if the MG 9000 already has that load.
- After a successful download command is performed on a card, a normal download will download a new patched image (PI) only if the requested PI base loadname is different from the PI base loadname specified for the prepare download. Note that patch content does not alter the PI base loadname.
- If a new image of an existing MG 9000 load is create, the only way the new load can be downloaded to the cards is to use the download command.
- The download command is not supported for card types MTA and XDSL.
- The mate load functionality on the MG 9000 does not copy over prepare (prep) download files.
- The mg9kuptool only provides support for a full node upgrade. The mg9kuptool does not allow
  - — single cards to be upgraded
  - — protection group upgrades
  - — load from mate
- If an upgrade fails, there is no retry mechanism. However, if all cards of a specific type (for example, ITP cards) are running the desired load and do not have a load in the prep download area, this card type is skipped during the upgrade command. This assumes that

the upgrade command is re-entered due to some failure. Patching of these cards is not skipped.

- The abort command stops processing the card type which is upgrading once the MG 9000 completes the command it is currently processing (such as, once the apply step is complete). If other card types are already upgraded, they remain on the upgraded or downgraded load.
- NTNY45FA Gigabit ethernet DCC cards are not included in the CLI upgrade.
- Auto processes on the NPM are not automatically turned off nor automatically turned on. The customer must turn off auto processing at the NPM prior to upgrading. The precheck only alerts the customer to ensure auto processes are turned off in the NPM. The upgrade and postcheck alerts the customer to manually check and turn auto processing on again.
- The download and upgrade times are only estimates.
- The following limitations apply to MTA and xDSL cards as part of the mg9kuptool upgrades:
  - Prior to upgrading MTA or xDSL cards, the MG 9000 Manager verifies that all the cards are in an Unlocked/Enabled state. If any card is not in the correct state, the MG 9000 Manager will not perform the upgrade.
  - To upgrade MTA and xDSL cards, the MG 9000 Manager will lock the card, download the load to the card, and then unlock the card. The order in which the MG 9000 Manager upgrades XDSL or MTA cards cannot be specified as part of the upgrade.
  - The lock request of an xDSL card will fail if the card has an active call. If the lock request fails for a given xDSL card, the MG 9000 Manager will note the failure and attempt to upgrade the remaining xDSL cards. Once the MG 9000 Manager has upgraded the remaining xDSL cards, the MG 9000 Manager will halt the upgrade process. The MG 9000 Manager will report that some of the xDSL cards could not be upgraded.
  - If the download or unlock of any MTA or XDSL card fails, the MG 9000 Manager immediately halts the upgrade process.
  - If an MTA or xDSL card already has the load file specified in the upgrade request, the MG 9000 Manager will consider the card already upgraded and move on to the next card to upgrade.
  - When upgrading xDSL cards, the MG 9000 Manager can upgrade only those cards with supported hardware. If a given xDSL card does not have a CLEI code of VA1AAAAAA, the

MG 9000 Manager will skip that card and move on to the next card to upgrade.

— If the user aborts an upgrade while the MG 9000 Manager is upgrading the xDSL or MTA cards, the MG 9000 Manager will return all cards to an unlocked state. However, the MG 9000 Manager will not roll back the loads on any of the cards. For instance, assume the user is upgrading all five xDSL cards on a given node. Assume the user aborts the upgrade after the first two cards have upgraded and a third card is in the process of upgrading. The MG 9000 Manager halts the upgrade process after the third card completes its upgrade. In the end, three XDSL cards are running the new load and two XDSL cards are running the old load.

- When the user enters the upgrade command, normally the cards already have a load in the prep load area and do not require another download from the SDM. Exceptions to this are if

  — the card does not have a prep download file

  — the card's prep download file contains a different base load name from the specified load file

Prerequisites

The mg9kuptool requires secure access by performing a telnet over Secure SHell (SSH). Root privileges are required to use the mg9kuptool.

Action

Upgrading the MG 9000 from SN06.2 or SN07 to SN08 using the mg9kuptool without options

At the MG 9000 Manager workstation CLI (server for t1400/N240 simplex or active unit on N240 cluster)

1 Log in to the server through the console port using the root user id and password by typing

znc0y0jm console login: root

The system responds with the following:

```
Password:
<enter the root password>
```

2 Enter the password.

3 To start the mg9kuptool in interactive mode, type

 # /opt/nortel/mg9ksrv_08/bin/mg9kuptool.sh

The system responds with the following

```
1 configure
2 prepare
3 download
4 precheck
5 upgrade
6 postcheck
7 abort
8 query
x exit

Please select an option:
```

4 To configure an NE, or up to 20 NEs for upgrade, type.

$ 1

The system responds with the following:

```
Which NE(s) do you want to upgrade/downgrade?
Enter NE number. If more than 1 NE, separate
them with commas (e.g. 8,9)?

Enter a directory where the loads reside?
(Default:/swd/mg9k)
```

Note 1: When a new upgrade plan is created using the Configure option, it will overwrite the existing plan. For example, if NEs 1 and 2 are configured in the first plan and if the technician plans to configure a second plan with NEs 3 and 4, it will overwrite the existing plan for NEs 1 and 2. Use the Configure option with care. Contact Nortel support for assistance.

Note 2: To identify the NEs to be upgraded, go the MG 9000 Manager. From the Subnet View, click once on an MG 9000 icon. From the menu bar, select Configuration->View/Modify NE Properties and retrieve the NE number from the Properties view.

a Enter the NE number, for example

1

b Enter the directory where the loads reside or accept the default by pressing Enter.

The system responds with the following:

```
220 wnc0y0m0 FTPD Server (Version 21.43.4.0
Oct 20 2004) ready.


Loads found on system:
MTAG07BW_GZ
MTAG08AK_GZ

Enter a load name for the MTA card?
```

c Enter the MTA card load to be used, for example

MTAG08AK_GZ

The system responds with the following:

```
Loads found on system:
DSLA06_2EI.bin
DSLA07BW.bin
```

```
DSLA08AE.bin

Enter a load name for the XDSL card?
```

d Enter the DSL card load to be used, for example

DSLA08AE.bin

The system responds with the following:

```
Loads found on system:
DS1G08AL_GZ
DS1G06FC_2_GZ.tar
DS1G07BW_GZ_wk39.tar

Enter a load name for the DS1 card?
```

e Enter the DS1 card load to be used, for example

DS1G08AL_GZ

The system responds with the following:

```
Loads found on system:
ABIG08AL_GZ
ABIG06FC_2_GZ.tar
ABIG07BX_GZ_wk39.tar
Enter a load name for the ABI card?
```

f Enter the ABI card load to be used, for example

ABIG08AL_GZ

The system responds with the following:

```
Loads found on system:
ITPA08AL_GZ
ITPA06FC_2_GZ.tar
ITPA07BY_GZ_wk42.tar
Enter a load name for the ITP card?
```

g Enter the ITP card load to be used, for example

ITPA08AL_GZ

The system responds with the following:

```
Loads found on system:
ITXA08AL_GZ
ITXA06FC_2_GZ.tar
ITXA07BW_GZ.tar
ITXA07BW_GZ_wk39.tar
Enter a load name for the ITX card?
```

h Enter the ITX card load to be used, for example

ITXA08AL_GZ

The system responds with the following:

```
Loads found on system:
SCOA08AL_GZ
SCOA06FC_2_GZ.tar
SCOA07BW_GZ_wk39.tar
Enter a load name for the SCO card?
```

i Enter the SCO card load to be used, for example

SCOA08AL_GZ

The system responds with the following:

```
Loads found on system:
SCIA08AL_GZ
SCIA06FC_2_GZ.tar
SCIA07BW_GZ_wk42.tar
Enter a load name for the SCI card?
```

j Enter the SCI card load to be used, for example

SCIA08AL_GZ

5 To prepare the NE(s) for upgrade, type

$ 2

Note 1: If faults appear, clear them and return to this step and re-enter the command.

Note 2: If the prepare step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to "Software upgrade errors and problem resolution" in *Upgrading the MG 9000*, NN10048-461 to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 2, and prepare the NE. Once the failed NE has completed the prepare step and other NEs have completed the prepare step, proceed with the download step on all NEs in the first mg9kuptool window.

The system responds with the following:

```
Enter the node number or the node number list
for the prepare request. Press Enter to
continue.
```

The system responds with the following:

```
Have you put the patch files on the NPM? Y/N
```

a Verify that patch files have been moved to the NPM and are available for loading and patching activities. After this is complete, type

Y

The system responds with the following:

```
Upgrading to loads:
/swd/mg9k/MTAG07EJ_1_GZ
/swd/mg9k/DSLA06_2EI
/swd/mg9k/DS1G08BV_GZ.tar
patchlist:
none
/swd/mg9k/ABIG08BV_GZ.tar
patchlist:
AMZ005
/swd/mg9k/ITPA08BV_GZ.tar
patchlist:
AMZ006
HDD013
HDD014
HDD015
/swd/mg9k/ITXA08BV_GZ.tar
patchlist:
none
/swd/mg9k/SCOA08BV_GZ.tar
patchlist:
AMZ007
AMZ008
HDD016
/swd/mg9k/SCIA08BV_GZ.tar
patchlist:
AMZ008
Please compare the patchlists above against
the Nortel web page.
NE# 8: time to download is 60 minutes
time to upgrade is 30 minutes
time to patch is 27 minutes
```

Note: Look for any errors after all the NE upgrade and patching times are listed.

6 To download the software to the cards, type

$ 3

The system responds with the following:

```
Enter the node number or node number list for
the download request:
```

Press Enter to continue.

Note 1: Wait for the system response. This may take a few minutes, depending on the size of the MG 9000 being downloaded. Also look for any error messages.

Note 2: If the download fails, it can be due to an SSH key mismatch. Remove the SSH keys using either procedure MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (one-server), step 4 on page 1449 or MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (two-server), step 5 on page 1455, depending on your server configuration.

Note 3: If the download step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to "Software upgrade errors and problem resolution" in *Upgrading the MG 9000*, NN10048-461 to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 3, and download the NE. Once the failed NE has completed the download step and other NEs have completed the Download step, proceed with the precheck step on all NEs in the first mg9kuptool window.

7 To perform a precheck of the system prior to upgrading the system, type

$ 4

Note 1: If faults appear, clear them and return to this step and re-enter the command. If necessary, repeat until no faults appear.

Note 2: If the precheck step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to "Software upgrade errors and problem resolution" in *Upgrading the MG 9000*, NN10048-461 to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 4, and precheck the NE. Once the failed NE has completed the precheck step and other NEs have completed the precheck step, proceed with the upgrade step on all NEs in the first mg9kuptool window.

The system responds with the following:

```
Enter the node number or node number list for
the precheck request:
```

Press Enter to continue.

8 To proceed with the upgrade of the system, type

$ 5

Note 1: This step is performed in the maintenance window.

Note 2: Check the upgrade time for each NE that was displayed in the prepare. If multiple NEs are being upgraded, add the upgrade times together to determine the amount of time required for the upgrade to run.

Note 3: Wait for the system to respond before proceeding. To check the status of the upgrade process, start another telnet over SSH process and perform a query using procedure Query the status of an upgrade step on page 1489.

Note 4: If the upgrade step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to "Software upgrade errors and problem resolution" in *Upgrading the MG 9000*, NN10048-461 to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 5, and upgrade the NE. Once the failed NE has completed the upgrade step and other NEs have completed the upgrade step, proceed with the postcheck step on all NEs in the first mg9kuptool window.

The system responds with the following:

```
This process will affect DSL traffic and should
be performed during a maintenance window only.

Enter the node number or node number list for
the upgrade request:
```

Press Enter to continue.

Note: If multiple NEs are being upgraded and one NE fails the upgrade process, perform a postcheck of NEs that successfully completed the upgrade before attempting to fix the NE. Proceed to the next step to perform the postcheck. If the postcheck on the successful NEs is not performed, it will not be known if all the patches were applied successfully on the NEs unless the upgrade is attempted again.

9 To perform a postcheck of the system after the upgrade of the system is complete, type

$ 6

Note: If the postcheck step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to "Software upgrade errors and problem resolution" in *Upgrading the MG 9000*, NN10048-461 to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 6, and postcheck the NE. Once the failed NE has completed the postcheck step and other NEs have completed the upgrade step, proceed with the next step.

The system responds with the following:

```
Enter the node number or node number list for
the postcheck request:
```

Press Enter to continue.

Did any NEs fail to upgrade? Fix the problem and go back to step 8.

10 This procedure is complete.

If this is a simplex (one-server) upgrade, go to step 6 on page 1450 of the MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (one-server)and continue with the upgrade process.

If this is a cluster (two-server) upgrade, go to step 6 on page 1456 of the MG 9000 SN06.2 or SN07 to SN08 upgrade checklist (two-server) and continue with the upgrade process.

Note: If the mg9kuptool has locked up, use Ctrl+C to come out of the tool lockup. If a download or upgrade step is in progress, Ctrl+C will behave the same as the Abort command used in the following procedure.

Aborting an upgrade step

At the MG 9000 Manager workstation CLI

1 Log in as root by typing

$ su - root

The system responds with the following:

```
Password:
<enter the root password>
```

2 Enter the password.

3 To start the mg9kuptool in interactive mode, type

 # /opt/nortel/mg9ksrv_08/bin/mg9kuptool.sh

The system responds with the following

```
1 configure
2 prepare
3 download
4 precheck
5 upgrade
6 postcheck
7 abort
8 query
x exit

Please select an option:
```

4 To abort an upgrade step, type

$ 7

```
Enter the node number or node number list for
the abort request:
```

Press Enter to continue.

5 This procedure is complete.

Query the status of an upgrade step

At the MG 9000 Manager workstation CLI

1 Log in as root by typing

```
$ su - root
```

The system responds with the following:

```
Password:
<enter the root password>
```

2 Enter the password.

3 To start the mg9kuptool in interactive mode, type

```
# /opt/nortel/mg9ksrv_08/bin/mg9kuptool.sh
```

The system responds with the following

```
1 configure
2 prepare
3 download
4 precheck
5 upgrade
6 postcheck
7 abort
8 query
x exit

Please select an option:
```

4 To query the status of the upgrade process, type

```
$ 8
```

```
Enter the node number or node number list for
the query request:
```

```
<the displayed default is the list of all NEs in
the plan>
```

5 This procedure is complete.

Universal Signaling Point

Before upgrading the Universal Signaling Point

Perform the required prerequisite upgrade as follows:

Network	USP applies to:	Previous Upgrade
ATM[1]	UA-AAL1	Media Gateway (MG) 9000 on page 1440
	PT-AAL2	Media Server 2000 Series on page 1413
IP	IAW, IAC, and PT-IP[2]	Media Server 2000 Series on page 1413
	UA-IP[3]	Media Gateway (MG) 9000 on page 1440
Tri-Modal	configured application	configured application

1.UA-AAL1 supports full chassis USP only.
2.Includes IP International: IAC and PT-IP
3.Includes IP International: UA-IP

After upgrading the Universal Signaling Point

Perform the next required upgrade as follows:

Network	USP applies to:	Next Upgrade
ATM	UA-AAL1 and PT-AAL2	Enhanced Network and Message Switch on page 1636
IP	IAW, IAC, UA-IP, and PT-IP[1]	Enhanced Network and Message Switch on page 1636
Tri-Modal	configured application	Enhanced Network and Message Switch on page 1636

1.Includes IP International: IAC, UA-IP, and PT-IP

About the Universal Signaling Point

The Universal Signaling Point (USP) provides a bi-directional message switching function between nodes in an SS7 network and application servers in a VoIP switch. The USP Compact functions include message routing, message discrimination, and signaling link and network management, supported by link error detection and correction. The full chassis based USP provides Signaling Gateway solutions for higher call capacity applications.

Preparing for a USP Software Upgrade

Complete the procedures in this section before you install a new GUI and begin a software upgrade.

Site configuration check

Before beginning the upgrade, determine if the site is using a route master configuration. Route master configurations will require additional test calls following the upgrade.

Verifying the site configuration

At the OAMP workstation

1 Select **Configuration>rm>system-id-mapping**.

2 Note whether entries are present in the table, which indicates the site is using a route master configuration.

Pre-upgrade check

Before beginning upgrade procedures, complete this check from the USP GUI 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.

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 and unlocked, or offline. 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**. 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.

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 "Application Server Process Paths Configuration" in document *USP Configuration Management*, NN10093-511 for more information on how to perform this procedure.

6 Delete old and unused snapshots from both RTC system nodes.

To do this, perform the following steps:

a In the File Manager panel, 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 panel.

7 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 USP8.0 on page 1493 or Create and change the alternate boot data snapshot on USP9.0 or USP10.0 on page 1495.

8 Perform test calls and verify the calls complete successfully.

9 Open the inactive RTC system node provisioning and maintenance window.

- In USP8: 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. Click the icon for the inactive RTC system node.
- In USP9: click **Configuration>platform>node**. Click **Graphical View**. Double-click on the icon for the inactive RTC system node.

10 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** and proceed to the next step.

11 Click **Load** to download the RTC system node boot image and re-initialize the RTC system node.

Note: You may see a message dialog box saying "Loss of Communication with RTC". This is normal, since the RTC is loading. If the dialog box appears, you must click **OK**.

12 When the initialization of the inactive RTC system node is complete, click **unlock** to unlock the RTC.

13 Click **SWACT** to make the inactive RTC system node Active.

14 Repeat step 9 to step 13 for the other RTC.

15 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

During the upgrade, you will be making many changes to the system. To ensure you have a backup in case a change has a performance degradation impact, you must take a snapshot when your system is operating properly. This allows you to revert the system to that snapshot. You must take a snapshot before you start the upgrade and once again after completing the upgrade.

To change the alternate boot data snapshot on a USP 8.0 system, perform the following steps:

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 and return to the Administration window.

5 Open the File Manager panel. 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.

6 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.

7 Select the active RTC system node from the **Destination** list in the right window pane.

8 Select the new data snapshot from the **Snapshot** box in the **Destination** portion of the window. Make note of the timestamp of the data snapshot.

9 Copy the snapshot to your alternate boot server by clicking **<-**. An hourglass appears while the 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.

10 When the file is transferred, click **Close.**

11 Select **Administration>ABS Settings**.

12 Select the data snapshot from the Alt. Boot Data Snapshot list. Once the snapshot is selected, the window displays the Description.

13 Click **Apply** to save the change. If you click **Close**, the window closes.

Create and change the alternate boot data snapshot on USP9.0 or USP10.0

During the upgrade, you will be making many changes to the system. To ensure you have a backup in case a change has a performance degradation impact, you must take a snapshot when your system is operating properly. This allows you to revert the system to that snapshot. You must take a snapshot before you start the upgrade and once again after completing the upgrade.

To change the alternate boot data snapshot on a USP9.0 or 10.0 system, perform the following steps:

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.

A "Confirmation required" dialog box appears, stating: "Backup create command may take up to 20 minutes, during which time

system write access will be disabled. Do you want to continue? Click **Yes** to continue.

5 When the data snapshot command is complete, close the Administration backup window by clicking the "X" in the top right corner.

6 If you selected both transfer snapshot to alt boot server and set as active snapshot on alternate boot server, go to step 14. If you only selected transfer snapshot to alt boot server, go to step 13.

7 Click **Administration>File Manager**.

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 Update the ABS Active Snapshot using the ABS Settings window:

- Open the Alternate Boot Server (ABS) Configuration Manager window by Clicking **Administration> alternate-boot-server**.
- Select the snapshot you have just created from the Snapshot name drop-down list.
- Click **Modify** to save your changes and close the window.

  A Confirmation dialog box appears, asking if you want to continue with the ABS Modify command. Click **Yes** to continue.

14 Your backup is complete.

Upgrading the USP

ATTENTION

This document details the upgrade procedures for major and point upgrades.

USP releases are designated by three numbers separated by periods, for example USP9.0.3. The first and second numbers, 9 and 0, specify the major release. The third number, 3, specifies a point release.

USP9.0.3 to USP10.0.0 is a major upgrade, whereas USP9.0.2 to 9.0.3 is a point upgrade

Examples of major releases include: USP9.0.0, USP9.1.0, USP10.0.0. The following are examples of point releases corresponding to the major releases: USP9.0.3, USP9.1.2, USP10.0.3.

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
- USP10.0.X/SN08 to USP10.0.Y/SN08 (minor release from X to Y)

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	20	20	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	2	one
two shelves	5	one
three shelves	8	two
four shelves	10	two
five shelves	12	two
eight shelves	20	four

Small systems are defined as one or two shelf systems, larger systems are defined as three or more shelves. Upgrades are performed during a maintenance window where system activity should be at its 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

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

For a list and detailed procedures of the card upgrade order for a one-and two-shelf system, see Upgrading the system nodes for one maintenance window upgrades on page 1526.

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 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 Upgrading the system nodes for multiple maintenance window upgrades on page 1526.

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

ATTENTION

USP GNPS strongly recommends that Gateway Screening not be used with USP10.0.5. In addition GNPS recommends that MSU Trace be disabled after any trace activities have been completed. This can be done by opening the configuration - gws - gws-control screen and ensuring that the:

```
criteria-name field is set to
"unassigned"

the gws-mode is set to "off"

the inbound-trace-mode is set to
"disabled"

the outbound-trace-mode is set to
"disabled"
```

This step must be performed for all linksets on the USP. Failure to do so may result in link cards not being able to successfully reload (both during an upgrade to USP10.0.5 and during regular maintenance while on USP10.0.5).

- 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 USP GUI

ATTENTION

Prior to installing the alternate boot server package, 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. Ensure that the OAMP workstation is set to either English or German language character sets.

This section describes the following software installation procedures and GUI installation procedures:

- Uninstalling the previous version of the USP GUI from Windows-based workstations
- Installing the new version of the USP GUI

Uninstalling the previous version of the USP GUI from Windows-based workstations

At the OAMP workstation

1 Close all open applications and exit the USP Distinct Servers (if running) and Signaling Server Monitor (if running).

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 Change or Remove Programs tab of the Add/Remove Programs window, select Universal Signaling Point from the alphabetical list of programs.

6 Click the **Change/Remove** button. A uninstall popup window appears prior to removing the application and its components.

7 Click **Next**. If a popup window asks if you want to remove shared files, click **Yes to All**. Click **Next** 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, 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 the GUI should be installed using the Add/Remove Programs utility in the Windows Control Panel.

ATTENTION

The following procedure requires approximately 15 minutes.

At the OAMP workstation

1 If you are upgrading from USP8.0, 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**.

Note: When adding the USP GUI on an NTST30DA workstation the GUI should be installed using the Add/Remove Programs utility in the Windows Control Panel.

7 At the Introduction 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 Upgrade the ABS software on a CS2000 Management Tools Server on page 809.
- 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, Marconi TNX-210 ATM Switch 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 1511.
you select the GUI package	step 9.
Acrobat Reader	step 12 to step d.

If:	Do:
select USP GR-310 Mediation Application	enter your Nortel Networks 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. Proceed to the next step.

If you want to install Adobe Acrobat Reader:

a Click **Next**. The Acrobat Reader License Agreement appears.

b Click **Yes** to accept the terms of the agreement. The Acrobat Reader Destination Location window appears.

c Click **Next**.

Note: Do not modify the destination path for Acrobat Reader.

d The Acrobat Reader Setup Complete window appears. Click **OK**.

13 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.

14 Log in to the USP from the new release of the USP GUI and monitor the OAMP workstation for 10 minutes while logged into

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 a 10.0 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:

Modifying the BOOTP file

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 Log in to the Alternate Boot Server Configuration Manager.

15 Under the File drop-down 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 Log out of the Alternate Boot Server Configuration Manager.

Configuring OAMP Workstations

The USP supports various workstations.

Windows 2000 workstation

Perform the following steps to replace a Windows 2000 workstation.

Replacing a Windows 2000 workstation

At the workstation site

1. Connect the new Windows 2000 workstation to the same hub to which the original Windows 2000 workstation is connected.
2. Disable the alternate boot functionality on the new Windows 2000 workstation.
3. Add the site information for your USP to the new Windows 2000 workstation.
4. Disable the alternate boot functionality on the original Windows 2000 workstation and enable it on the new Windows 2000 workstation.
5. Ensure that the new Windows 2000 workstation is functioning normally.
6. Disconnect the original Windows 2000 workstation.

   Refer to the next section, Installing and Configuring External Reachthrough Client Software, for information about setting up client software on Windows and UNIX reachthrough workstations.

Installation and configuration of the Windows client software

You must install Windows client software on each remote Windows workstation before you can use the remote reachthrough feature. For details refer to the Administrator's guide, Citrix ICA Win32 Client, Version 7.0 or Administrator's guide, Citrix ICA Win16 Client, Version 7.0.

Alternate boot server (NTST30DA)

NTST30DA servers support five terminal server licenses for remote Windows workstations and five Citrix licenses for remote Windows or UNIX workstations. Nortel Networks recommends using the terminal server licenses for remote Windows workstations, reserving the Citrix licenses for remote UNIX workstations. If you need more than five terminal server licenses for remote Windows workstations, use the Citrix licenses.

Connecting to an alternate boot server (NTST30DA)

At the OAMP workstation

1 Insert Diskette 1 from the set of Windows client software diskettes into the disk drive of your remote Windows workstation.

2 Run the setup.exe file on the diskette.

3 Follow the on-screen instructions to install the client software on your remote Windows workstation.

4 After you install the client software you will see a Citrix Program Neighborhood icon on your desktop. Double-click the icon. Select **Add ICA Connection**.

5 After you have created a connection you will see an icon for the new connection in Citrix Program Neighborhood - ICA Connections.

6 After you have finished configuring the new connection icon, double click on it to connect your remote Windows workstation to your alternate boot server and run the selected application.

Installation and configuration of external Reachthrough client software

Reachthrough support for Windows 2000

If your USP alternate boot workstation supports external reachthrough you can access the USP GUI using a remote Windows or UNIX workstation.

> ***Note:*** Each remote workstation supports up to 16 GUI sessions at once, provided each session is connected to a different site. Each USP supports up to 16 simultaneous connections in total.

You must install and configure client software on all remote workstations except for UNIX workstations that do not support the Independent Computing Architecture (ICA) protocol.

The following sections describe the procedures for installing and configuring client software on remote Windows and UNIX workstations.

Connecting to the Citrix Server

At the OAMP workstation

1 Log in as **Administrator**.

> ***Note:*** The system displays error messages as the ABS software attempts to start. Since this software is already

running errors will be generated, this will not affect the operation of the ABS server. Changing the ABS settings via reachthrough should only be done via the USP GUI and not by changing the settings directly.

Adding new Windows users for Citrix

At the OAMP workstation

1 From the Windows Start Menu, click **Start>Programs>Administrative Tools >Computer Management**.

2 Click **Local Users and Groups** on the left hand window of the Computer Management Utility. A Users folder will be displayed in the right hand window of the Computer Management Utility.

3 Right-click on the folder and select **New User**. The New user panel appears.

4 Enter **uspgui** in the User Name dialog box.

5 Enter **USP GUI Access** in the Full Name dialog box.

6 Enter a password in the Password dialog box.

7 Re-enter the password in the Confirm Password dialog box.

8 Uncheck the User must change password at next logon box.

9 Check the Password never expires box.

10 Click **Create**.

11 Create a second user for desktop access. If you require desktop access, this is the preferred method as it will prevent possible resource conflicts with the ABS server software.

- **a** Enter **desktop** in the User Name dialog box.
- **b** Enter **USP desktop Access** in the Full Name dialog box.
- **c** Enter a password in the Password dialog box.
- **d** Re-enter the password in the Confirm Password dialog box.
- **e** Uncheck the User must change password at next logon box.
- **f** Check the Password never expires box.
- **g** Click **Create**.

Publishing Citrix applications

At the OAMP workstation

1 From the Windows Start Menu, click **Start>Programs>Citrix>Citrix Management Console**.

2 Press **Ctrl-P** (Publish Application). The Application Publishing Wizard will start.

3 Enter **USP GUI** in the Display Name dialog box.

4 Enter **Nortel Networks USP GUI** in the Application Description dialog box.

5 Click **Next**. The Specify what to publish panel appears.

6 Click the **Application** radio button.

7 Click **Browse**.

8 Select your installation directory path from the file browser. The default path is **c:\ntssgusp\gui\Graphical User Interface Client.exe**.

9 Click **Next**. The Program Neighborhood Settings appears.

10 Click **Next**. The Specify Application Appearance panel appears.

11 Select **Session Windows size** of 1024x768 and **256 colors**.

12 Click **Next**. The Specify ICA Client Requirements panel appears.

13 Click **Next**. The Specify Servers panel appears.

14 Click the **Add All** button located in the middle of the screen. All Citrix Servers will be added to the right hand list.

15 Click **Next**.

16 Activate the Show Users check box on the Specify Users screen.

17 Double-click on the server name in order to display all provisioned users.

18 Find the uspgui user and click **Add**. The uspgui user is added to the list of Configured Accounts.

19 Click **Finish**.

Creating an.ica file

At the OAMP workstation

1 From the Windows Start Menu, click **Start>Programs>Citrix>Citrix Management Console**.

2 Right-click the **Applications** folder on the left window of the Citrix Management Console. A list of published applications will be displayed.

3 Right-click the **USPGUI** application.

4 Click the **ICA** button on the toolbar. The ICA File Wizard starts.

5 Select the **Minimum explanation required** radio button.

6 Click **Next**. The ICA Files Settings (1 of 2) screen appears.

7 Click **Next**. The ICA Files Settings (2 of 2) screen appears.

8 Note the ICA File Name which indicates where the file will be created. Use the browse feature if you would like to save it elsewhere.

9 Click **Next**. The Create HTML File screen appears.

10 Select the **No** radio button.

11 Click **Next**. The ICA File Summary screen appears.

12 Click **Finish**.

Windows remote workstations

Perform the following procedures for Windows remote workstations.

Windows Client software diskettes

You must have a set of Windows client software installation diskettes before you can install the client software on a remote Windows workstation. If you do not already have a set of client software diskettes you must create one.

Windows 2000 Advanced Server

You can also use this procedure to load client software on a Windows 95 (NTST30AA) workstation.

Use the Terminal Services Client Creator software on your alternate boot server to create a set of Windows client software diskettes.

Creating Windows client software diskettes

At the alternate boot server

1 Open the Terminal Services Client Creator. Open the Administrative Tools program group. Double-click the **Terminal Services Client Creator** icon.

2 Ensure that you have several blank formatted diskettes available. The 16-bit Windows client software requires four diskettes and the 32-bit client software requires two diskettes.

3 Insert a blank diskette into the disk drive of your alternate boot server.

4 Select either 16 or 32-bit Terminal Services and click **OK**. Normally, you will select 32-bit terminal services unless your remote Windows workstation is using Windows 3.1.

5 Follow the on-screen instructions until you have finished creating your set of client diskettes.

Windows 2000 Advanced Server (NTST30DA) with Metaframe

Use the ICA Client Create software on your alternate boot server to create your client software diskettes.

Using the ICA Client Create software to create your client software diskettes

At the alternate boot server

1 Open the ICA Client Creator (**Start>Programs>Metaframe Tools>ICA Client Creator**).

2 Ensure that you have several blank formatted diskettes available.

3 Insert a blank diskette into the disk drive of your alternate boot server.

4 Follow the on-screen instructions until you have finished creating the set of client diskettes.

UNIX remote workstations

If you have an NTST30DA USP alternate boot server you can access the USP GUI from a remote UNIX workstation. The following procedures describe the installation and configuration of client software on a remote UNIX workstation. This procedure applies to most common UNIX workstation configurations. For more details refer to the Citrix ICA UNIX Client Administrator's Guide, Version 3.0, which is available on the Citrix Metaframe software CD.

Installing and configuring client software on a remote UNIX workstation

At the remote UNIX workstation

1 Log in as administrator on your remote UNIX workstation and open a command window.

2 Insert the Citrix Metaframe CD-ROM disk into the UNIX workstation CD player and mount the CD-ROM using the procedure for your workstation.

3 Go to the ICA Client/Ica unix directory on the CD-ROM disk.

4 Run the setup program by entering /.setupwfc at the UNIX command line. Press **Enter**.

5 Select item 1 from the displayed menu to install the Citrix ICA client. Press **Enter**.

6 Follow the on-screen instructions to complete the installation of the ICA client.

7 After you have finished installing the ICA client you will see a Citrix ICA Client window on your desktop.

8 Add a new connection by selecting **Entry>New** from the ICA Client window. Enter a description for your connection and select the alternate boot server from the server list.

9 Select the application that you want to run when you connect to the alternate boot server by selecting Application from the list at the top left of the ICA Client window. Enter the name of the application file and the path to that file for the application that you want to run.

For example, to run the USP GUI when you connect to your alternate boot server, enter the following information: **c:\ntssgusp\gui\Graphical User Interface Client.exe**. (This is the default installation path. If you have selected another directory location, enter your installation directory path information.)

10 You can connect to the alternate boot server and run the application by double clicking on the connection name in the Citrix ICA Client window.

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 NPC, NPS, and NPE nodes on page 1531.

Upgrading NPC, NPS, and NPE system nodes is only applicable to systems that include the optional Universal Number Portability Master (UNPM) capability.

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

Running the setup

At the OAMP workstation

1 Log in 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 v10.0.0).

3 Click the **Run Setup** button. A confirmation dialog box is displayed.

4 Click **Yes**.

Note: Setup can take up to an hour to complete. A confirmation that the setup is complete will appear at the bottom left corner of the dialog box.

5 Click **Next** when the command is completed.

Precheck

Run the precheck to ensure that the upgrade is ready to proceed. The system confirms:

- 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.

2 Click **Yes** to confirm the action.

3 Click **Next** when you see the message "upgrade precheck successful" at the bottom left corner of the dialog box.

Note: If the status panel indicates that the precheck is successful, proceed to the next section. If the precheck was not successful, address any error messages and repeat the precheck before you proceed. For example, if the precheck status panel indicates that disk space is low, delete any unused snapshots and loads from the RTC SCSI disk using the File Manager.

Limit user access

Before you begin 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.

Although the following procedure is not a part of the Upgrade Wizard, it is performed at this point since you are now ready to proceed with the upgrade.

To view and/or restrict user access to the USP during a software upgrade, perform the following procedure.

Viewing and restricting user access to the USP

At the OAMP workstation

1 To modify user account information, click **Security>user-account**.

2 Click the **Search** tab.

3 Select **All** from the **Records** drop-down menu.

4 Click **Retrieve**.

5 Select all records by clicking on the first one and then hold the shift key down and click on the last record.

CAUTION

Do not include your own user account with the records you have selected. Find your own record in the list and while holding down the Ctrl key, click on your record. This will de-select your record, while keeping the others selected.

6 Click on **Post**. An "X" appears to the left of all the records.

7 You should create a record showing the currently enabled and disabled users so that you can restore them to their proper status after completion (refer to "Complete the upgrade", step 4). Do this as follows:

a Click on the **Export posted records** icon (the second button to the left of the context-sensitive Help button). A message box appears, asking: "Do you want to continue?". Answer **Yes**.

b The **Export** dialog box appears. Enter a filename and specify a file type for the exported records file. Click **Save**.

The file you have just created is a list of all user accounts. It shows which users were enabled or disabled before beginning the upgrade procedure. Use this list to restore the correct user account status after the upgrade is complete. Refer to

8 Double-click on any posted record. The Administration tab then appears.

9 Ensure the **enabled** option not selected.

10 Click **Modify**. A confirmation dialog box appears.

11 Click **Posted**. The multi-modify field selection dialog box appears.

12 Select the **enabled** option field. The letter "n" should appear to the right.

13 Click **OK**. All posted users will be disabled once the command completes.

Create a pre-upgrade data snapshot

After you have copied the upgrade files, create a new data snapshot, copy the data snapshot to the OAMP workstation, and change the alternate boot data snapshot for your site.

Note: The procedure that follows assumes the GUI was upgraded and that the upgraded GUI is the one being used.

Although the following procedure is not a part of the Upgrade Wizard, it is performed at this point since you are now ready to proceed with the upgrade.

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 do not 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 do not 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. Close the window. The data snapshot is named for the date and time of its creation.

5 If you selected both transfer snapshot to alt boot server and set as active snapshot on alternate boot server, you have completed the procedure. If you only selected transfer snapshot to alt boot server, go to step 12.

6 Open the File manager panel. 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.

7 Select the active RTC system node from the drop-down list box.

8 Open the snapshot folder.

9 Open the folder corresponding to the version of the USP software that is running on the active RTC.

10 Select the snapshot file you want to copy. When you select a file, its description is displayed in the Description box.

11 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. Close the window.

12 Open the Alternate Boot Server Configuration Manager. In the menu bar, click **Administration>alternate-boot-server**.

13 Select the snapshot from the Alternate Boot Data Snapshot List.

14 Click **Modify** and close the window.

Start the upgrade

Run the Start Upgrade procedure to begin the software upgrade. All pre-check conditions must be met before the upgrade is allowed to start. 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 abort the software upgrade, all nodes must be running the original back-level release (no nodes must have an upgrade-status of *upgraded*. If nodes are upgraded, they must be downgraded before you click the Stop Upgrade button.

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. Note that the **ss7mtp2hslink_750_xx_xx_xx_xxy** and **ss7mtp2hslink_pp5_xx_xx_xx_xxy** loads must be manually mapped.

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 software upgrade for a specific node. You can also select multiple nodes to upgrade using the Shift+Ctrl keys or Ctrl+click with a mouse.

Upgrading the system nodes for one maintenance window upgrades

Upgrade the system nodes in the following order for a one- or two- shelf system:

1. Inactive RTC in slot 15, see Upgrading the inactive RTC in slot 15 on page 1528.
2. CC in slot 1 on control CAM shelf, see Upgrading the CC node on page 1529.
3. CCs in slot 1 on extension CAM shelves, see Upgrading the CC node on page 1529.
4. Link system nodes on control and extension CAM shelves, see Upgrading a link node on page 1530.
5. If your system includes the optional Universal Number Portability Master (UNPM) capability, upgrade the NPC, NPS and NPE nodes on control and extension CAM shelves, see Upgrading NPC, NPS, and NPE nodes on page 1532.
6. CCs in slot 18 on extension CAM shelves, see Upgrading the CC node on page 1529.
7. CC in slot 18 on control CAM shelf, see Upgrading the CC node on page 1529.
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 1537.

Upgrading the system nodes for multiple maintenance window upgrades

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.

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. (See NPC, NPS, and NPE nodes on page 1531.) Re-ordering of the upgrade sequence may be required if performing a multi-node upgrade operation.

Upgrade the system nodes in the following order for a system with three or more shelves:

1. Inactive RTC in slot 15, see Upgrading the inactive RTC in slot 15 on page 1528.
2. CC in slot 1 on control CAM shelf, see Upgrading the CC node on page 1529.

3. CCs in slot 1 on extension CAM shelves, see Upgrading the CC node on page 1529.
4. Link system nodes on control CAM shelf, see Upgrading a link node on page 1530.
5. NPC, NPS and NPE nodes on control CAM shelf, see Upgrading NPC, NPS, and NPE nodes on page 1532.
6. CCs in slot 18 on control CAM shelf, see Upgrading the CC node on page 1529.

   Note: When you perform the SWACT command in step 7, you will be informed if you have not upgraded one card of each unique card type in your system. In this case, upgrade the card which will be on an extension shelf. You can perform the SWACT again until it is successful.

7.

CAUTION

Before upgrading RTC12, you should perform test calls and ensure the system is performing properly. Once RTC 12 is upgraded, the abort of the upgrade requires an out-of-service alternate boot to the snapshot taken before starting the upgrade.

SWACT and upgrade inactive RTC in slot 12, see Performing a SWACT and upgrade for the inactive RTC node in slot 12 on page 1537.

Note: The required cards have been upgraded for the first maintenance window. You can continue to upgrade cards now or in the next maintenance window.

8. Link system nodes on extension CAM shelves, see Upgrading a link node on page 1530.
9. NPC, NPS and NPE nodes on extension CAM shelves, see Upgrading NPC, NPS, and NPE nodes on page 1532.
10. CCs in slot 18 on extension CAM shelves, see Upgrading the CC node on page 1529.

Inactive RTC node in slot 15

The upgrade of the RTC in slot 15 can take up to 20 minutes to complete.

Upgrading the inactive RTC in slot 15

At the OAMP workstation

1 Select the RTC node to upgrade from the list of available nodes in the software upgrade wizard.

2 Click the **Upgrade** button. A confirmation dialog box appears. Click **Yes** to continue.

3 Wait for node upgrade to complete (the upgrade-status will change to *upgraded* on completion).

Note 1: The system raises a minor alarm, indicating a mismatch in boot images between the two RTCs.

Note 2: In the event that automatic node upgrade fails to complete successfully, then the upgrade may need to be performed manually. See Upgrading nodes manually on page 1539.

Note 3: The system raises a minor alarm, indicating an image mismatch between mate nodes.

4 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.

5 Set the alternate boot load for RTC system nodes to the new upgrade load.

Note: The alternate boot settings are used when an RTC is not able to boot from disk. After upgrading RTC15, if RTC15 were to boot, it would be able to data sync from RTC12 and upgrade. But if RTC12 were to boot, it would be booting the old release load and would not be able to data sync from RTC15, which is now running the upgrade load. So RTC12 would alternate boot. If the alternate boot load is the old release load, RTC 12 would again, not be able to data sync and become enabled. This is why the active alternate boot loads for both RTCs must be changed to the new upgrade load, thus permitting RTC12 to alternate boot the upgrade load and then data sync with RTC15 (also running the upgrade load).

Note: A special case occurs if both RTCs were to alternate boot at the same time, before you changed the active snapshot to one taken with the active RTC running the upgrade load. In this case, you will have to change the active alternate boot loads to the old release loads, since the snapshot would contain data from the old release.

a Click **Administration>alternate-boot-server**.

b Update RTC 12 to the new release version by selecting the new release from the ABS Active Loads drop-down menu.

c Update RTC 15 to the new release version by selecting the new release from the ABS Active Loads drop-down menu.

Note: When you upgrade RTC 15, you must set the alternate boot load for both RTC 12 and RTC 15. If RTC 12 reboots before being upgraded, it cannot become enabled because it is loading the old release and the upgraded RTC 15 cannot provide the old release data. To avoid this situation, set the alternate boot load for RTC 15 and RTC 12 to the new release load.

d Click **Modify**.

Note: The system raises a minor alarm, indicating a mismatch in boot images.

6 Continue to upgrade the next system node in the order appropriate to your system.

CC node

To upgrade a CC node, perform the following steps:

Note: Start with CC1 on the control shelf.

Upgrading the CC node

At the OAMP workstation

1 Select the node to upgrade in the list of available nodes in the software upgrade wizard.

2 Click the **Upgrade** button. The system asks for confirmation.

3 Wait for the node upgrade to complete (the upgrade-status 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 upgrade the next system node in the order appropriate to your system.

Link node

ATTENTION
To upgrade an NPC, NPS, or NPE node see NPC, NPS, and NPE nodes on page 1531.

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 in the software upgrade wizard.

2 Click the **Upgrade** button. The system asks for confirmation.

3 Wait for node upgrade to complete (upgrade-status 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 1531.

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 in the software upgrade wizard.

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.

4 Wait for the node upgrade to complete (upgrade-status 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 upgraded 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.

Note: Upgrading NPC, NPS, and NPE nodes is only applicable to systems that include the optional Universal Number Portability Master (UNPM) capability.

For a multiple maintenance window, the upgrade order for NPC and NPS system nodes without NP chains is listed as follows:

1. For the first maintenance window, upgrade the inactive NPC system node.
2. For the first maintenance window, upgrade one NPS system node.
3. For subsequent windows, upgrade the remaining NPS system nodes.
4. For subsequent windows, SWACT to the newly-upgraded NPC node.
5. For subsequent windows, upgrade the inactive NPC system node.

For a multiple maintenance window, the upgrade order for NPC, NPS, and NPE system nodes with NP chains is listed as follows

1. For the first maintenance window, upgrade the inactive NPC system node, the NPE nodes in that chain and any associated NPS nodes.
2. For the first maintenance window, if no NPS card has been upgraded, upgrade one NPS node and the NPE nodes in its chain.
3. For subsequent windows, upgrade the remaining NPS chains, their associated NPS nodes and the NPE nodes in those chains.
4. For subsequent windows, SWACT to the newly-upgraded NPC node.
5. For subsequent windows, 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-status 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**.

If:	Do:
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-status 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-status 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.
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.

SWACT and upgrade the Inactive RTC node in slot 12

CAUTION

After completing the following procedure, you will not be able to abort the upgrade process, except by performing an out-of-service alternate boot to the data snapshot taken before you started the upgrade procedure.

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 Double-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 12 node from the list of available nodes in the software upgrade wizard.

3 Click the **Upgrade** button.

4 Wait for the node upgrade to complete (upgrade-status will change to *upgraded* on completion).

Note 1: Once RTC12 becomes enabled, the system clears the minor alarm that indicated a mismatch between boot images between the two RTCs.

Note 2: 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.

Note: If the upgrade was successful, you can continue with the procedure Activating new features on page 1541

7 Click **Next** to continue to Activate Features.

Upgrade nodes manually

Perform the steps in the following procedure to manually upgrade any system node type including link nodes, as appropriate.

CAUTION

The following is a general description of how to upgrade a system node. However, nodes must be upgraded in a specific order. Refer to the section: Upgrading the system nodes for one maintenance window upgrades or Upgrading the system nodes for multiple maintenance window upgrades as appropriate.

Upgrading nodes manually

At the OAMP workstation

1 If you are manually upgrading a system link node and if the system link node is unlocked and enabled, proceed to step 2. Otherwise, proceed to step 3.

If you are manually upgrading a non-link node, and if the system node is unlocked and enabled proceed to step 5. Otherwise, proceed to step 4.

2 Inhibit all of the links on the system node, if applicable. See the USP Configuration Management guide for these procedures.

Note 1: You cannot inhibit IPS7 links.

Note 2: 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.

3 Deactivate all of the links or paths on the system node, as applicable to the system node. See the USP Configuration Management guide for these procedures.

4 Set the boot image of the node by completing the following steps. For link nodes, complete steps a - f. For non-link nodes, complete steps a - d and then f.

a Click **Configuration>platform>node**.

b Click **Graphical View**.

c Click the slot for the node you need to upgrade to open the node in the Administration panel.

d Select the drop-down menu to set the boot image to the new release version.

e For link nodes, you also need to set its HA boot image to the new HA release version.

Note: IPS7 and IP high-speed (HSL) link cards do not require HA loads.

f Click **Modify**.

Note: The card must be reloaded immediately after the boot image is set to the new release version.

The system raises minor alarms for each mismatch in boot images until the system node is loaded.

If the system node is off-line, the setting of the boot image reset the status to “Upgraded”. There are no alarms for an offlined node.

5 Lock and load the system node. See the USP Configuration Management guide for these procedures.

The system raises SS7 alarms when the system node is locked.

6 When the system node becomes enabled, **unlock** it.

7 Verify that the running load is the new version. If not, make sure that the correct image is selected in the platform-node Administration panel. If not, contact your next level of support.

8 For link nodes, **Activate** and **uninhibit** all of the links on the system link node.

9 Monitor the USP for 15 minutes after you upgrade the first card and each unique card type in the system (i.e. ATM, IP). Make sure the USP performs normally and does not report any LOG_SWERRs or LOG_TRAPs. During this period, perform test calls to verify that the newly loaded system node performs consistently with its pre-upgrade status. Take steps to ensure test calls are routed through links on this Link system node.

10 After the first linkset is upgraded (a linkset upgrade requires the upgrade of several link cards), perform a test call to make sure all of the link cards in the linkset have been correctly upgraded. If there are any errors, contact your next level of support. The test call for the linkset is required only for the first linkset upgraded.

11 Repeat step 1 to step 9 for the remaining system nodes on the remaining CAM shelves. Upgrade the system nodes from the lowest slot on the lowest-numbered shelf to the highest slot on the highest-numbered shelf. After you have successfully upgraded the first system node, remaining system nodes only need to be monitored for stability. A complete set of test calls will be performed when all system nodes are upgraded.

12 Perform a complete set of test calls when all system nodes are upgraded.

If it was determined prior to the upgrade, that the site is using a route master configuration, perform the following test calls:

- network to host
- network to donor
- host to donor
- migrated donor to donor

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 log out and log back in automatically to re-initialize in order to pick up the new USP10.0 features. Select Administration>software-upgrade. Click Next to go to the feature activation screen.

Activating new features

At the OAMP workstation

1 Click **Activate Features**.

2 Click **Yes** to accept the activation and continue.

3 Perform test calls to verify that messages are correctly routed.

If it was determined prior to the upgrade that the site is using a route master configuration, the following test calls must be performed:

- network to host
- network to donor
- host to donor
- migrated donor to donor

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. If there is a degradation in service, perform the procedure Deactivating new features on page 1542. If there is no degradation and you want to keep the features activated, continue to the procedure Running the cleanup on page 1542.

Deactivate upgrade features

Complete this procedure only if you want to deactivate new features from a software upgrade (for instance, in the event of a degradation in service). If features for the new release were activated, deactivate the features using the Upgrade Administration window.

Deactivating new features

At the OAMP workstation

1. Open the Upgrade Administration window. To do this, click **Administration>software-upgrade> Deactivate New Features**. A confirmation dialog box will appear.
2. Click **Yes** to deactivate or **No** to leave features active.

Cleanup

The cleanup stage, deletes some of the upgrade files that were used during the upgrade.

Running the cleanup

At the OAMP workstation

1. Before you run the cleanup, you must first re-launch the upgrade software from the Upgrade Administration window. To do this, perform the following steps:
2. Click **Administration>software-upgrade**.
3. Ensure that the new features are activated.
4. Click **Next**.
5. Click **Run Cleanup**. A confirmation dialog box appears.
6. Click **Yes**.
7. Click **Next**.

Complete the upgrade

The complete stage stops the upgrade, shuts down the wizard, creates a data snapshot, restores access privileges, and if it was determined prior to the upgrade that the site is using a route master configuration, checks the donor switch for SS7 alarms.

Stopping the upgrade

At the OAMP workstation

1. Click **Stop Upgrade**. A confirmation dialog box appears.To inform the system that the upgrade has completed successfully, click **Yes**.
2. Click the "X" at the top right corner of the wizard action panel to close the wizard.
3. Create a data snapshot, copy it to the alternate boot server and set the alternate boot server snapshot.

4 Set user privileges back to pre-upgrade settings and re-enable any user accounts that were disabled during the upgrade. Refer to the file you created in "Limit user access" section, step 7 for the correct user status. Refer to the sections Security: User accounts and Security: User session in the *USP Administration and Security* guide for additional information.

5 If it was determined prior to the upgrade that the site is using a route master configuration, check the donor switch for SS7 alarms.

Configure the Nortel Multiservice Switch port to auto-negotiate

ATTENTION

Perform this procedure if you have a Nortel Multiservice Switch 8600 in your Carrier Voice over IP Solution, and you want to enable auto-negotiation.

If you are not using auto-negotiation, skip this procedure and continue to the procedure Performing the post-upgrade checklist on page 1546.

To enable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Nortel Multiservice Switch router switch.

Note: After you execute step 1 of this procedure and you confirm that you will need to modify auto-negotiate, you will lock the IPS7 card before you make the 8600 port change. After the port change, you need to load and unlock the card. You perform these steps at the USP OAMP workstation.

Configuring the Nortel Multiservice Switch port

At the CLI for the Nortel Multiservice Switch

1 Determine the slot and port on the Nortel Multiservice Switch 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 Nortel Multiservice Switch unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.

At the OAMP workstation

2 Lock the IPS7 card connected to the 8600 port. To do this, perform the following steps:

a Click **Configuration>platform>node**.

b Click the **Graphical View** tab.

c Double-click the slot of the IPS7 card you want to lock.

d Click **Lock**. A confirmation dialog box appears.

e Click **Yes**.

At the CLI for the Nortel Multiservice Switch

3 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>
```

4 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
```

5 Commit the change:

```
> save config
```

At the OAMP workstation

6 Load the IPS7 card. To do this, perform the following steps:

- **a** Click **Configuration>platform>node**.
- **b** Click **Graphical View**.
- **c** Double-click the slot of the IPS7 card you want to load.
- **d** Click **Load**. A confirmation dialog box appears.
- **e** Click **Yes**.

7 Unlock the IPS7 card. To do this, perform the following steps:

- **a** Click **Configuration>platform>node**.
- **b** Click the **Graphical View** tab.
- **c** Double-click the slot of the IPS7 card you want to unlock.
- **d** Click **Unlock**. A confirmation dialog box appears.
- **e** Click **Yes**.

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>Log>New Period**.

2 Delete all snapshots associated with the previous USP release from both RTC system nodes.

Note: If you have changed your boot image file for a new release, Nortel Networks recommends that you delete the out-of-date image file from your system using the File Manager function.

To do this, perform the following steps:

a In the File Manager panel, 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 panel.

3 Delete old loads from the Alternate Boot Server:

a Open the ABS configuration manager application. If your ABS is on a PC, then open the configuration manager from the Windows **Start** menu. If your ABS is on the CMT, then do the following:

i 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.

ii Login to the CMT as *root.*

iii 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.

iv Enter **export DISPLAY**. To confirm the export, enter **echo $DISPLAY**.

v Enter **cd /data/usp/ntssgusp/abs**.

vi Launch the ABS Configuration Manager. Type **./ABS &**

b Click on the file, then select **uninstall release** from the drop-down menu. The uninstall existing release window appears.

c Select the load to be deleted from the drop-down 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.

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 local PC (or alternatively, a field technician's laptop) you are using 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	
List all PC usernames and passwords that will be needed DISTINCT BOOTP/FTP/NFS Server passwords ABS Configuration Manager password	
Configured Sites	

System variable	Actual value
Alternate Boot Loads RTC-12 RTC-15	
ABS Snapshot	
CS2000 Management Tools Server (new ABS)	
CMT HostName	
CMT IP Address	
Root user Root password	root (root password is set to root during factory loading of the ssPFS)
User account Password	FIELD 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 Carrier Voice over IP 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 1551
- Creating a user account for the CMT Server on page 1552
- Install/configure the ABS application using only one of the following procedures:
  - Install and configure the ABS application using Exceed on page 1553
  - Install and configure the ABS application using a console on page 1555
- Access verification and pre-migration completion on page 1556
- CMT Server migration on page 1557
- Verification procedure on page 1564
- Post migration procedures on page 1567

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 1549.)

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 Carrier Voice over IP 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 1555. 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 local 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 local 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 local 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.

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 1557.
- Set permissions on the ABS files, see Setting permissions on the ABS files (CMT) on page 1560.
- Verify the data transfer, see Verifying the data transfer on page 1561.
- Enable and configure the BOOTP server on the CMT ABS, see Enabling and configuring the BOOTP server on the CMT ABS on page 1561.
- Disable the BOOTP server on the PC ABS, see Disabling the BOOTP server on the PC ABS on page 1563.
- Verify correct settings for the USP (RTC), see Verifying correct settings for the USP (RTC) on page 1563.

Configuring the FTP and NFS servers

From the local 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 local PC. An abstemp folder will need to be created on the local PC 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 local PC 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 local 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 local 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 local 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 1552.

32 Ensure that the local PC has the abstemp directory expanded and that the CMT has the */data/usp* directory expanded.

33 Copy folders from the local 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 local PC has the abstemp/sites directory expanded. Ensure that the CMT has the /data/usp expanded.

35 Copy all files and folders from the local 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 local 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 local 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 local 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 panel 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 local 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 local PC 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.

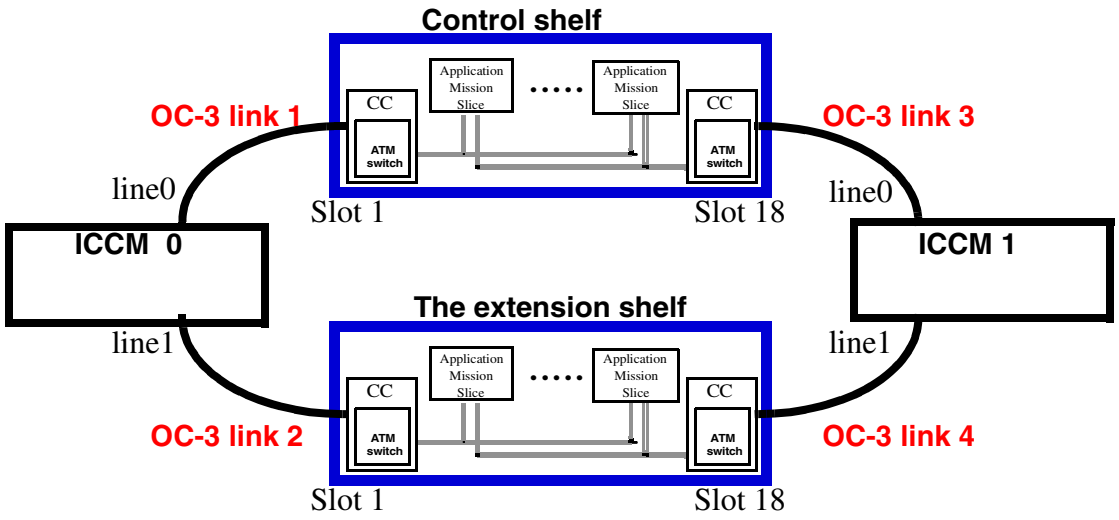
In-service introduction of ICCMs process

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 in-service 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 1497.

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 1584.

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 1584.

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 criteria 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 1584.

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 1584.

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 1584. 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 1579.

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 1580.

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 1580.

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 1581.

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 1581.

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 1576.
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 1576.
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 1577.
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 1577.
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 1578.

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.

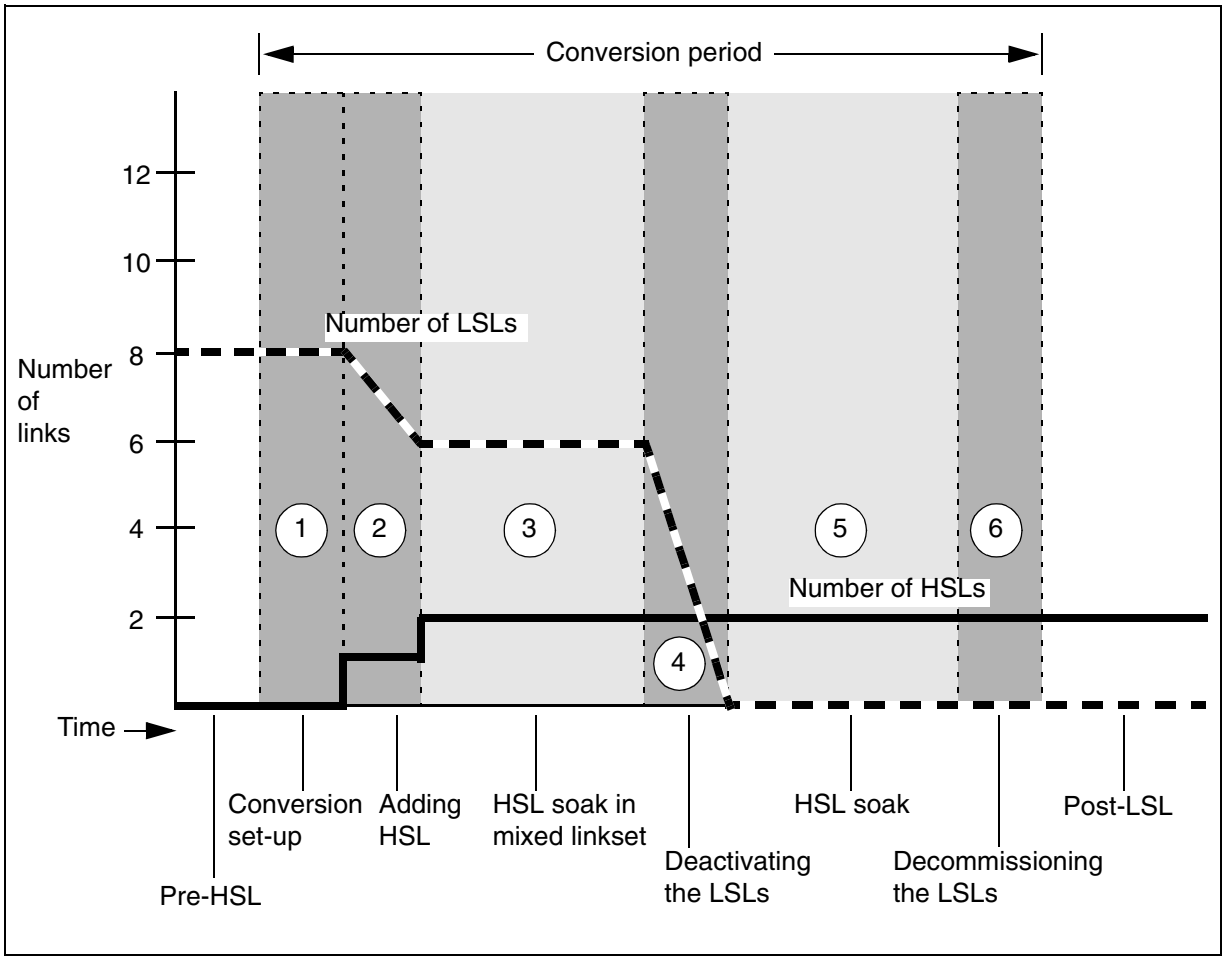
HSL cutover procedures

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 1594.

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 1594.
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 1595.

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 5.
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.

Installing Using ESD

You can use a PC or Solaris machine to install the USP software. The following procedure is required to load the installation files onto the respective platforms.

The image file must be uncompressed and available on your ESD repository server.

Setup

At least 500 MBytes must be available on the destination system to accommodate the USP install. You will have to perform the following actions to prepare for a USP software installation.

- Create a temporary directory
- Using FTP transfer the Electronic Software Delivery (ESD) software files from the drop box on the repository server.

Transfer the files

At a PC terminal

1 Make a temporary directory to store the ESD software on the PC.

```
c:/usp/loads
```

2 Change directory to the newly created directory.

3 Using binary FTP transfer the ESD software files from the drop box on the repository server.

```
$ ftp <repository_server>
```

<repository_server>
is the machine owned by the telephone operating company that was selected as the destination for the ESD software files.

4 Log in and change directory to the drop box location on the repository server.

5 Retrieve the ESD software load where the ESD filename is the USP software load

Note: Determine the actual ESD filename from the Nortel Networks notification, or by listing the contents of the drop box.

6 Repeat step 5 for all ESD software loads recorded in the notification from Nortel.

7 End the FTP session.

Start the install

Once you have retrieved the ESD software files you can begin the installation.

Installing the ESD software

At the workstation

1 Use the following table to determine your next step.

If:	Do:
You are performing a Solaris-based install	Continue to step 2.
You are performing a Windows-based install	Continue to step 8.

2 From a terminal located on the Solaris machine, create a temporary directory to store the ESD software by typing

$ mkdir /data/usp/iso_esd

3 Change directory to the newly created location by typing

$ cd /data/usp/iso_esd

4 Display the available disk space in the directory by typing

df -k

and pressing the Enter key.

Example response

```
# df -k
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2         3082223  144125 2876454    5%    /data/iso_esd
```

5 Record the amount of available disk space, which is provided in kilobytes. You will need the information later in this procedure.

Note: Recommended minimum disk space is 2.3 GBytes.

6 Transfer the ESD software load from the drop box on the repository server to the server as follows:

a Access the repository server through FTP by typing

 # ftp <repository_server>

where

<repository_server>
is the machine owned by the operating company that was selected to be the destination for ESD software.

b Log in and change directory to the drop box location on the repository server.

c Change the transfer mode to binary by typing

```
ftp> bin
```

d List the contents of the drop box by typing

```
ftp> ls
```

e Transfer the ESD software load onto the SSPFS-based server by typing

```
ftp> get <iso_image>
```

where

<iso_image>
is the CS2M ISO image filename for the software load.

f End the FTP session by typing

```
ftp> bye
```

g Uncompress the software load file.

```
# gunzip -d
CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar.gz
```

h Untar the software load file.

```
# tar -xvf
CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar
```

i Remove the .tar file by typing

```
# rm CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar
```

j Access the directory that contains the software load file by typing

```
# cd CS2M0080.80.P.NCL.NAP.VAULT.1.D
```

and list the file in the directory.

k Change the name of the file in the directory by typing

```
# mv CS2M0080_load.iso.tape
CS2M0080_load.iso
```

7 Confirm on the Solaris machine that the file was properly transferred.

8 ***for a Solaris-based install:***

Follow the instructions in the install.bin file to install.

for a PC-based install:

Execute the install.exe file to install.

Upgrading the USP Compact

ATTENTION

This document details the upgrade procedure for major and point upgrades.

USPc releases are designated by three numbers separated by periods, for example USPc9.0.3. The first and second numbers, 9 and 0, specify the major release. The third number, 3, specifies a point release.

USPc9.0.3 to USPc10.0.0 is a major upgrade, whereas USPc9.0.2 to 9.0.3 is a point upgrade

Examples of major releases include: USPc9.0.0, USPc9.1.0, USPc10.0.0. The following are examples of point releases corresponding to the major releases: USPc9.0.3, USPc9.1.2, USPc10.0.3.

ATTENTION

The USPc10.0 software upgrade supports direct in-service software upgrade from USPc9.0/SN07 to USPc10.0/SN08. USPc10 does not support a direct upgrade from USPc7.0.x. Customers with USPc7.0.x must upgrade to USPc9.0.x and then upgrade to USPc10.0. See the USPc9.0 customer documentation for the specific procedures used to upgrade to USPc9.0.

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 OAMP 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
The CLI is not available for use during an upgrade.

ATTENTION
The USP Compact must be at the latest release of USPc9.0.x before upgrading to USPc10.0. 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:

- USPc9.0/SN07 to USPc10.0/SN08

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 Networks 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
The procedures for cutover from Core Bounce to Direct Messaging are not performed during an upgrade. Contact Nortel Networks for more information.

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
- SS7 management (MSU Trace Screening)
  - — deleting MSU Trace criteria file
- IPS7 management
  - — adding, deleting, or modifying application server process (ASP)
  - — adding, deleting, or modifying application server process path (ASP Paths)
  - — adding, deleting, or modifying application server (AS)
  - — adding, deleting, or modifying application server destination (AS destination)
  - — adding, deleting, or modifying application server assignment (AS 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 OAMP 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:

- The GUI can only be used to access existing USP capabilities. You cannot access the new capabilities until the USPc is fully upgraded to USPc10.0.
- The GUI allows you to log in to a USPc9.0 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 GUI can be installed at a time because the GUI upgrade requires the conversion of local files.

Software upgrade preparation

Complete the following procedure before you install the 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. Log in to the USP.
2. Make sure that both USPc cards are in-service. Click **Configuration>platform>node**. Verify that the LED icons for each in-service system node are green.
3. Take corrective action to clear all outstanding alarms.
4. 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 steps:

   a. Click **Configuration>mtp>linkset**.

b Click the **Search** tab, select **(All)** for the Records Retrieval Criteria, and click the **Retrieve** button.

c Check the protocol-type column and ensure that none of the linksets are set to virtual.

d If any of the linksets are set up as virtual linksets, these must be removed prior to starting the upgrade.

5 Take a snapshot of the current running configuration. To do this, perform the following steps:

a Click **Administration>backup**.

b Enter a description for the data snapshot in the **Description** field. You can enter a maximum of 32 alphanumeric characters.

c If necessary, select the checkbox to activate the option to delete the oldest snapshot on rtc if maximum reached (5).

d Click **Create** to create the data snapshot.

6 Perform test calls and verify the calls complete successfully.

7 Ensure that the left USPc card (as seen on the platform node window on the GUI) is the Master. If not, perform a SWACT. Wait 10 minutes before proceeding. Monitor logs and OMs during the 10-minute period.

Upgrade the USP Compact GUI

This section contains the following GUI installation procedures:

- Uninstalling the previous version of the USPc GUI on page 1605.
- Installing the new GUI for USPc10.0 (when NOT on the CMT) on page 1606.
- Installing the new GUI for USPc10.0 (when on the CMT) on page 1608

Uninstalling the previous version of the USPc GUI

CAUTION

Before you begin this procedure, close all open applications.

At the 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 new GUI for USPc10.0 (when NOT on the CMT)

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 OAMP 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.

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 GUI is complete. Keep the USP Software CD-ROM disk handy to your system hardware.

17 Your new USPc10.0 Java GUI is now installed. You will use the GUI once you have activated new features in the procedure Activating new features on page 1619. This GUI will not work with the USP prior to the activation of new features.

Installing the new GUI for USPc10.0 (when on the CMT)

At the OAMP workstation

1 At the Laptop/PC launch the Exceed Xconfig application. The xconfig.exe application is located in the Exceed folder.

2 In the xconfig window, double click on Security.

- **a** Ensure that in the "Host Access Control List", the Disabled (any host access) radio button is selected.
- **b** Click [OK].

3 In the xconfig window, double click on Communication.

- **a** Ensure the Mode is set to Passive.
- **b** Click [OK].

4 In the xconfig window, double click on Screen Definition.

- **a** Ensure that Window Mode is set to Multiple.
- **b** Click [OK].
- **c** Exit the xconfig window.

5 Start an Exceed session. The Exceed application is located in the Exceed folder. The program will be running and minimized to the task bar.

6 At the window that is running telnet session to the CMT, set the DISPLAY back to your Laptop/PC. You should see:

>DISPLAY=<IP address of your PC>:0.0

>export DISPLAY

>echo $DISPLAY

Note: To find the IPaddress of the PC you are using, you may need to enter: ipconfig from a DOS window.

7 Insert the USP System Software CD into the CD drive on the CMT server.

8 Change directories to the CD drive on the CMT:

>cd /cdrom/cdrom0

>ls

For USP8.0 - USP8.0.6 installations, change to the following directory on the CMT:

>cd /data/usp/absCD

>chmod 755 install.bin

>ls

Ensure that you see the file install.bin

9 Launch the USP Installation CD. It may take several minutes to for the application to launch.

>./install.bin

Note: A new window will appear on you PC (from the Exceed session)

10 Click [Next] in the Introduction window.

11 Check USP Graphical Interface Client to install the USP JAVA GUI on the CMT.

12 Click [OK] in the Disk Space Warning window.

13 Click [Install] to start the Installation.

14 For SN06.2 only using the USP 8.0.x releases:

a Change the radio button to "Choose a Java VM already installed on this system".

b Select /opt/java/JDK/j2sdk1.4.1_02/jre/bin/java as the java directory.

c Click [Install].

15 Click [Done] to complete the Installation.

16 Remove the USP CD from the CD Drive using the eject cdrom command. Keep the USP Software CD-ROM disk handy to your system hardware.

17 This completes the procedure.

Verification of GUI on the CMT

From you web browser:

1 Enter the IP of the CMT and press Enter.

The Application Launch Point window should appear.

2 Click on the Application Launcher link.

The Carrier Voice over IP Login screen should appear.

3 Enter your Login Name and Password.

The Application Launch Point window should appear after a valid login.

4 Click on the Universal Signaling Point Interface Client item in the displayed list.

The Java Web Start should appear and begin launching the GUI.

5 The USP Interface Client window should appear, with either the Session-Login or Site Manager dialog box displayed in the window.

6 This completes the verification of the GUI installation.

Upgrade the USP Compact cards

This section contains the following software upgrade procedures for the USP Compact:

Transferring software to the NFS Server

At the OAMP workstation

1 Locate these files on your upgrade media (for example, Program\ntssgusp\loads):

- uspc_10_00_XX_XXX
- uspc_10_00_XX_XXX_base
- uspc_10_00_XX_XXX_t1e1ha

Note: XXX is a build version, for example,

uspc_10_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 Connect using SSH to both NFS server cards, and ensure that the samss7 user has read permission for the load files.

Transferring the upgrade package to the NFS Server

At the 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 both of the NFS server cards:

/nfsserv/usp/sd0/<data_dir>

4 Execute the following commands on both the NFS servers:

cd /nfsserv/usp/sd0/<data_dir>

gunzip upgrade_pkg.tar.gz

tar -xvpf upgrade_pkg.tar

chmod -R 777 upgrade_pkg

5 Verify the directory owner and group settings by executing the following commands:

cd / nfsserv/usp

ls -la

For the sd0 directory, the owner and group name should be samss7, as shown in the example below:

drwxrwxrwx 7 samss7 samss7 84 Dec 2 01:37 sd0

6 Log in as root and execute the following commands:

chown -R samss7 sd0

chgrp -R samss7 sd0

Running the setup

At the OAMP workstation

1 Log in 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 v10.0.0).

3 Click the **Run Setup** button. A confirmation dialog box is displayed.

4 Click **Yes**.

5 Click **Next** when the command is completed.

Precheck

Run the precheck to ensure that the upgrade is ready to proceed. The system confirms:

- Both USP Compact cards are in-service with an operational state of enabled.
- The master USP Compact card is the current active card.
- Software upgrade packages have been transferred to both the USP Compact NFS servers.

If any of the checks fail, resolve them before you proceed with the upgrade.

Running the precheck

At the OAMP workstation

1 Click the **Run Precheck** button.

2 Click **Next** when you see the message "upgrade precheck successful."

Note: If the status panel indicates that the precheck is successful, proceed to the next section. If the precheck was not successful, address any error messages and repeat the precheck before you proceed. For example, if the precheck status panel indicates that disk space is low, using the File Manager, delete any unused snapshots and loads from the RTC SCSI disk.

Limit user access

Before you begin 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.

Although the following procedure is not a part of the Upgrade Wizard, it is performed at this point since you are now ready to proceed with the upgrade.

To view and/or restrict user access to the USP during a software upgrade, perform the following procedure.

Viewing and restricting user access to the USP

At the OAMP workstation

1 To modify user account information, click **Security>user-account**.

2 Click the **Search** tab.

3 Select **All** from the **Records** drop-down menu.

4 Click **Retrieve**.

5 Select all records by clicking on the first one and then hold the shift key down and click on the last record.

CAUTION

Do not include your own user account with the records you have selected. Find your own record in the list and while holding down the Ctrl key, click on your record. This will de-select your record, while keeping the others selected.

6 Click on **Post**. An "X" appears to the left of all the records.

7 You should create a record showing the currently enabled and disabled users so that you can restore them to their proper status after completion (refer to "Complete the upgrade", step 3). Do this as follows:

a Click on the **Export posted records** icon (the second button to the left of the context-sensitive Help button). A message box appears, asking: "Do you want to continue?". Answer **Yes**.

b The **Export** dialog box appears. Enter a filename and specify a file type for the exported records file. Click **Save**.

The file you have just created is a list of all user accounts. It shows which users were enabled or disabled before beginning the upgrade procedure. Use this list to restore the correct user account status after the upgrade is complete. Refer to

8 Double-click on any posted record. The Administration tab then appears.

9 Ensure the **enabled** option not selected.

10 Click **Modify**. A confirmation dialog box appears.

11 Click **Posted**. The multi-modify field selection dialog box appears.

12 Select the **enabled** option field. The letter "n" should appear to the right.

13 Click **OK**. All posted users are now disabled.

Create a pre-upgrade data snapshot

After you have copied the upgrade files, create a new data snapshot, copy the data snapshot to the OAMP workstation, and change the data snapshot for your site.

Changing the data snapshot

At the OAMP workstation

1 Click **Administration>backup**.

2 Enter a description of the data snapshot in the **snapshot-description** field. You can enter a maximum of 32 characters.

3 If necessary, select the checkbox to activate the option to delete the 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. Close the window. The data snapshot is named for the date and time of its creation.

Start the upgrade

Run the Start Upgrade procedure to begin the software upgrade. All pre-check conditions must be met before the upgrade is allowed to start.

Running the Start Upgrade procedure

At the OAMP workstation

1 Click the **Start Upgrade** button.

2 Click **Next**.

Abort the upgrade

To abort the software upgrade, both cards must be running the original back-level release (no cards can have an upgrade state of upgraded). If cards are upgraded, they must be downgraded before you click the Stop Upgrade button. See the procedures Downgrading both USP Compact cards on page 1622 and Downgrading a single USP Compact card on page 1624.

Upgrading the slave USP Compact card

At the 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 GUI. To do this:

- **a** Click **Configuration>platform>node**
- **b** Click **Graphical view**.
- **c** Double-click on the slave USPc card to open it in the administration panel.
- **d** Click on **Lock**.

At the SAM21 Element Manager

5 Lock the slave USP Compact card. This will disable the card on the USP Compact GUI.

6 Change the load name of the slave USP Compact card to the new boot ROM load name (example: uspc_10_00_00_07b). The boot ROM load is the load that does not have a load type suffix (example: “_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. Wait until the card is rebooted before proceeding to the next step. In the SAM21 GUI, ensure the message "Card unlocked successfully" message is received. In the USP GUI, under Configuration, node, double click on the slave USPc card and ensure the activity state shows enabled. At this point you may proceed to the next step.

At the OAMP workstation

8 Unlock the USP Compact card. To do this:.

Note: The system raises logs and alarms when the loads and images on the USP Compact cards do not match.

a Click **Configuration>platform>node**

b Click **Graphical view**.

c Double-click on the slave USPc card to open it in the administration panel.

d Click on **Unlock**.

9 Verify the USP Compact 10 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, 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.

ATTENTION

Prior to upgrading the Master USP Compact card, the Slave USP Compact card should be fully enabled via the USP GUI before the Master is locked.

At the 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:

- **a** Click **Configuration>platform>node**
- **b** Click **Graphical view**.
- **c** Double-click on the slave USPc card to open it in the administration panel.
- **d** Click on **Lock**.

At the SAM21 Element Manager

6 Lock the slave USP Compact card. This will disable the card on the USP Compact GUI.

7 Change the load name of the slave USP Compact card to the new boot rom load name (example: uspc_10_00_00_07b). The

boot rom load is the load that does not have a load type suffix (example: “_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. In the SAM21 GUI, ensure the message "Card unlocked successfully" message is received. In the USP GUI, under Configuration, node, double click on the slave USPc card and ensure the activity state shows enabled. At this point you may proceed to the next step.

At the OAMP workstation

9 Unlock the USP Compact card. To do this:

Note: The system clears logs and alarms when the loads and images on the USP Compact cards match.

a Click **Configuration>platform>node**

b Click **Graphical view**.

c Double-click on the slave USPc card to open it in the administration panel.

d Click on **Unlock**.

10 Verify the USP Compact 10 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, 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.

Activate features

You must activate the new features of the software load. All cards must be upgraded to activate features.

ATTENTION

When you activate new features, all GUI connections will log out and log back in automatically to re-initialize in order to pick up the new USPc10.0 features. Select Administration>software-upgrade to continue with the feature activation.

Activating new features

At the OAMP workstation

1. Open the Upgrade Administration window. To do this, click **Administration>software-upgrade**.
2. Click **Activate Features**. A confirmation dialog box appears.
3. Click **Yes**.
4. Perform test calls to verify that messages are correctly routed. Monitor the USPc to ensure it does not report any LOG_SWERRs or LOG_TRAPs.
5. Monitor the USPc for 15 minutes. Ensure that the USPc performs without degradation. If there is a degradation in service, perform the procedure Deactivating new features on page 1619.

Deactivate features

Perform this procedure if the performance of the USPc is degraded after activating the new features.

Deactivating new features

At the OAMP workstation

1. Open the Upgrade Administration window. To do this, click **Administration>software-upgrade**.
2. Click **Deactivate New Features**. A confirmation dialog box appears.
3. Click **Yes**.

Cleanup

The cleanup stage deletes some of the upgrade files that were used during the upgrade.

Running the cleanup

At the OAMP workstation.

1 Before you run the cleanup, you must first re-launch the upgrade software from the Upgrade Administration window. To do this, perform the following steps:

   a Click **Administration>software-upgrade**.

   If you have performed the Activate features step, the Deactivate Features panel is displayed.

   b Click **Next**.

2 Click **Run Cleanup**. A confirmation dialog box appears.

3 Click **Yes**.

4 Click **Next**.

Complete the upgrade

The complete stage stops the upgrade, shuts down the wizard, creates a data snapshot, and restores access privileges.

Stopping the upgrade

At the OAMP workstation

1 Ensure all cleanup procedures have been performed.

2 Click **Stop Upgrade**. A confirmation dialog box appears.

3 Set user privileges back to pre-upgrade settings and re-enable any user accounts that were disabled during the upgrade. Refer to the file you created in "Limit user access" section, step 7 for the correct user status.

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 OAMP workstation

1 Begin a new log time period to end the upgrade log tracking time period. To do this, select **Fault > Logs** and click the **New Period** button.

2 Connect using SSH to one of the NFS servers.

3 Remove the following files corresponding to the previous software version:

- /nfsserv/usp/sd0/loads/uspc09_00_XX_XXX
- /nfsserv/usp/sd0/loads/uspc09_00_XX_XXX_base
- /nfsserv/usp/sd0/loads/uspc09_00_XX_XXX_t1e1ha

Note: XXX is a build version, for example, uspc_09_00_03_47c

4 Repeat step 3 on the other NFS server.

Downgrade the USP Compact Cards

This section contains the following software downgrade procedures for the USP Compact:

- Downgrading both USP Compact cards on page 1622.
- Downgrading a single USP Compact card on page 1624.

Downgrading both USP Compact cards

ATTENTION
Perform this procedure if both USPc cards have been upgraded and it is necessary to abort the upgrade.

CAUTION

Downgrading both USP Compact cards requires a valid USP Compact 9.0 snapshot.

CAUTION

A Complete Office Recovery is required to downgrade both USP Compact cards. This action will cause an interruption in service.

At the 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 9.0 snapshot the active snapshot for both cards. To do this, perform the following steps:

   a Select **Configuration>platform>node**.

   b Double-click on the left card and select the snapshot from the drop-down list beside the boot-snapshot field.

   c Click **Modify** to save the changes.

   d Repeat this procedure for the right card.

   e Log out of the USP Compact 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 9.0 boot ROM load name (example: uspc_09_00_03_47c). The boot ROM load is the load that does not have a load type suffix (example: “_base” or “_t1e1ha”). It is located in the following directory:

/nfsserv/usp/sd0/loads/

6 Unlock the left (as seen on the USP GUI System Configuration screen) USP Compact card.

At the OAMP workstation

7 Log in with the USP GUI.

8 Verify that the USP Compact is running the correct snapshot and load. To see the snapshot information:

a Click **Configuration>platform>node**

b Click **Graphical view**.

c Double-click on the USPc card to open it in the administration panel.

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 10.0 version of the USP GUI.

11 Install the USP Compact 9.0 version of the USP GUI.

Downgrading a single USP Compact card

> **ATTENTION**
> Perform this procedure only if one blade is at an older release. To downgrade both blades at the same time, perform the procedure Downgrading both USP Compact cards.

At the OAMP workstation

1 Ensure that the upgraded card is the slave. Perform a SWACT if it is not. This can be checked by doing the following:

   a Click **Configuration>platform>node**

   b Click **Graphical view**.

   c Double-click on the USPc card to open it in the administration panel.

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 5 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:

   a Click **Configuration>platform>node**

   b Click **Graphical view**.

   c Double-click on the slave USPc card to open it in the administration panel.

   d Click on **Lock**.

At the SAM21 Element Manager

7 Lock the slave card. This will disable the card on the USP GUI.

8 Change the load name of the slave card to the USP Compact 9.0 boot ROM load name (example: uspc_09_00_03_47c). The boot ROM load is the load that does not have a load type suffix (example: “_base” or “_t1e1ha”). It is located in the following directory:

/nfsserv/usp/sd0/loads/

9 Unlock the slave card.

At the 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, contact Nortel Networks technical support.

Note: The system clears logs and alarms when the loads and images on the USP Compact cards match.

11 Stop the upgrade by doing the following:.

a Click **Administration>software-upgrade**.

b Click **Next** until the Stop Upgrade button is displayed.

c Click **Stop Upgrade**.

12 Unlock the slave card. To do this:

a Click **Configuration>platform>node**

b Click **Graphical view**.

c Double-click on the slave USPc card to open it in the administration panel.

d Click on **Unlock**.

13 Activate all of the paths on the slave USP Compact card.

14 Activate all of the links on the slave USP Compact card.

15 Uninhibit any links you inhibited.

16 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.

17 Uninstall the USP Compact 10.0 version of the USP GUI.

18 Install the USP Compact 9.0 version of the USP GUI.

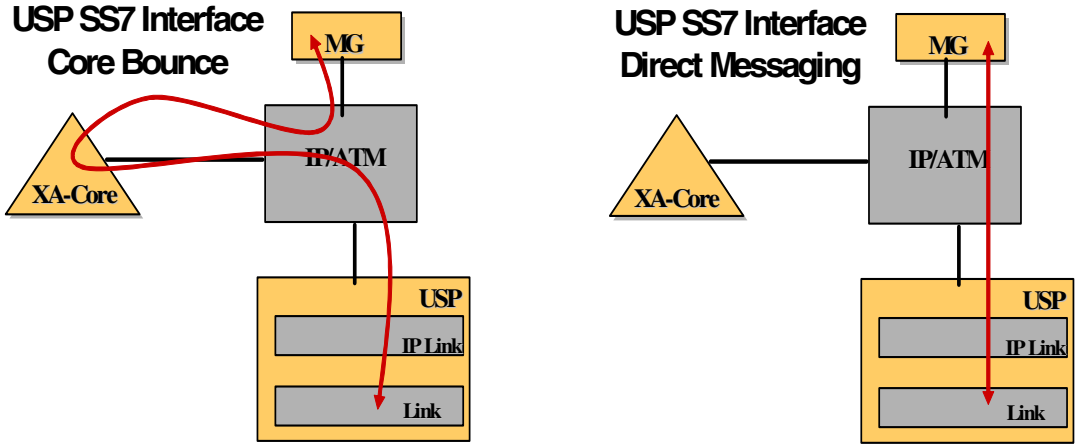
USP core bounce to direct messaging cutover

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 1630 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 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.

Enhanced Network and Message Switch

Before upgrading the Enhanced Network and Message Switch

Perform the required prerequisite upgrade as follows:

Network	Enhanced Network and MS applies to:	Previous Upgrade
ATM	UA-AAL1 and PT-AAL2	Universal Signaling Point on page 1490
	PT-AAL1	Peripheral Modules on page 1065
IP	UA-IP, PT-IP, IAC, , PT-AAL2, CHS-North America, and IAW[1]	Universal Signaling Point on page 1490
	CHS-International	Gateway Controller on page 1330
Tri-Modal	configured application	one of above based on configuration

1.Includes IP International IAC, IAW, PT-IP, and UA-IP

After upgrading the Enhanced Network and Message Switch

Perform the next required upgrade as follows:

Network	Enhanced Network and MS applies to:	Next Upgrade
ATM	PT-AAL1 and UA-AAL1	XA-Core - CS 2000 on page 1638
	PT-AAL2	Depending on configuration: XA-Core - CS 2000 on page 1638 Call Agent - CS 2000 Compact on page 1639
IP	CHS,UA-IP, PT-IP, IAC, and IAW[1]	Depending on configuration: XA-Core - CS 2000 on page 1638 Call Agent - CS 2000 Compact on page 1639
Tri-Modal	configured application	XA-Core - CS 2000 on page 1638

1.Includes IP International: CHS, IAC, PT-IP, and UA-IP

About 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 Helmsman collection.

XA-Core - CS 2000

Before upgrading the XA-Core - CS 2000

Perform the required prerequisite upgrade as follows:

Network	XA-Core applies to:	Previous Upgrade
ATM	PT-AAL2, PT-AAL1 and UA-AAL1	Enhanced Network and Message Switch on page 1636
IP[1]	UA-IP, PT-IP, IAC, IAW, and CHS [2]	Enhanced Network and Message Switch on page 1636
Tri-Modal	configured application	Enhanced Network and Message Switch on page 1636

1.Includes IP International: CHS, IAC, IAW and UA-IP.
2.UA-IP, PT-IP, and IAC applications support either Call Agent or XA-Core.

After upgrading the XA-Core - CS 2000

Perform the next required upgrade as follows:

Network	XA-Core applies to:	Next Upgrade
ATM	PT-AAL1 and UA-AAL1	upgrades are complete
	PT-AAL2	Media Gateway 7400/15000/20000 on page 1769
IP	UA-IP, PT-IP, IAC, IAW, and CHS[1]	Media Gateway 7400/15000/20000 on page 1769
Tri-Modal	configured application	Media Gateway 7400/15000/20000 on page 1769

1.Includes IP International: CHS, IAC, IAW and UA-IP

About the XA-Core - CS 2000

The extended architecture core (XA-Core) is the call processing component of the Communication Server 2000 (CS 2000) that controls signaling gateway and media gateway functionality. Refer to the following documentation regarding XA-Core upgrades:

- *XA-Core Maintenance Manual*, 297-8991-510
- *One Night Process Software Delivery Procedures*, 297-8991-303

Call Agent - CS 2000 Compact

Before upgrading the Call Agent - CS 2000 Compact

Perform the required prerequisite upgrade as follows:

Network	Call Agent applies to:	Previous Upgrade
ATM	PT-AAL1 and UA-AAL1	not applicable
	PT-AAL2	Enhanced Network and Message Switch on page 1636
IP	CHS, UA-IP, PT-IP, IAW, and IAC[1]	Enhanced Network and Message Switch on page 1636
Tri-Modal	not applicable[2]	not applicable

1.Includes IP International: CHS, IAC, PT-IP, and UA-IP.
2.Tri-Modal applications support XA-Core only.

After upgrading the Call Agent - CS 2000 Compact

Perform the next required upgrade as follows:

Network	Call Agent applies to:	Next Upgrade
ATM	PT-AAL1 and UA-AAL1	not applicable
	PT-AAL2	Media Gateway 7400/15000/20000 on page 1769
IP	UA-IP, PT-IP, IAW, and IAC[1]	Media Gateway 7400/15000/20000 on page 1769
Tri-Modal	not applicable	not applicable

1.Includes IP International: CHS, IAC, PT-IP, and UA-IP.

About the Call Agent - CS 2000 Compact

The Call Agent is the key Call Processing component in the Communication Server 2000 - Compact (CS 2000 - Compact). The Call Agent hardware is a Single Board Computer (SBC) based on commercially available Compact PCI (cPCI) technology that resides in a Services Application Module 21 (SAM21) shelf. Two Call Agent cards and two SAM21 shelves are required for redundancy. Each Call Agent card resides in its own SAM21 shelf.

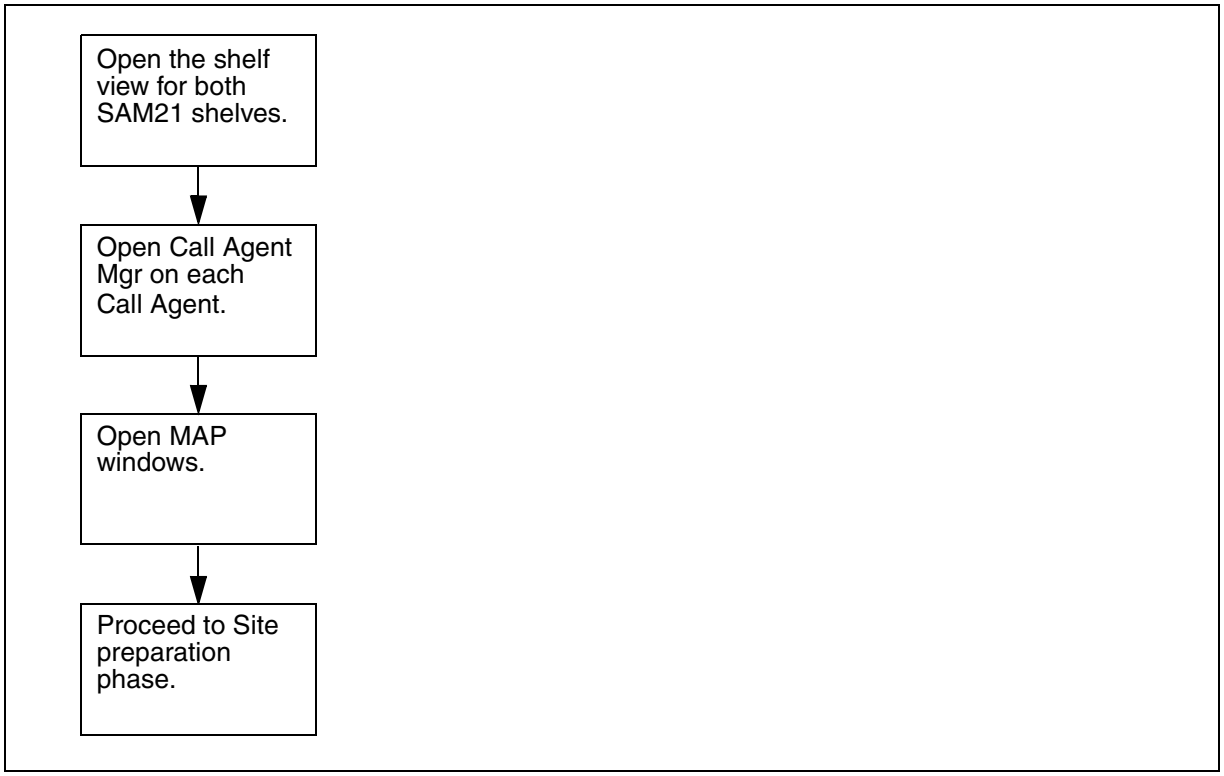
Interface setup

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.

Interface setup

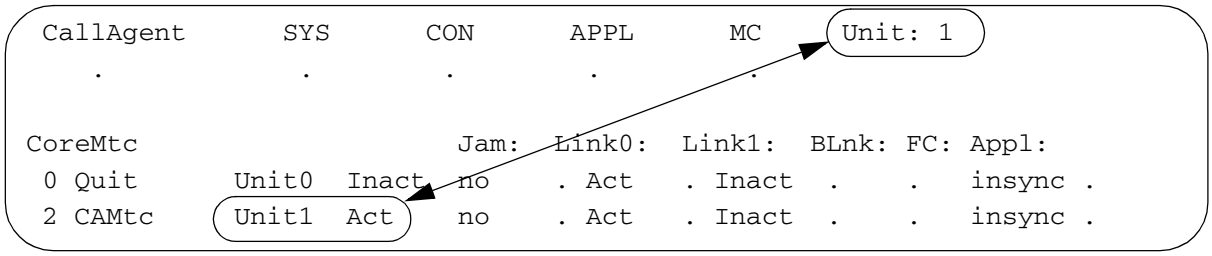


Each procedure indicates the interface used to perform the procedure or step. The following table describes the interfaces.

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.
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.
Active maintenance window (CORE0 or CORE1)	the active maintenance window (CORE0 or CORE1) that is connected to the active Call Agent. The example in figure SN06 and newer Call Agent Manager with Message Controllers in the office: Example on page 1642 shows CORE1 as the active maintenance window.
SDM	a window connected to the CS 2000 Core Manager. The **sdmmtc** program and UNIX system activities are completed from this window. SDM is relevant only where it is present.
CBM	TBD
CMT	TBD

SN06 and newer Call Agent Manager with Message Controllers in the office: Example



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

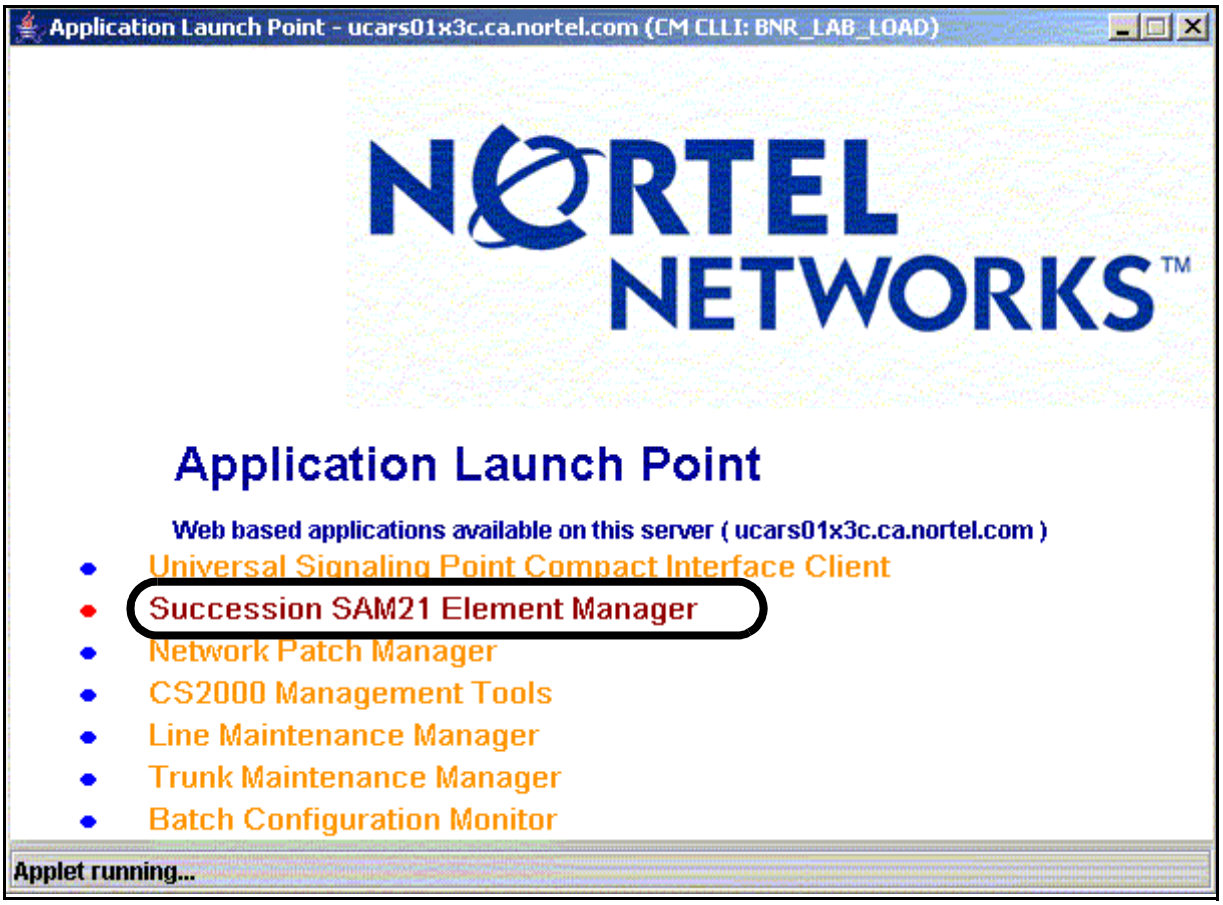
4 This procedure is complete.

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 Identify and open the Shelf View window for shelves that contain call agent cards by double-clicking on the shelf icons from the Subnet View window. (Additional shelves may not contain call agent cards.)

4 Position the screens so that alarms and access to locking and unlocking cards are available.

5 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 preparation phase

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

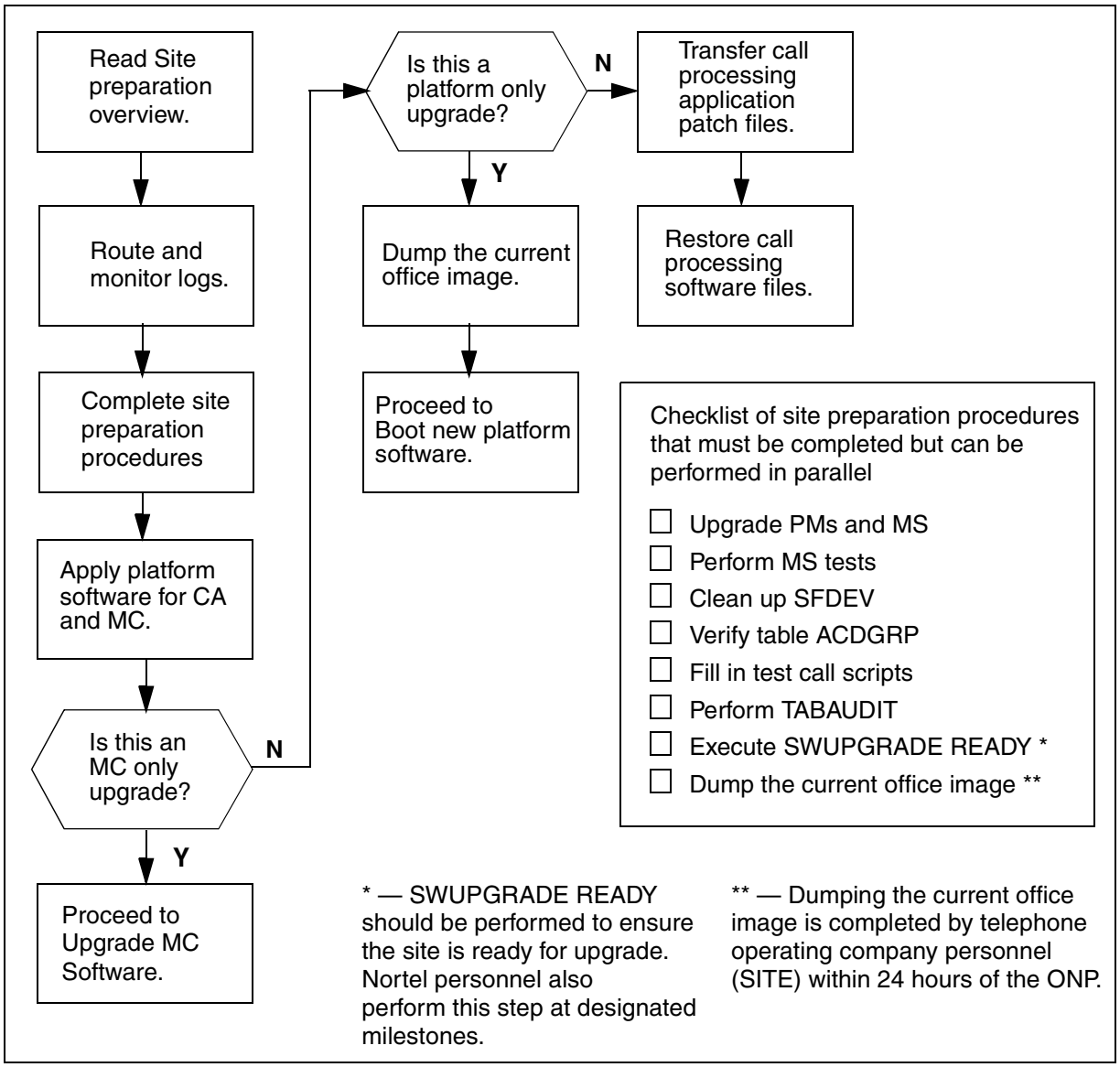


Table , Process timeline indicates the timing of events that need to be completed by telephone operating company personnel for an ONP. This timeline does not apply to platform only MR upgrades or Message Controller only upgrades.

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 • site begins checking logs daily, refer to Monitor logs on page 76. Check logs for CCA, SAM21 EM and Ethernet Routing Switch 8600 to be sure links are stable. ***Note:*** Continue monitoring logs until the day of SWACT. • begin upgrading and verifying PMs and other network components with the latest software loads, refer to "Upgrade Peripheral Modules and Message Switch" in *Upgrading the Call Agent*, NN10065-461
30 days	Begin data consistency checks, refer to Perform TABAUDIT on page 1678
15 days	Ensure that scheduled RExTsts complete successfully
7-4 days	• ensure SFDEV is clear, refer to Clean up SFDEV on page 1672 • continue to monitor logs for CCA, SAM21 EM and Ethernet Routing Switch 8600 *until the day of SWACT*. *Continue to check the logs to be sure links are stable*. • if office is equipped with PMs, ensure that the latest PM loads and XPM patch files are restored to the proper disk volumes • site receives final shipment of software media and documentation

Process timeline

Days before the upgrade	Site preparation activity
6 days	• verify all network nodes are loaded, patched, and working • verify dial in connectivity, refer to Remote site access on page 1704 • ensure all software media are on site • verify that site personnel are familiar with the upgrade process
5 days	The final site readiness check is performed by Nortel personnel. Nortel Software Delivery Engineer dials in an runs Execute SWUPGRADE READY on page 1683.
3-2 days	• verify site personnel has prepared test calls plan • obtain name of site personnel representative with the authority to decide in case of an abort with the CANCEL command • verify patches for the new software load are downloaded to the site • ensure all site preparation checklist items are complete • continue monitoring logs for CCA, SAM21 EM and Ethernet Routing Switch 8600 *until the day of SWACT*. *Continue to check the logs to be sure links are stable.*
Day of upgrade	Refer to Site responsibilities the day of the software delivery on page 1699.
Night of upgrade	Refer to SWUPGRADE on page 1707.

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_7.x.y.z`, and the Message Controller software, `ncgl_mc_image_7.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 1658.

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 2005
                CDROM is mounted.
                Listing file names in the rpm on the cd.

/swd/3pc/ncgl_cca_7.32.1.0
/swd/3pc/ncgl_mc_7.32.1.0

                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-7.32-1.0.noarch.rpm
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2005
ncgl_cca_mc_image-7.32-1.0.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-7.32-1.0
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2005
ncgl_cca_mc_image-7.32-1.0.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 2005
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 1653 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 1690
otherwise	Transfer call processing application patch files on page 1667

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 Installation Services engineer, or documentation provided by Nortel 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 configuration on CS 2000 Core Manager

The following figure shows the upgrade configuration on the CS 2000 Core Manager for passthru accounts. Please read Important password information.

Upgrade 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.

Important password information

For new installations, new PassThru accounts are created without passwords. 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 to a customer dropbox. An example of the PCL is CSNN07BG, and an example of the NCL is ncgl_cca_image_7.33.1.0.

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. When the agreement was established, the operating company furnished Nortel with the location of an electronic dropbox and a username and password pair for delivering software loads. When Nortel 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 8 and is part of the product order code

vault
is a string that identifies the Nortel 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 Display the available disk space in the directory by typing

```
# df -k
```

and pressing the Enter key.

Example response

```
# df -k
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2         3082223  144125 2876454    5%    /data/iso_esd
```

4 Record the amount of available disk space, which is provided in kilobytes. You will need the information later in this procedure.

Note: Recommended minimum disk space is 2.3 GBytes.

5 Transfer the ESD software load from the drop box on the repository server to the server as follows:

a Access the repository server through FTP by typing

```
# ftp <repository_server>
```

where

<repository_server>
is the machine owned by the operating company that was selected to be the destination for ESD software.

b Log in and change directory to the drop box location on the repository server.

c Change the transfer mode to binary by typing

```
ftp> bin
```

d List the contents of the drop box by typing

```
ftp> ls
```

e Transfer the ESD software load onto the SSPFS-based server by typing

```
ftp> get <iso_image>
```

where

<iso_image>
is the CS2M ISO image filename for the software load.

f End the FTP session by typing

```
ftp> bye
```

g Uncompress the software load file.

```
# gunzip -d
CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar.gz
```

h Untar the software load file.

```
# tar -xvf
CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar
```

i Remove the .tar file by typing

```
# rm CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar
```

j Access the directory that contains the software load file by typing

```
# cd CS2M0080.80.P.NCL.NAP.VAULT.1.D
```

and list the file in the directory.

k Change the name of the file in the directory by typing

```
# mv CS2M0080_load.iso.tape
CS2M0080_load.iso
```

6 The remainder of this procedure depends on the ESD file:

If the ESD file is a	Do
PCL	step 7
NCL	step 8

7 This step applies to PCL ESD software loads only.

a Record the location of the call processing application files, /data/iso_esd/<esd_filename>, such as /data/iso_esd/SNC00008.8.R.PCL.PPC3.SDC.2.D.

b Go to procedure Restore call processing application files on page 1669 and specify this location for the call processing application files instead of /cdrom/cdrom0 in step 5. This procedure is complete.

8 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.

9 Mount the ISO image 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)
```

```
X - exit


select -
```

c Enter the number next to the "mount_image" option in the menu.

If the response is	Do
Enter the full path of the ISO image	substep e
ISO Image Already Mounted	substep d

d Enter the number next to the "mount_image" option in the menu and retry substep c.

Note: If the umount_image or mount_image command is unsuccessful a second time, contact your next level of support.

e When prompted, enter the full path name of the ISO image on the server from the root.

The contents of the ESD software file are placed in directory /tmpmnt

Note: Do not attempt to access the /tmpmnt directory until the mount command is complete.

If the response is	Do
It 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.	step f
Provided full path to ISO image does not exist	Verify the location and name of the ISO 9660 image.
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 your next level of support.

If the response is	Do
ERROR MOUNTING <ESD_filename>	This response indicates that either the ISO 9660 file is corrupt, or the /tmpmnt directory has been deleted. Repeat this procedure, and if it fails a second time, contact your next level of support.

f Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

`select - x`

and pressing the Enter key.

10 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.

11 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 10 except specify the location of the software instead of /tmpmnt.

12 Unmount the ISO image 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)


 X - exit


select -
```

c Enter the number next to the "umount_image" option in the menu.

d Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

`select - x`

and pressing the Enter key.

13 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 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
MUC00021810335_MS.img1020
SNC00008810335_CM.img1020
ftp> bin
200 Type set to I.
ftp> prompt
Interactive mode off.
ftp> mget *
local: SNC00008810335_CM.img1020 remote: SNC00008810335_CM.img1020
200 PORT command successful.
150 Opening data connection for SNC00008810335_CM.img1020 (binary mode)
226 Transfer complete.
150 Opening data connection for MUC00021810335_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>
> QUIT
```

Example of IMPORTing image files

```
DISKUT:
>IMPORT SD00IMAGE1

Attempting to import 2 files selected on SD00IMAGE1.

Imported MUC00021810335_MS.img1020 as MUC00021810335_MS  IMAGE 1020.
Imported SNC00008810335_CM.img1020 as SNC00008810335_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 SNC00008547159_CM 15

```
> QUIT
```

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.

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 If required, access the disk administration level to create a disk volume in which to copy the files from SFDEV:

```
> diskadm <disk_prefix>
```

disk_prefix
is the disk on which you want to create the volume, either sd00 or sd01

3 Create the storage volume:

```
> cv <vol_name> <size>
```

vol name
is the name you want to give the new volume, for example SD00TEMP

size
is the size required for the new volume, for example 128 for 128 Megabytes

4 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

5 Erase files that are not essential from SFDEV:

```
> ERASESF <file_name>
```

6 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:2005/06/20 09:30:00 THU; STOP: 2005/06/20 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 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 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: • EAS outgoing (one route) • ‘0’ plus ‘0’ minus • CAMA ANI • 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 Global Software Delivery recommends scheduling automatic TABAUDITs (AUTOTABAUDIT), rather than manual TABAUDITs.

Nortel recommends using TABAUDIT as part of normal maintenance practices for regular ongoing table data integrity checks. This can be done by using the automatic scheduling function. For assistance with TABAUDIT, contact your Nortel regional customer representative.

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 options include SINGLE, DAILY, WEEKLY and MONTHLY sessions. A timeframe cannot be less than 30 minutes or more than six hours. For the MONTHLY option, the 31st day of the month cannot be used. Up to eight sessions can be set up. Timeframe definitions must not overlap.

Scheduling a minimum of 3 hours to complete the AUTOTABAUDIT is recommended. The time can be spread over more than one session, if required.

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  |
-------------------------------------------------------------------------
|                                                                       |
|2005/06/24 2005/06/24    18:30      20:00   | SINGLE      |  REGULAR   |
|                                                                       |
-------------------------------------------------------------------------
Current time      : 2005/06/24 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 Execute the scheduled AUTOTABAUDIT session

> EXECUTE

The system displays a STATUS. If the status is correct, enter **YES** at the prompt.

Note: The scheduler starts AUTOTABAUDIT at the specified start time(s), and stops testing at the specified stop time(s). Only the included tables are tested in the order they are listed in table DART.

8 Check the status of AUTOTABAUDIT after the scheduled stop time. Enter:

> STATUS

Determine if AUTOTABAUDIT has completed verifying all tables.

If AUTOTABAUDIT	Do
has completed verifying all tables	step 9
has not completed verifying all tables (process failed, insufficient time, or other reasons)	determine what steps are necessary to complete the process. It may be necessary either to repeat steps 1 through 3, or to schedule multiple sessions to verify all tables in the office.

9 After AUTOTABAUDIT completes, obtain an error report. Enter:

```
> REPORT ERRORS
```

If	Do
no errors are reported	step 11
errors are reported	Correct the errors using the table editor and repeat from step 4. Refer to the Additional information.

10 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.

11 Quit to the CI level:

```
> QUIT ALL
```

12 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 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

```
> 21
```

Note: CSP 21 is equivalent to the SN08 release.

e Set the PM_VERIFY_FILE variable, and 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 default 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                         =    21
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 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 1699.

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 2005
9.11% done, estimate finish Tue Feb 10 14:52:00 2005
13.67% done, estimate finish Tue Feb 10 14:52:00 2005
...
95.67% done, estimate finish Tue Feb 10 14:52:05 2005
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.

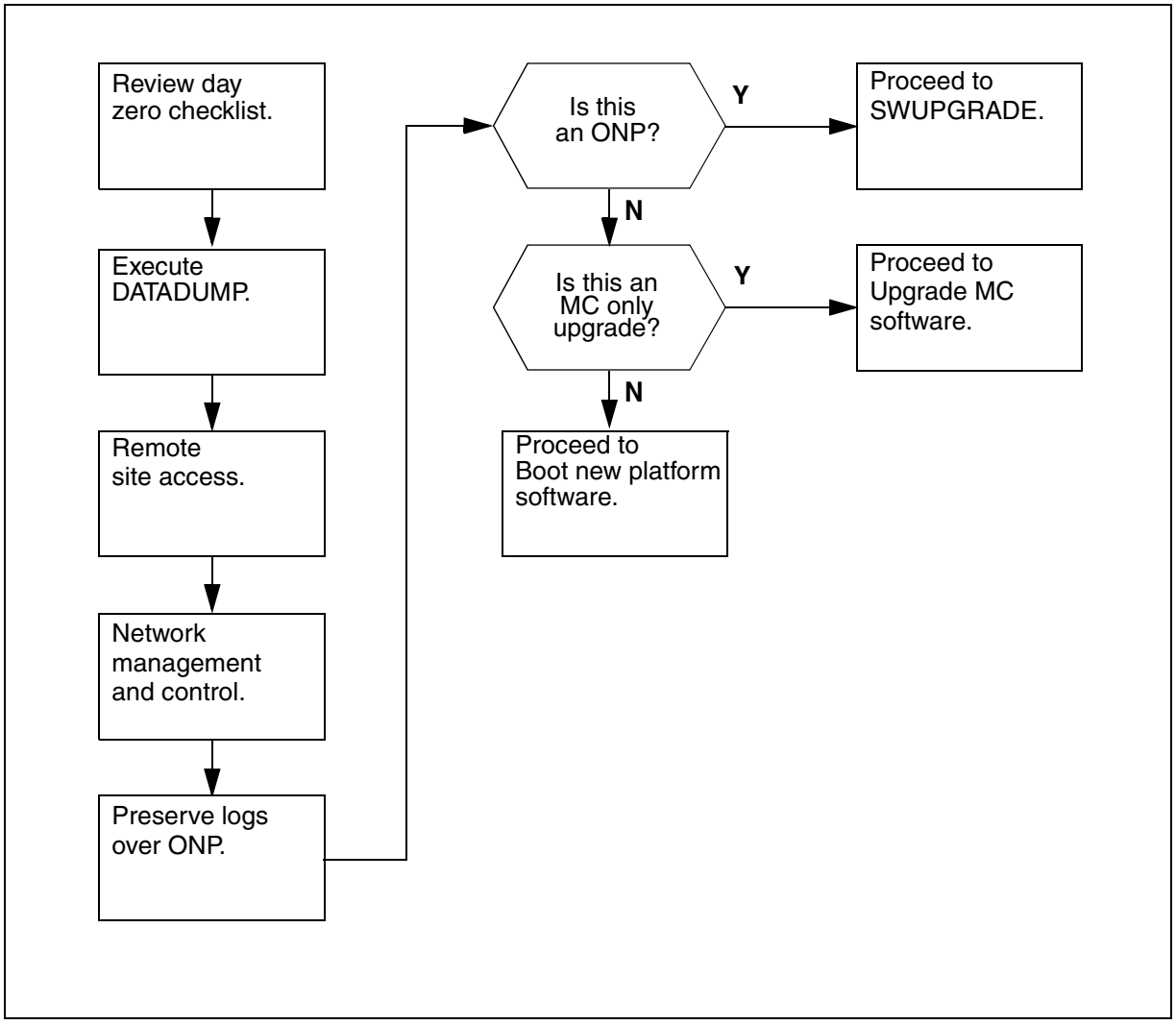
19 Store the DVD-RW per office procedure.

20 This procedure is complete.

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 74, Perform TABAUDIT on page 1678, and Restore call processing application files on page 1669.

2 Verify the ONP start time. Either Nortel 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 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 1690. 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, 2005  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 Applicator. If not provided to Nortel 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 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 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 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 remote access can cause problems during the software upgrade.

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

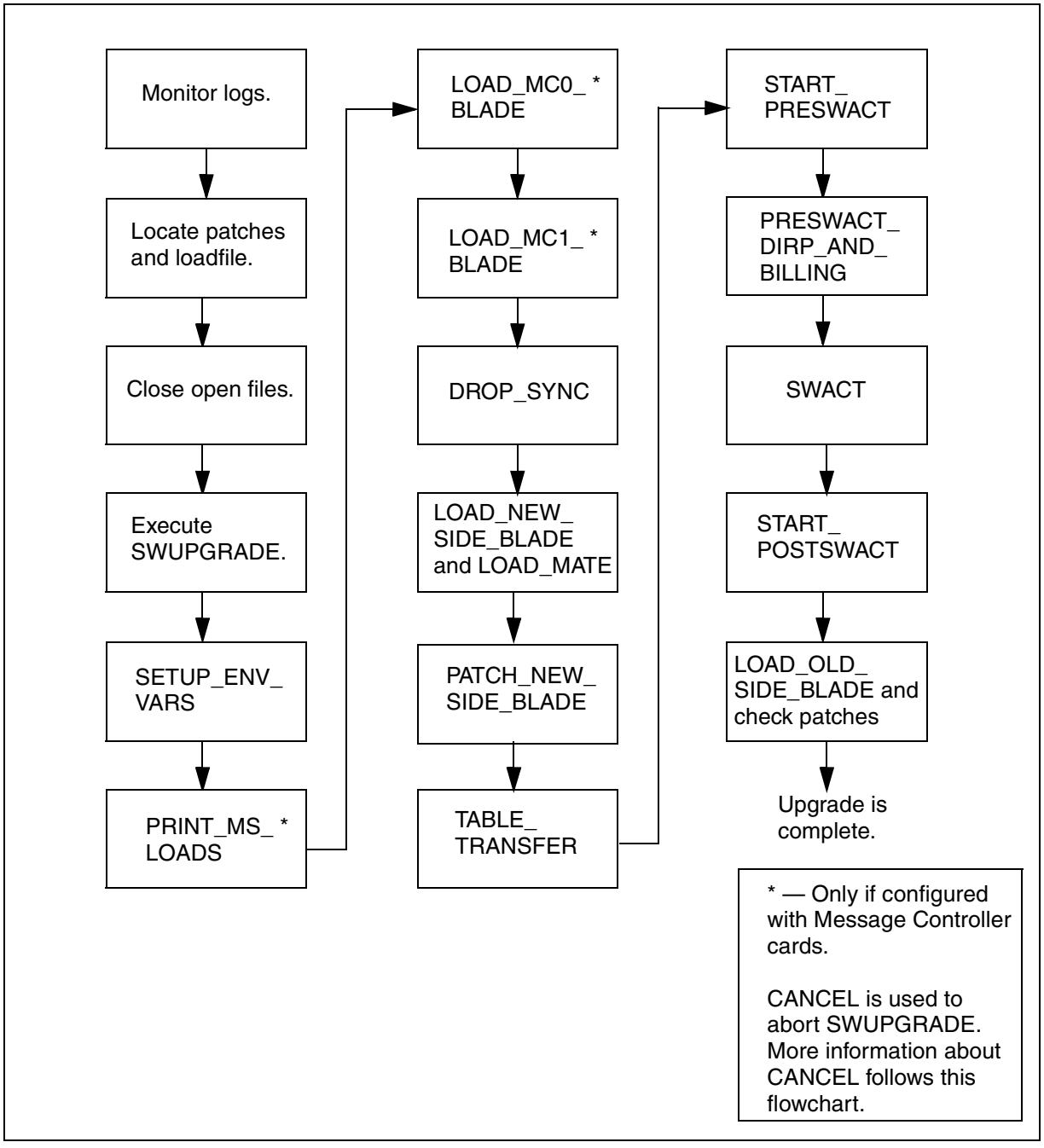
4 Repeat step 3 for each required change and then exit the LOGUTIL level:

```
> 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 Interface setup on page 1640, Site preparation phase on page 1647, and Site responsibilities the day of the software delivery on page 1699.

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 1650.

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 1669.

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" in *Upgrading the Call Agent*, NN10065-461.

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 56 CE built on 2005-APR-12 at 19:26:00
using mux21ce
LOAD: NIL.000
LAYER: BAS.22.0.CE
LAYER: TL.21.0.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 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 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 the user name logged in for TRACE_DEVICE:

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> where user_name is the username of the trace user

Note: For clarity, it is recommended that you set this variable to the user logged in to the TRACE_DEVICE.

The USER must be LOGGED IN when this variable is set. The current setting is: <none>

2 It is recommended that you 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, 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 SN000008 17/MAR/2005 ***

6 Enter the LDMATE_IMAGE variable:

LDMATE_IMAGE
Holds the volume name and filename used to load the inactive unit.

Example
SD00IMAGE0 CSN0008BG

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 CSN0008BG
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-U22BC
Load in MS 1 = MS-U22BC

Please check the above MS loads for correctness.
Step PRINT_MS_LOADS is complete.

The SWUPGRADE process has paused. Enter GO.
```

Note: MS-U22xx is the correct value for upgrading to SN08.

2 If the value reported is not correct, do not proceed. Contact Nortel 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.

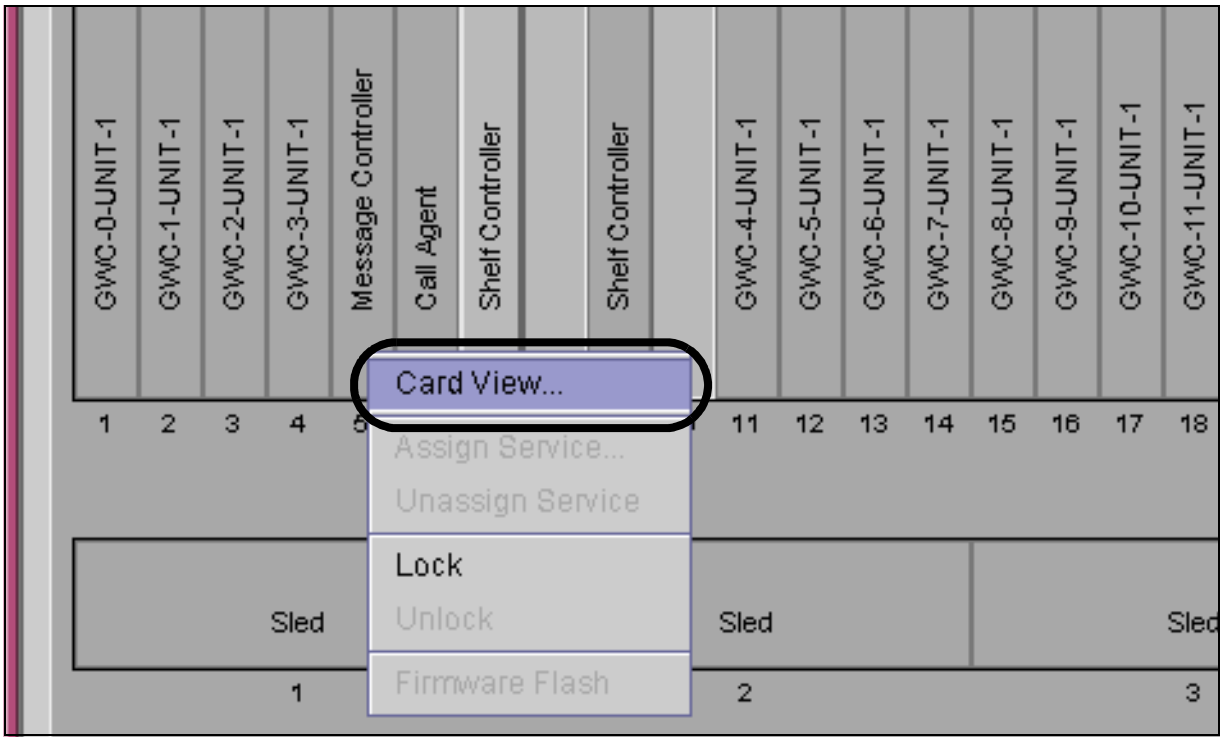
```
10.40.54.60 mc0
```

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.



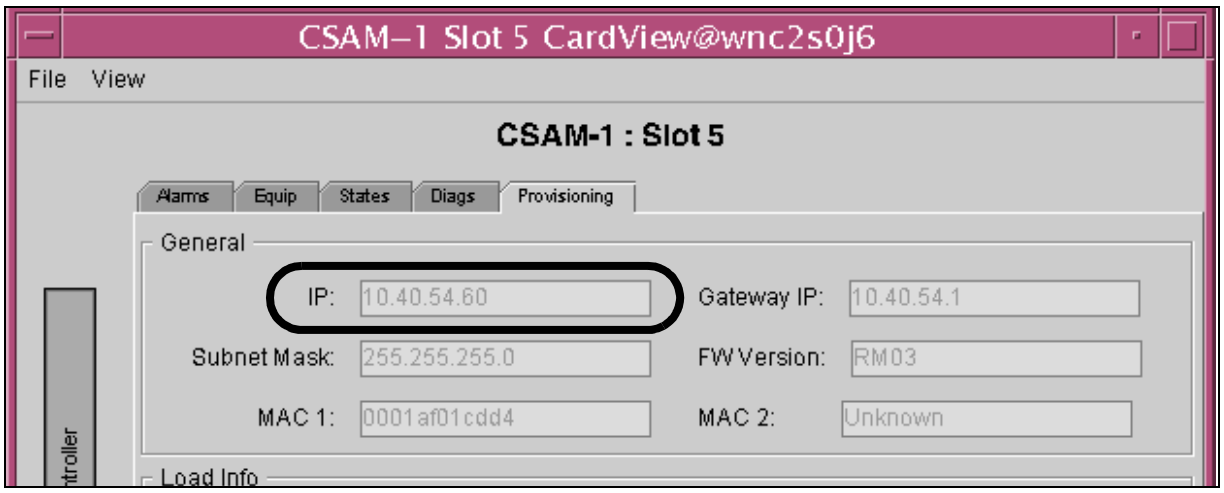
Note: The Shelf View window will reflect office provisioning and the hardware configuration of the SAM21 shelf.

The Card View window opens.

8 Select the Provisioning tab on the Card View window.

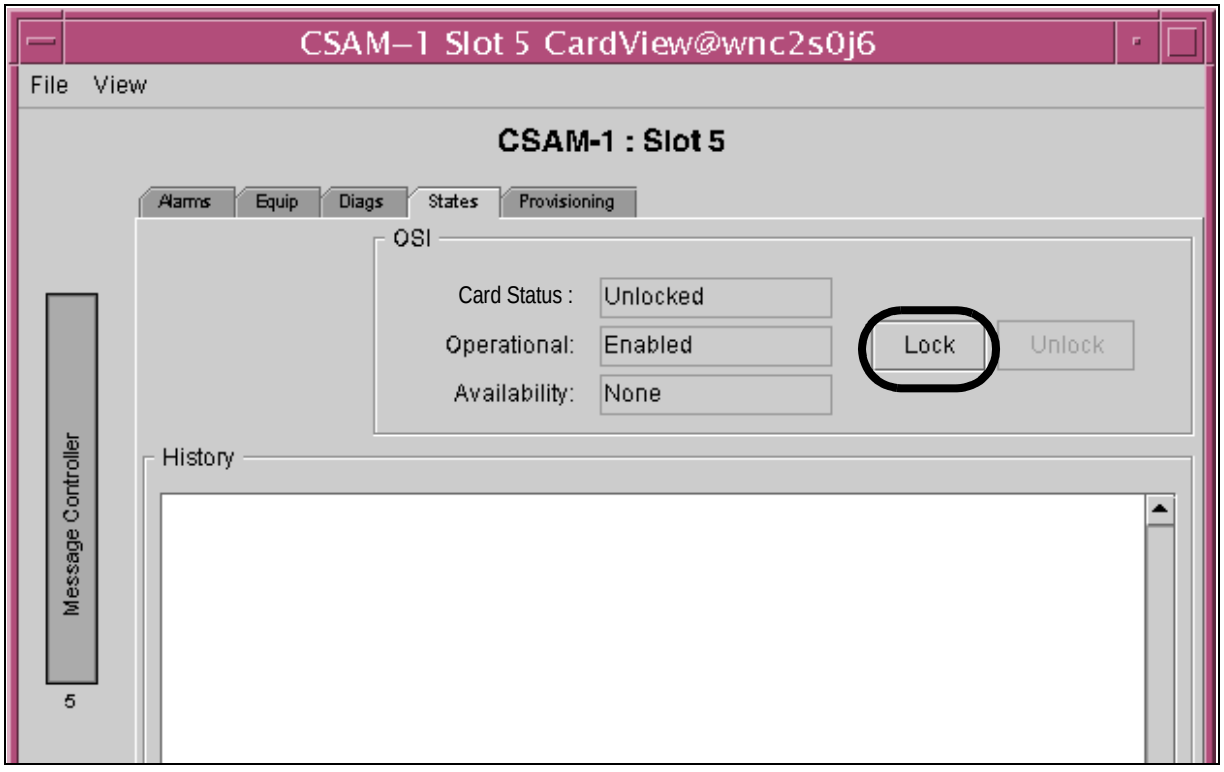
Ensure that the IP address specified in the IP field matches the IP address of Message Controller 0 from step 5. If the values do not match, open the other Shelf View from the CS 2000 SAM21

Manager and check the Message Controller provisioning for that shelf.



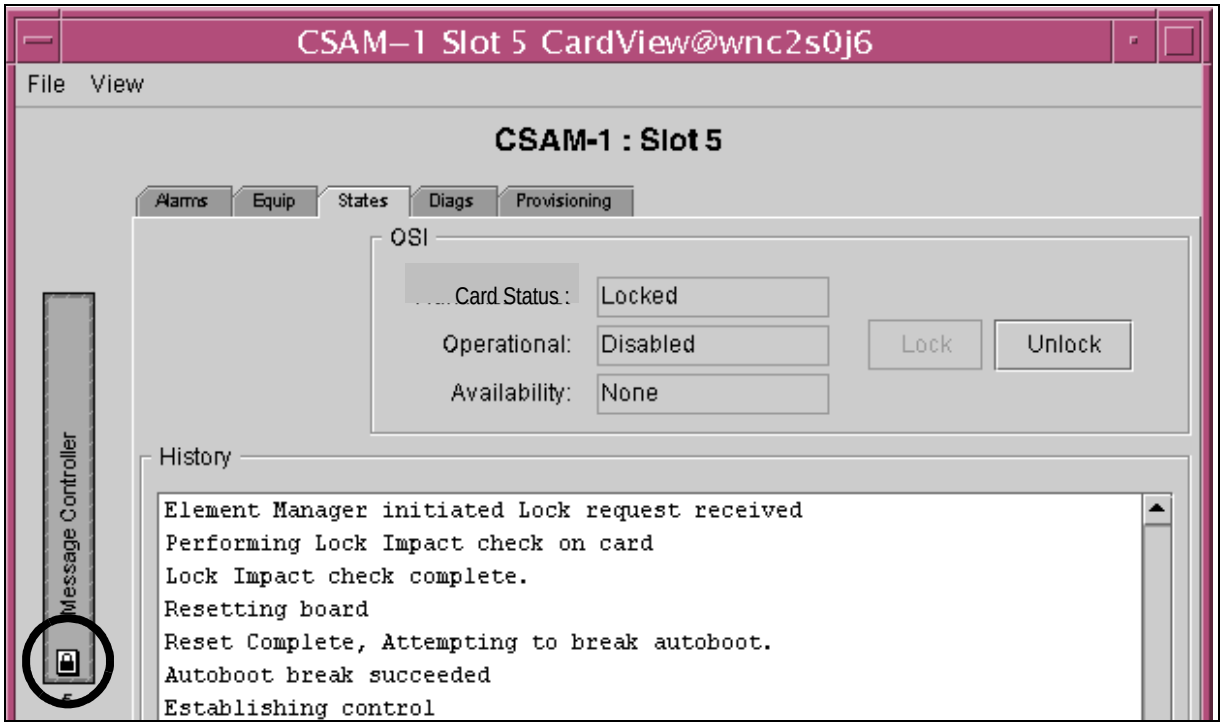
9 Click on the States tab.

Click on the Lock button.



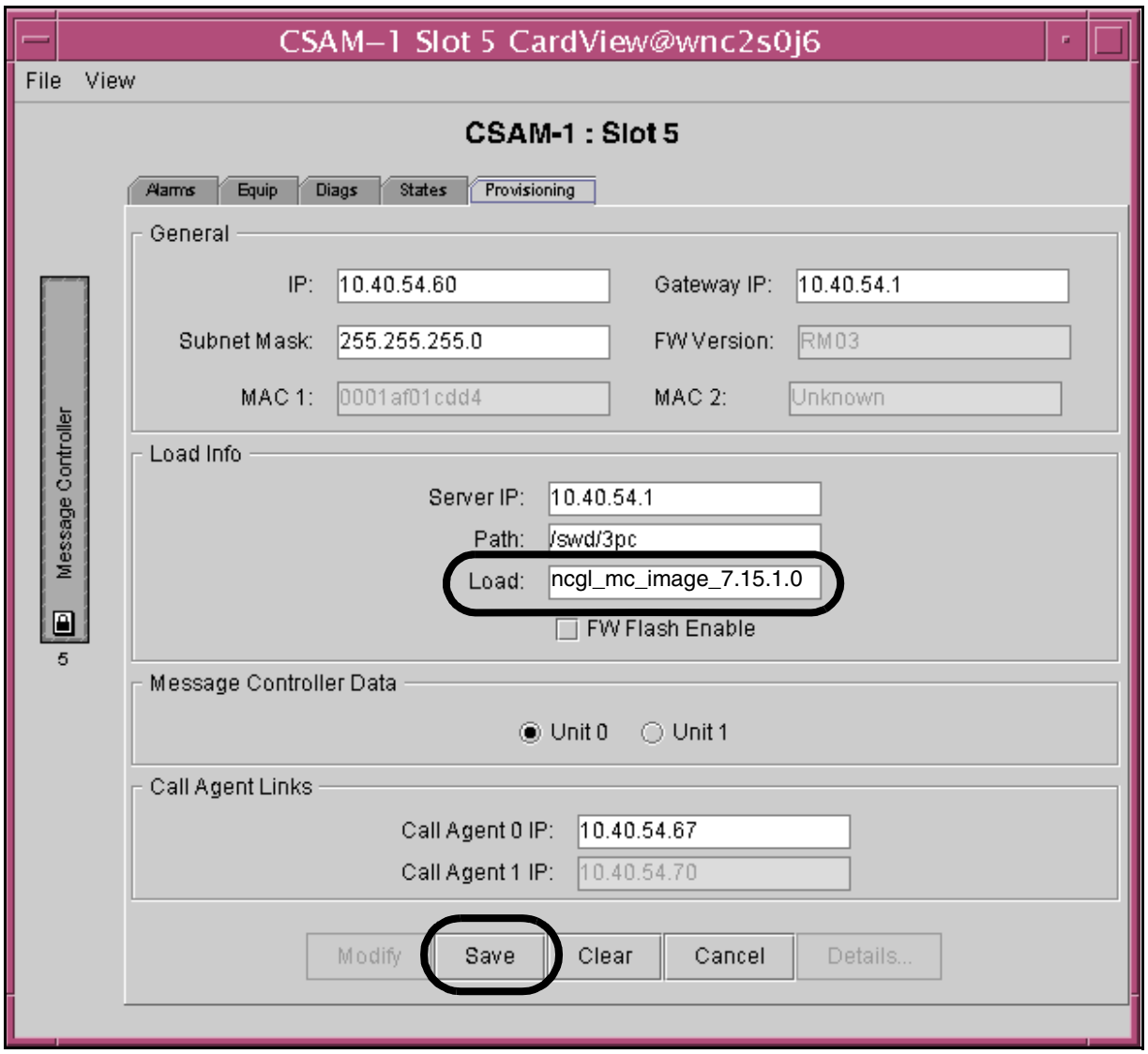
A lock warning dialog window opens. Confirm the lock warning.

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.

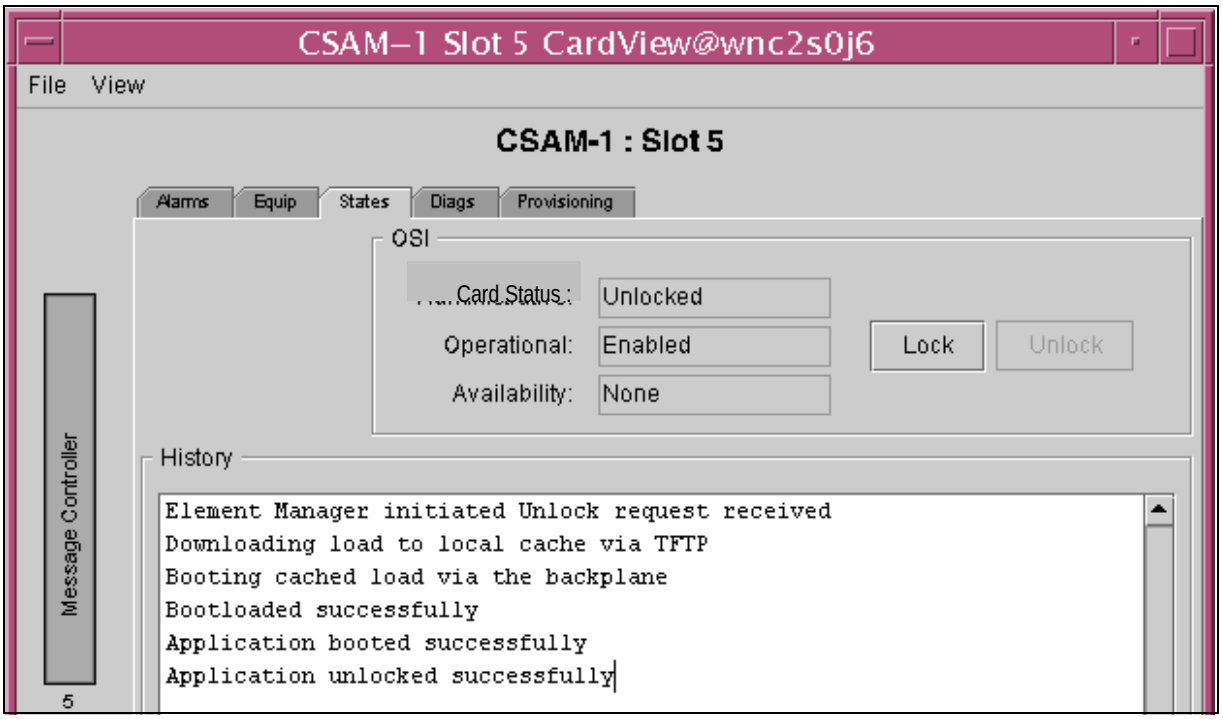
11 Click on the Provisioning tab, change the Load value to the new software load name, and click Save.



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 Mar 19 13:48:45 2005:
17 Help
18 Refresh         Ramdisk ncgl_mc_image_7.15.1.0
  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.

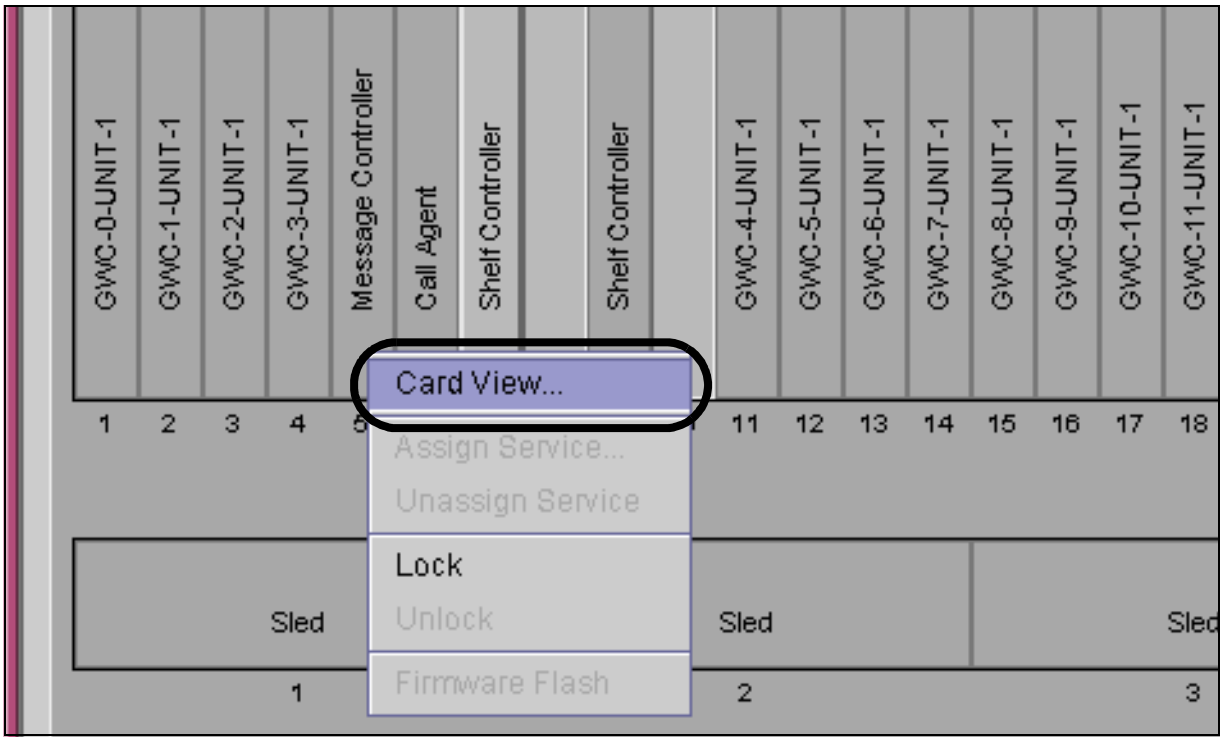
```
10.40.54.61 mc1
```

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.

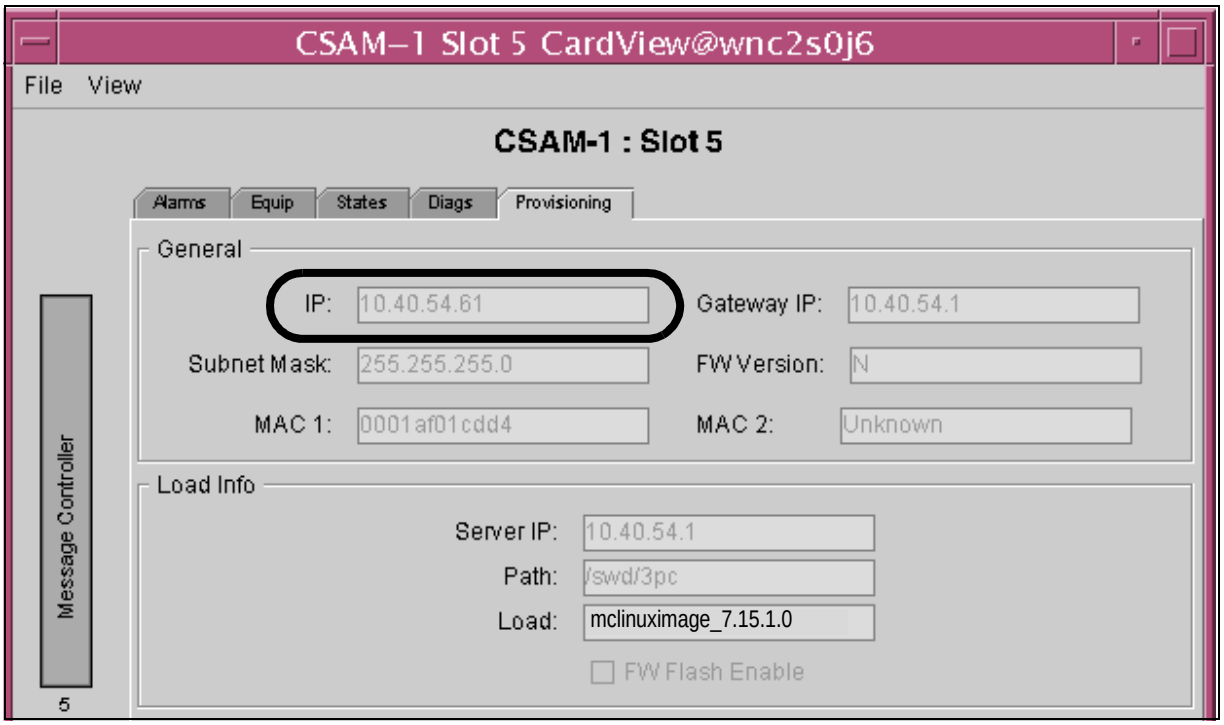


Note: Message Controller 1 is located in slot 12 for some markets.

The Card View window opens.

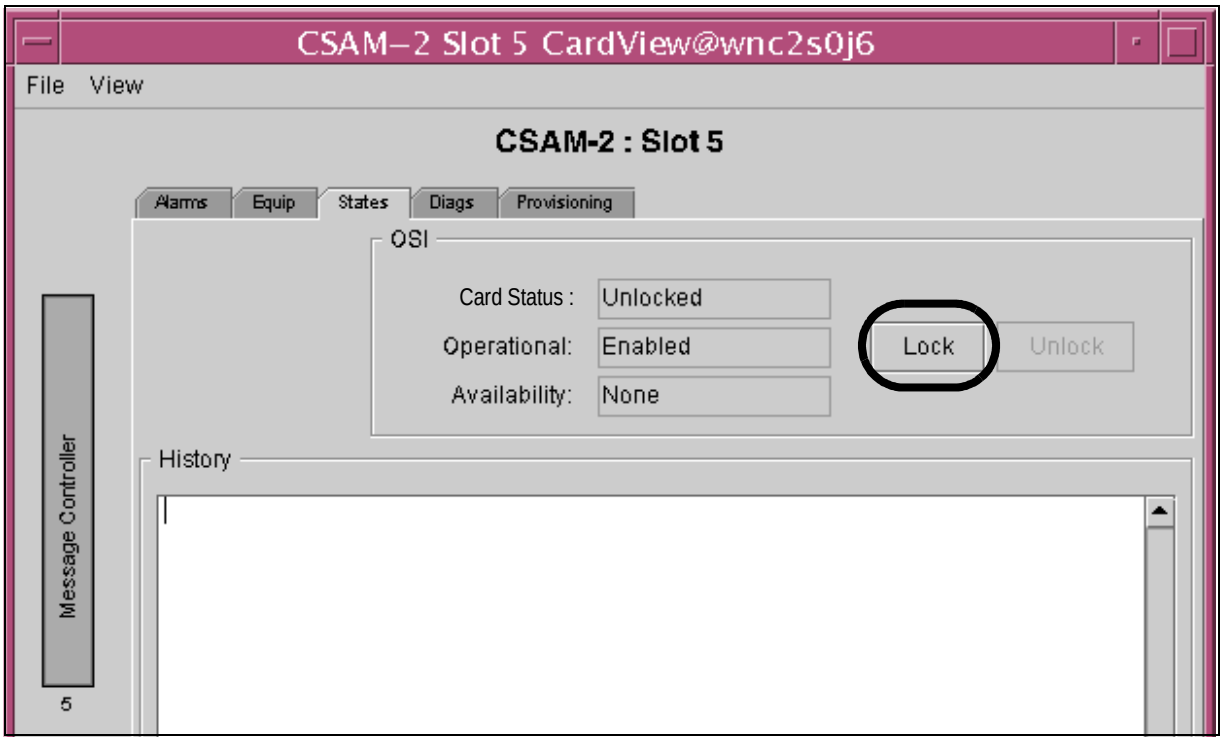
8 Select the Provisioning tab on the Card View window.

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.



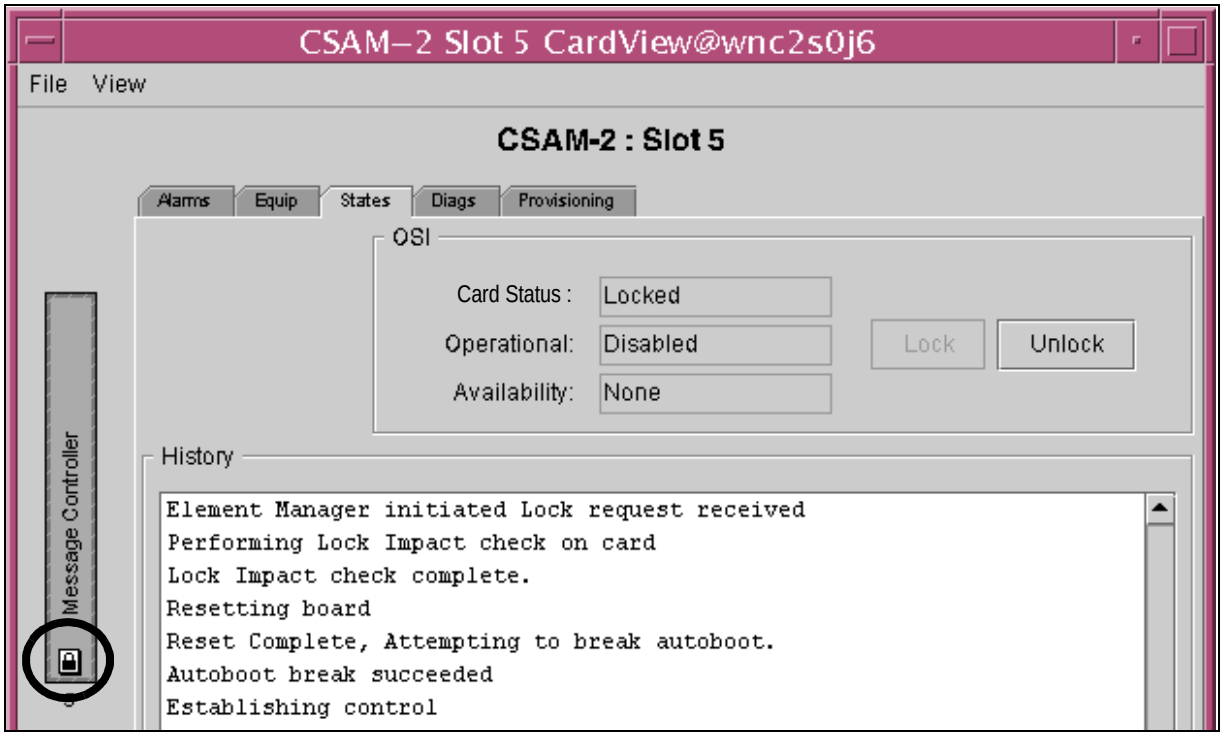
9 Click on the States tab.

Click on the Lock button.



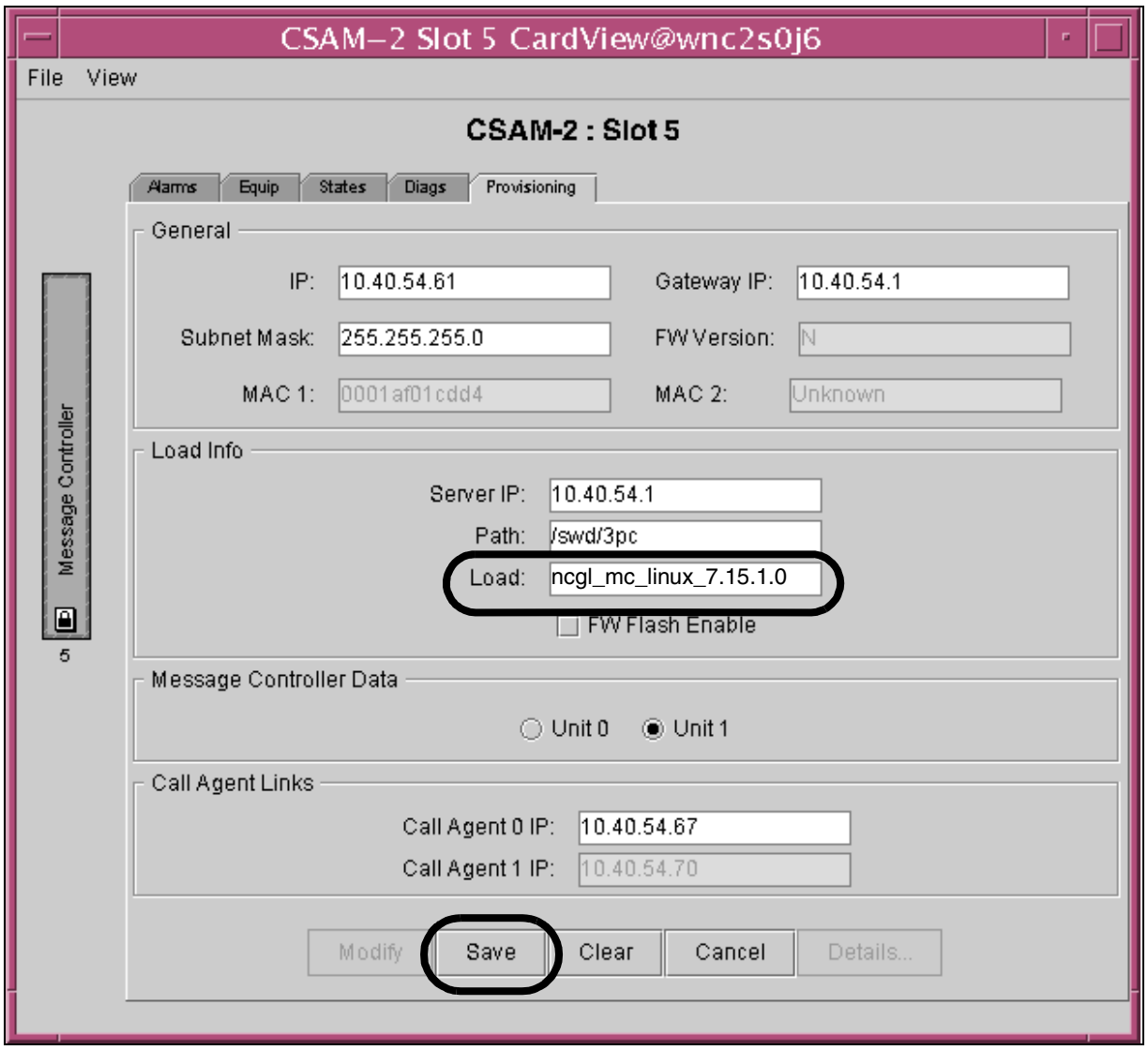
A lock warning dialog window opens. Confirm the lock warning.

10 Wait for the lock icon to appear on the card icon.



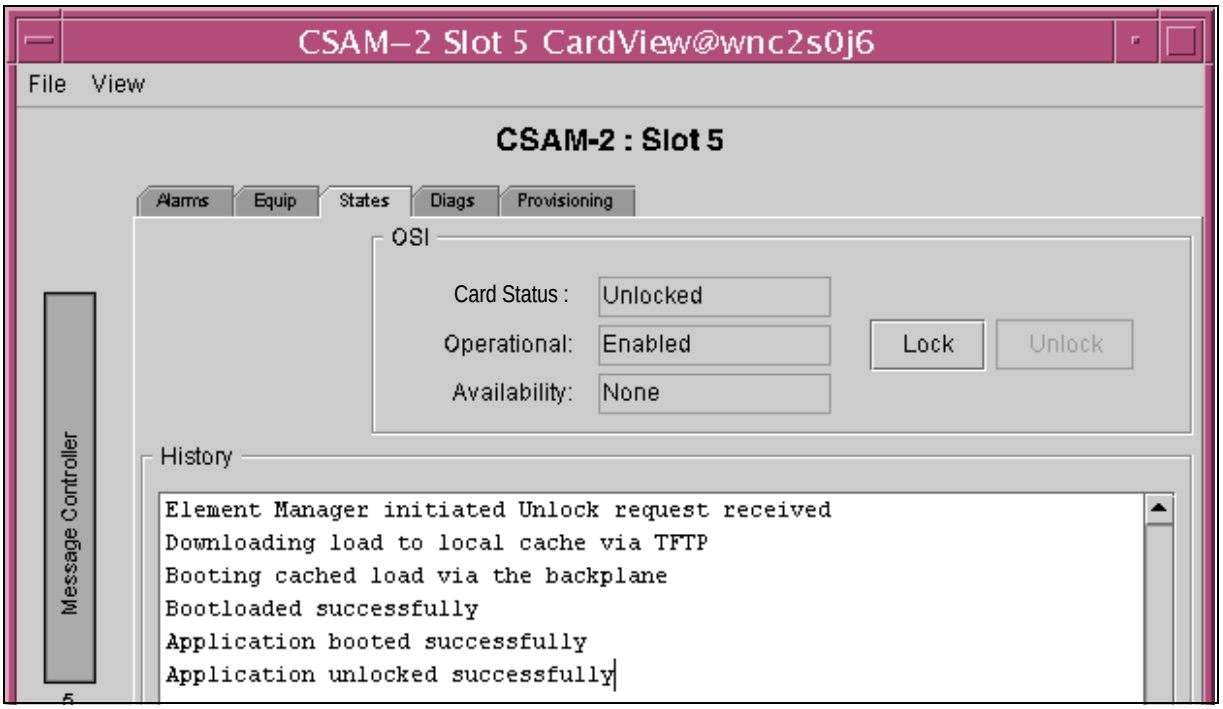
At the Call Agent Manager, a major ATM alarm is raised, the Message Controller enters the Remote Busy (R) state and is reported as out of service.

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_7.15.1.0
  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 COREMTC MAP (ccamtc coremtc); 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 *Upgrading 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 software on page 2003 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 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 60 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.

6 Wake up the active side terminal. Enter:

> <Ctrl+B> HX

At the ACTIVECM window

7 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.

8 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.

       AMA and SMDR Billing subsystem information
       ------------------------------------
MAPCI:
MTC:
IOD:
DIRP:
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
AMA    3    1     4       1      NONE     NO

REGULAR
FILE(S)  STATE  VOLUME   RECCOUNT BLOCK E V  V_B VLID FNUM FRN#
ACTIVE   AVAIL  SD00AMA0  181941  9098  0 71 NO  8402 0000 718F
STANDBY1 AVAIL  SD01AMA0  0       0     0 69 NO  8442 0001 5191

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

MAPCI:
MTC:
IOD:
DIRP:
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
SMDR   7    1     2       5      NONE     NO

REGULAR
FILE(S)  STATE  VOLUME   RECCOUNT BLOCK E V  V_B VLID FNUM FRN#
ACTIVE   AVAIL  SD00SMDR 1        1     0 71 NO  8407 0058 6190

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

```
       TRANSFERRING 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# 719->      DIRPPOOL: Restored     13, Failed    0

  To prepare DIRP billing subsystems for the SWACT, please follow
  instructions in the NTP 'One Night Process Software Delivery
  Procedures.'

  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 billing file and open a new one.
    - prepare tape billing standby volumes.
    - prepare tape parallel standy 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.

System response:

```
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

CAUTION
Possible loss of service
Check the GUIs for CCA, SAM21 EM and Ethernet Routing Switch 8600. *Before proceding with SWACT:* Check the logs for those devices to be sure that the links are stable and clear and any alarms for those devices.

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 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.

```
2005/07/08 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: 2005/07/08, 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 1761

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.

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.
Confirm that the Inactive CA Application is NOT JAMmed,
-or- RELEASE the JAM and confirm when complete:
At the Active COREMTC MAP (ccamtc coremtc); CAMtc Level:
 1)RELJAM - Release the Jam on the Inactive application
Type GO to confirm, and to continue the SWUPGRADE
Step SYNC_SWITCH is not complete.
The SWUPGRADE process has paused. Enter GO.

Starting step SYNC_SWITCH step.
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.

Staring step SYNC_SWITCH.
  Step Footprint transfer is 0 % complete.
  Step Footprint transfer is 10 % complete.
  Step Footprint transfer is 20 % complete.
  Step Footprint transfer is 30 % complete.
  Step Footprint transfer is 40 % complete.
  Step Footprint transfer is 50 % complete.
  Step Footprint transfer is 60 % complete.
  Step Footprint transfer is 70 % complete.
  Step Footprint transfer is 80 % complete.
  Step Footprint transfer is 90 % complete.
  Step Footprint transfer is 100 % complete.
  Step Memory Sync is 0 % complete.
  Step Memory Sync is 10 % complete.
  Step Memory Sync is 20 % complete.
  Step Memory Sync is 30 % complete.
  Step Memory Sync is 40 % complete.
  Step Memory Sync is 50 % complete.
  Step Memory Sync is 60 % complete.
  Step Memory Sync is 70 % complete.
  Step Memory Sync is 80 % complete
  Step Memory Sync is 90 % complete.
  Step Memory Sync is 100 % complete.
Finished step SYNC_SWITCH.
```

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.

DUMP_OFFICE_IMAGE

SITE — At the ACTIVECM window

1 Nortel recommends making a backup of the new load.

If the **AUTODUMP MANUAL** command is used, the ITOC is updated to reference the newly dumped load. Otherwise, use the SBF command within ITOCCI to set the boot file to the new load.

Once the dump is complete, use the **ITOCCI;LBF CM** to verify that the boot file is set to the new load.

The procedure for backing up a call processing application image is listed in procedure Dump call processing application image under heading Backup image on page 1692.

Media Gateway 7400/15000/20000

Before upgrading the Media Gateway 7400/15000/20000

Perform the required prerequisite upgrade as follows:

Network	Media Gateway applies to:	Previous Upgrade
ATM	PT-AAL1 and UA-AAL1	not applicable
	PT-AAL2	Depending on configuration: XA-Core - CS 2000 on page 1638 Call Agent - CS 2000 Compact on page 1639
IP	UA-IP, PT-IP, IAC, IAW, and CHS[1]	Depending on configuration:[2] XA-Core - CS 2000 on page 1638 Call Agent - CS 2000 Compact on page 1639
Tri-Modal	configured application	configured application

1.Includes IP International: PT-IP, CHS, IAC, and UA-IP.
2.UA-IP, PT-IP, and IAC applications support either Call Agent or XA-Core. CHS supports only XA-Core.

After upgrading the Media Gateway 7400/15000/20000

Perform the next required upgrade as follows:

Network	Media Gateway applies to:	Next Upgrade
ATM	PT-AAL1 and UA-AAL1	not applicable
	PT-AAL2	upgrade is complete
IP	PT-IP, UA-IP, IAC, and CHS[1],	Centrex IP Client Manager (CICM) on page 1771
	IAW	MCS Management Server upgrade on page 1835
Tri-Modal	configured application	configured application

1.Includes IP International PT-IP, CHS, IAC, and UA-IP.

About the Media Gateway 7400/15000/20000

Nortel Networks Media Gateway application is a carrier-grade integrated voice and data interworking service. Multiservice Switch Media Gateway creates a gateway between a time division multiplexed (TDM) network and a Multiservice Switch ATM or IP network.

Formally known as Packet Voice Gateway (PVG), the Media Gateway is a software application built on a Multiservice Switch chassis with the addition of a Voice Services Processor (VSP) card.

For upgrade procedures, refer to IP Applications on page 934 in the upgrade section Multiservice Switch (MSS) 15000/20000 on page 820.

Centrex IP Client Manager (CICM)

Before upgrading the Centrex IP Client Manager (CICM)

Perform the required prerequisite upgrade as follows:

Network	CICM applies to:	Previous Upgrade
ATM	not applicable	not applicable
IP	UA-IP, PT-IP, IAC, and CHS[1]	Media Gateway 7400/15000/20000 on page 1769
Tri-Modal	not applicable[2]	not applicable

1.Includes IP International: CHS, PT-IP, UA-IP, and IAC.
2.Carrier Hosted Services introduced to Tri-Modal in the SN08 release. Only CHS conversions and new installations are supported for the Trii-Modal SN08 applications.

After upgrading the Centrex IP Client Manager (CICM)

Perform the next required upgrade as follows:

Network	CICM applies to:	Next Upgrade
ATM	not applicable	not applicable
IP	IAC and CHS[1]	Original Equipment Manufacturer (OEM) gateways and gateway managers on page 1833
	UA-IP and PT-IP[2]	upgrade is complete
Tri-Modal	not applicable	not applicable

1.Includes IP International: IAC and CHS.
2.Includes IP International: PT-IP and UA-IP.

About the Centrex IP Client Manager (CICM)

Centrex IP Client Manager (CICM) is part of Nortel Networks Carrier Hosted Services (CHS), which is a portfolio of products and services that provides IP-based solutions to IP network-based subscribers. CHS delivers legacy Digital Multiplex System (DMS) and Centrex capabilities to users connected to an IP network using voice multimedia integration. CICM delivers Centrex capabilities to users connected to an IP network using VoIP technology on a PC SoftClient or an IP P-phone.

Preparing to upgrade CICM software

This section provides the software strategy to prepare for upgrading the software of the Centrex IP Client Manager (CICM) element manager (EM) and its pairs of CICM nodes.

Preparing to do a CICM software upgrade includes these sections:

- Understanding CICM software upgrades
- Hardware revision compatibility
- Backing up the CICM-EM and CICM node software configuration
- Software upgrade restrictions and limitations
- Software upgrade strategy of CICM

Understanding CICM software upgrades

An upgrade must always be applied to both CICM-EMs of a redundant pair or both CICM nodes of a redundant pair. Prepare for a software upgrade to CICM-EMs and CICM nodes by understanding:

- CICM software versions
- An upgrade by maintenance release or product release
- MR upgrade implementation guidelines
- Sources of software files for CICM
- High-level methodology for applying upgrades

CICM software versions

The software to operate CICM nodes and CICM-EMs is applied independently to each. Each pair of CICM nodes must have the same version of software. For example, while the CICM-EMs have version 8.0 (for SN08), each pair of CICM nodes can operate with either version 7.0 (for SN07) or 8.0 (for SN08).

The software version has the format <release_number>.<build_number>

Example
8.10.183

The release number is 8.10

The build number is 183.

The lower left corner of the CICM-EM web pages shows the base release of the software version (for example, 8.0 for SN08). The version

that is running on the CICM-EM or on the pair of nodes is located on the page maintenance (cicm-nnn).

An upgrade by maintenance release or product release

The types of upgrades that can be applied to redundant pairs of CICM-EMs or CICM nodes are:

- An upgrade by maintenance release
- An upgrade by product release

An upgrade by maintenance release

An upgrade by maintenance release (MR) involves loading an increment of the build number within the same version of the software release. For an MR upgrade to CICM software SN08, the MR changes the build number from 8.10.xxx to 8.10.MRy. The first maintenance release is MR0 (zero), which is An upgrade by product release. For SN08 or later, any upgrade to the CICM nodes (excluding the CICM-EM) cannot exceed three MR increments. Examples of the range are shown with the upgrade procedure in Prerequisites to upgrading a CICM node with an MR.

To ensure that an MR is appropriate to a specific node (CICM-EM or CICM), the system also checks that the load is intended for the type of node it is being applied to, and for an appropriate range of load build numbers. The node and the load criteria must be met for the MR to be applied.

Applying an MR over-writes previous software and requires at least one system restart.

See also MR upgrade implementation guidelines.

The task flow and procedures to upgrade CICM-EMs and CICM nodes with an MR are in Upgrading CICM software.

An upgrade by product release

A upgrade by product release involves loading an increment of a different version of software, that is, the software release number increments (for example, from x.y to x+1.y). Applying a product release over-writes previous software and will require a series of system restarts for each upgraded node.

CICM product releases are made available from the ISO vault. Each release includes its own upgrade file. Separate releases are available for each of the following:

- the CICM-EM using the CPV5370 cards
- the CICM-EM using the CPN5385 cards
- the CICM nodes using the CPV5370 cards
- the CICM nodes using the CPN5385 cards

The task flow and procedures to upgrade CICM-EMs and CICM nodes are in Upgrading CICM software.

MR upgrade implementation guidelines

The guidelines for implementing upgrades are as follows.

- Always read the release notes prior to an upgrade.
- The sequence of upgrading is to upgrade the CICM-EM, then the CICM nodes, then the terminals. If a primary and backup CICM-EM pair are deployed, both EMs must be upgraded prior to the first CICM node upgrade.

  Terminal upgrades are addressed in *Upgrading CICM*, NN10230-461 in Upgrading firmware on IP phone sets".
- Each node of the CICM is upgraded individually. However, paired nodes are upgraded to the same software version. Running paired nodes at different versions for can result in degradation in performance or behavior while the nodes are running different software versions.
- No network re-configurations are to occur during an upgrade. Rolling back from the upgrade, that is, returning operation to the former software version, is not possible.
- Do the upgrade during the lowest call traffic period to minimize impact on users.
- The upgrade takes one to two hours to complete. Service degradation by call capacity reduction occurs only for portions of the upgrade period.
- For MR upgrades only, resource use (that is, active call count) can be monitored from the CICM-EM.
- To do an upgrade procedure, you must use administrator userids and passwords to login to the CICM-EM.

Sources of software files for CICM

The source of software upgrade files for either the CICM-EMs or the CICM nodes are handled by the following computer setups and delivery methods:

- Computer setups to handle software files
- Recognizing the type of source file for an upgrade
- Compact disks

The details of file management are included in various procedures that are invoked in sequence by the task flows in this document.

Computer setups to handle software files

The computer setup you can use to handle the software files for CICM-EMs and CICM nodes must be able to access the CICM-EMs. The setup can involve one of the following:

- a personal computer (PC)
- a Nortel server, such as a Server Foundation Platform Software (SPFS) or the Integrated Element Management System (IEMS)
- your own server

The PC and your server must comply with the specifications identified in *CICM Basics*, NN10044-111 and run the supported operating system (OS) software.

Recognizing the type of source file for an upgrade

The source files for upgrades have different naming convention to distinguish what each file applies to. The naming conventions are as follows:

- for SN08 and earlier CICM-EM upgrade files: EM_<release>.cab
- for SN08 and earlier CICM node upgrade files: GW_<release>.cab
- for m6350 SoftClient MR upgrade software: CICM_m6350_SoftClient(x.x_MRn).exe

The <release> indicates the software version as an increment of MRs, where the n in MRn is:

- 0 (zero), denoting a product release upgrade
- from 1 (one), denoting a maintenance release (MR) upgrade

Compact disks

A series of compact disks (CDs) provides the following software for both the CICM-EMs and the CICM nodes:

- a product release (which is an MR zero)
- the latest MR increment

The label on a CD containing CICM software begins CICM..., for example:

- on the 3 CDs from order code CICM0080 for CICM nodes:
  - CICM 5370 8.10.183.iso
  - CICM 5385 8.10.183.iso
  - CICM Upgrade 8.10.183.iso
- on the 1 CD from order code CICE0080 for CICM-EMs:
  - CICMEM 5370 8.10.183.iso
  - CICMEM 5385 8.10.183.iso

The 5370 indicates software for the SAM16 while 5385 indicates software for the SAM21.

High-level methodology for applying upgrades

The high-level methodology for handling upgrade files is:

- copying the files from a source onto a computer that interfaces the CICM-EMs (this is not required if you are set up for point-of-use distribution)
- electronically transferring the files into appropriate directories on the master CICM-EM
- switching the activity of CICM node pairs to enable downloading the mate
- electronically transferring the files into appropriate directories on the new master CICM-EM
- applying the appropriate files from the master CICM-EM to its slave mate or the slave CICM node
- verifying the success of the upgrade
- switching the activity of node pairs to enable downloading to the mate
- verifying both nodes of a pair are operating normally and fully

Hardware revision compatibility

The table Hardware revision compatibility with software summarizes the hardware to software compatibility with CICM.

CICM with SN08 and later supports two hardware revisions. If the telco wants to upgrade from a release prior to CICM with SN07, an interim upgrade to SN07 is required.

Hardware revision compatibility with software

Hardware revision	CICM node	CICM-EM	Supported software releases
B	SAM16 Shelf CPV5370 processor	CXIP1204 Shelf CPV5370 processor	SN6.12, SN07, SN08
C	SAM21 Shelf CPN5385 processor	CXIP1204 Shelf CPV5370 processor	SN07, SN08

Backing up the CICM-EM and CICM node software configuration

Back up the software of the CICM-EM and CICM nodes prior to an upgrade as a contingency plan to a failed or aborted upgrade. The back-up files are required for the procedures to roll back from an upgrade and restore the former software configuration.

The application that does a CICM node backup resides on the CICM and is controlled by a scheduler through the CICM-EM.

Backing up files can be done at any time either on-demand (manually) or daily (automatically). Backing up on-demand is handled through the CICM-EM while backing up daily is scheduled to run at a user-designated time or the 2:00 am default. The schedule is decided during initial configuration of a CICM node. The procedures to handle an on-demand backup are in Upgrading CICM software.

Backing up files can be done at any time either on-demand (manually) or daily (automatically). Backing up on-demand is handled through the CICM-EM while backing up daily is scheduled to run at a user-designated time or the 2:00 am default. The schedule is decided during initial configuration of a CICM node. The procedures to handle an on-demand backup are in Upgrading CICM software.

For either backup method, the result is a file with the name *backupconfig_<day_number>_em.xml* for a CICM-EM or *backupconfig_<day_number>.xml* for a CICM. The files are sent to the CICM-EM through anonymous FTP and stored in this node-specific folder on the D drive of the PC with CICM software:

D:\CentrexIP\support\backups\<cicm_node>

The <day_number> is from the current month. The <cicm_node> is the full name of the CICM so that the backups of Nodes A and B are stored separately. When the first backup is taken, the node-specific folder is automatically created. The craftsperson is responsible for moving or copying the back-up files from the CICM-EM folders to a different and safer storage location before the files are automatically overwritten by the next day with the same date. The CICM-EM has a limited amount of storage space for the back-up files.

What the back-up file stores

The back-up procedure stores all elements of the MIB registry that are static data and that are directly relevant to the configuration of the CICM. The kind of data that is backed up by the procedure includes:

- virtual media gateways
- user configurations, including passwords, locality preferences, and contacts
- terminals, including locality preferences and the auto-login preference
- lines, including their features
- profiles of end-point equipment, including the global profile overrides stored on the CICM

Software upgrade restrictions and limitations

The restrictions and compatibility issues of the software changes are:

- Upgrading CICM to SN08 can be applied only from a CICM:
  - — running 7.0 MR5 or later
  - — running 8.0 MR2 or later
- With SN07, terminals can be connected to the master and slave nodes. With SN08 and later, terminals are connected only to the master. During an upgrade from SN07, a switch of activity (SWACT) cannot automatically recover terminals. When upgrading from SN07, a manually initiated terminal transfer is necessary. When upgrading from SN08 or later, terminals are automatically transferred as part of the SWACT. That is, the CICM SN08 master (becoming the slave) transfers its terminals to the CICM SN08 slave (becoming the master) so that the new master has all of the terminals.
- During the upgrade when nodes temporarily have different versions of software, initiating a SWACT while the SN08 or later node is the master will cause the floating UNIStim address to be unbound. Any terminals connected to this node will be lost. Manually transfer the terminals away from the SN08 or later node before the SWACT.
- During the upgrade to CICM Node A, the CICM selects its existing static UNIStim address as the floating address.
- During the upgrade, the operator must provide an alternative static address to replace node A's old static address (used as the floating address following the upgrade).
- During the upgrade, the CICM does not update the S1 and S2 entries of the terminals connected to the CICM at the time of the upgrade. The operator must make any required configuration changes to the terminals following the upgrade (for example, through DHCP).
- For CICM SN08 or later, the Carrier Voice over IP (VoIP) environment and datafill remains consistent with how it was in SN07 Plus.

CAUTION
Risk of service prevention
When upgrading from SN07, it is critical to upgrade Node A first since the upgrade results in the use of Node A's pre-upgrade (SN07) static UNIStim address as the floating UNIStim address for the post-upgrade (SN08 or later) operation.

Software upgrade strategy of CICM

The software upgrade strategy of CICM is divided into:

- Prerequisites for a CICM software upgrade
- CICM software upgrade summary
- Follow-up after a CICM software upgrade
- Conversion from TDM

Prerequisites for a CICM software upgrade

Before the software of a CICM node is upgraded, the following must be done.

1. Upgrade the CS2M, Core, and GWC.
2. Copy the CICM-EM upgrade file to the location on the CICM-EM that is used for an upgrade.
3. Copy the CICM node upgrade file to the location on the CICM-EM that is used for an upgrade.
4. Upgrade the CICM-EMs.
5. Upgrade the CICM nodes.

For the sequence of procedures, refer to the task flow in Upgrading CICM software.

CICM software upgrade summary

The CICM software upgrade strategy is summarized as follows.

- The supported software upgrade paths are from these CICM release versions:
  - SN6.12 to SN07
  - SN07 to SN08
- MR upgrades for the CICM-EM and CICM nodes may be performed by telco CICM administrators.
- The CICM upgrade from SN07 to SN08 or later must be done remotely by telco CICM administrators using a process similar to a maintenance release (MR) upgrade.
- No hardware changes are required for the CICM release SN07 to SN08.
- For any upgrades prior to SN6.12 (such as releases 2.4 to 2.5), refer to the Upgrades section of the previous CICM versions of *CICM Basics* (formerly titled *CICM Product and Technology Fundamentals*), NN10044-111.

Follow-up after a CICM software upgrade

After an upgrade from SN07 to SN08 or later is completed, address or note the following.

- Node B's static UNIStim address is no longer valid for use by terminals in the network. Once the upgrade is complete, it is recommended that the operator take the necessary steps to update all terminals in their network so that they do not attempt to contact the CICM on this (now) invalid address.

  If using dynamic host configuration protocol (DHCP), its configuration should be changed. Refer to DHCP documentation for information on configuration DHCP servers.

- Leaving terminals configured with the old B UNIStim address will not cause harm to the network. However, it can cause individual terminals to take longer to actually locate the CICM following a terminal reboot, since it can use the invalid address for its search. This is not an issue when upgrading from SN08 or later.

- If a survivable remote gateway (SRG) is to be deployed, this can safely be done once the CICM has been upgraded. In doing so, the terminal must be reconfigured such that S1 is set to the CICM's floating UNIStim address, and S2 is set to the SRG's address. These must not be reversed. The SRG uses S2.

- For those terminals in the network not serviced by an SRG, it is recommended that both their S1 and S2 entries be set to the CICM's floating UNIStim address.

Conversion from TDM

CICM with SN08 or later does not support a conversion from TDM to Carrier Voice over IP (VoIP).

Software upgrades to Nortel IP Phone sets

The Nortel IP Phone sets that are connected to the CICM nodes receive their software upgrades over the IP network. A software upgrade for a phone set is referred to as a firmware upgrade. For details about handling phone set upgrades, see "Upgrading firmware on IP phone sets" in this document.

Upgrading CICM software

This section of *Upgrading CICM*, NN10230-461 provides the task flow and procedures to upgrade the software of a pair of redundant Centrex IP Client Manager (CICM) element managers (CICM-EMs) and their pairs of redundant CICM nodes.

The topics in this section are:

- CICM-EM and CICM node preparation for an upgrade
- CICM-EM and CICM node upgrades
- Upgrade procedures for CICM-EM and CICM nodes

CICM-EM and CICM node preparation for an upgrade

Prepare a pair of Centrex IP Client Manager (CICM) element managers (CICM-EM) and their pairs of CICM nodes for an upgrade by doing a series of procedures in a task flow. The preparation is divided into:

- Prerequisites to the task flow of CICM-EM and CICM node preparation
- Task flow of CICM-EM and CICM node preparation

Prerequisites to the task flow of CICM-EM and CICM node preparation

Before following the task flow, ensure that you have addressed these requirements.

- The task flow and all procedures in it apply to doing these upgrades for either SAM21 and SAM16 hardware:
  - — an MR from your current release up to three increments apart, for example, 8.0 MRx to 8.0 MRy where x and y are less than or equal to three increments apart or for example

    8.0 MR1 with 8.0 MR2, 8.0 MR3, or 8.0 MR4
  - — a product release from your current release to a subsequent release, for example, from:
    - – 7.0.MRx (MR5) or later to 8.10 or later (MR2)

  Refer to the CICM Release Notes for the actual supported versions.
- All Carrier Voice over IP (VoIP) components that are non-gateway-specific (including the CS2000, CS2000 Management Tools server (formerly SESM), and gateway controllers) must already have been successfully upgraded to the target upgrade release and be fully in service.

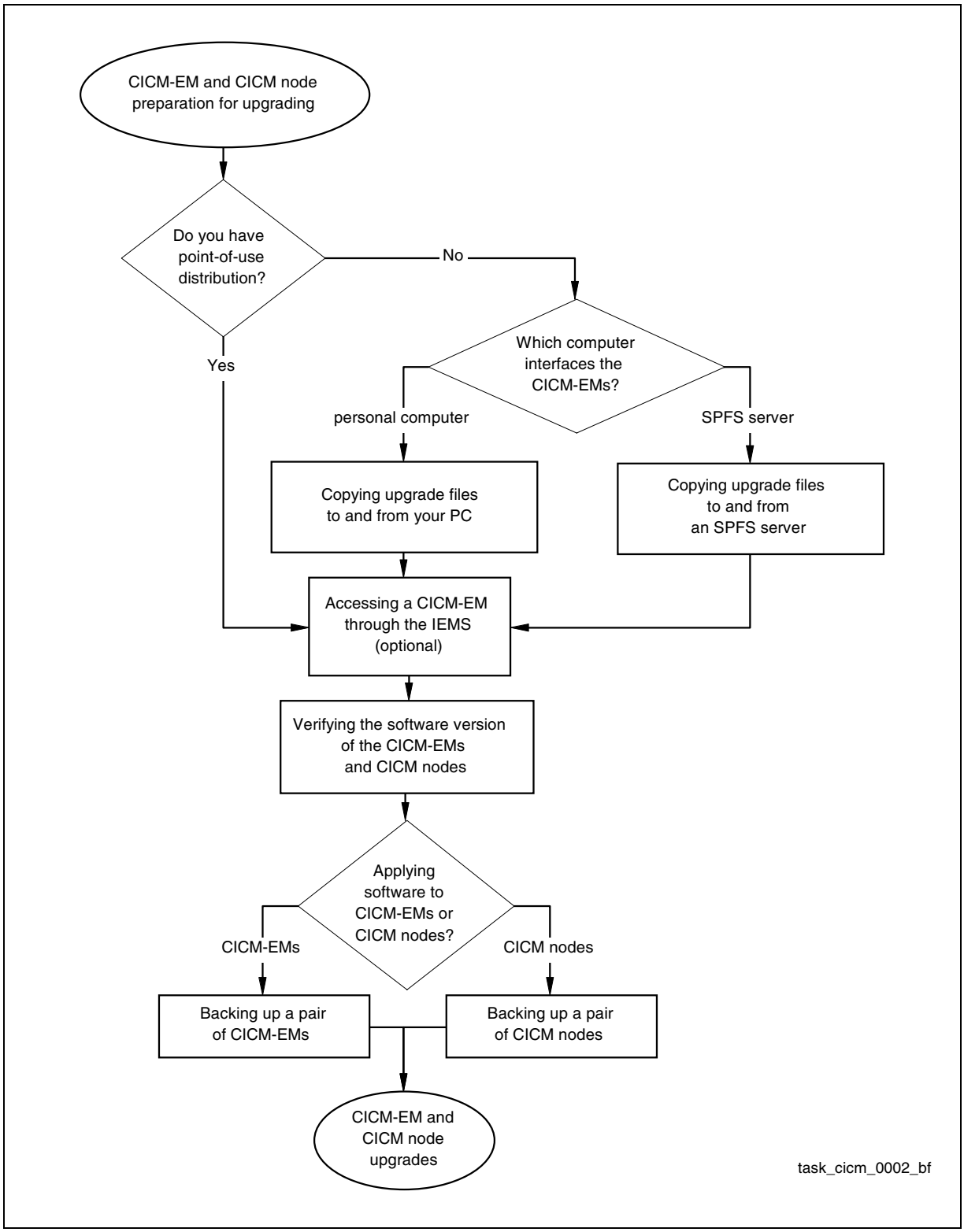
- IEMS must be configured to enable accessing the CICM-EM, usually as part of an initial installation. Otherwise refer to *Integrated EMS Configuration Management*, NN10330-511.
- CICM must be configured to interwork with IEMS, usually as part of an initial installation. Otherwise refer to *Configuration Management*, NN10240-511.
- Read and understand Preparing to upgrade CICM software.
- You must have access to the appropriate upgrade files from Nortel. Refer to the possibilities in Sources of software files for CICM on page 1775

Task flow of CICM-EM and CICM node preparation

The task flow shows the sequence of procedures and other task flows that are required to prepare for applying an upgrade to a redundant pair of CICM-EMs and a redundant pair of CICM nodes. Follow the figure Task flow of CICM-EM and CICM node preparation.

To link any procedure or imbedded task flow, go to Navigation immediately following the figure.

Task flow of CICM-EM and CICM node preparation



Navigation

The procedures and tasks in the task flow are listed alphabetically.

- Accessing a CICM-EM through the IEMS
- Backing up a pair of CICM nodes
- Backing up a pair of CICM-EMs
- CICM-EM and CICM node upgrades
- Copying upgrade files to and from an SPFS server
- Copying upgrade files to and from your PC
- Verifying the software version of the CICM-EM and CICM nodes

CICM-EM and CICM node upgrades

Upgrade a pair of Centrex IP Client Manager (CICM) element managers (CICM-EM) and their pairs of CICM nodes by doing a series of procedures in a task flow. The upgrade is divided into:

- Prerequisites to the task flow of CICM-EM and CICM node upgrades
- Task flow of CICM-EM and CICM node upgrades

Prerequisites to the task flow of CICM-EM and CICM node upgrades

Before following the task flow, ensure that you have addressed these requirements.

- The CICM-EM and CICM nodes must be in service without faults.
- Read and understand Preparing to upgrade CICM software.
- Upgrading with an MR or product release is a manual operation. Start an upgrade during a period of lowest traffic for the CICM-EMs and CICM nodes.

- The pair of CICM-EM nodes must always be upgraded before the pair of CICM nodes for an MR or a product release.
- Once an upgrade has been started, do not attempt any software configuration changes to any node until each node-pair is confirmed to be upgraded and fully operational.

CAUTION
Risk of service prevention
Before starting the upgrades task, read each procedure to determine what data you will need for entries, especially the preboot and preboot upgrade IP addresses. It is critical to have all the data readily available before starting any procedure in the task flow CICM-EM and CICM node preparation for an upgrade.

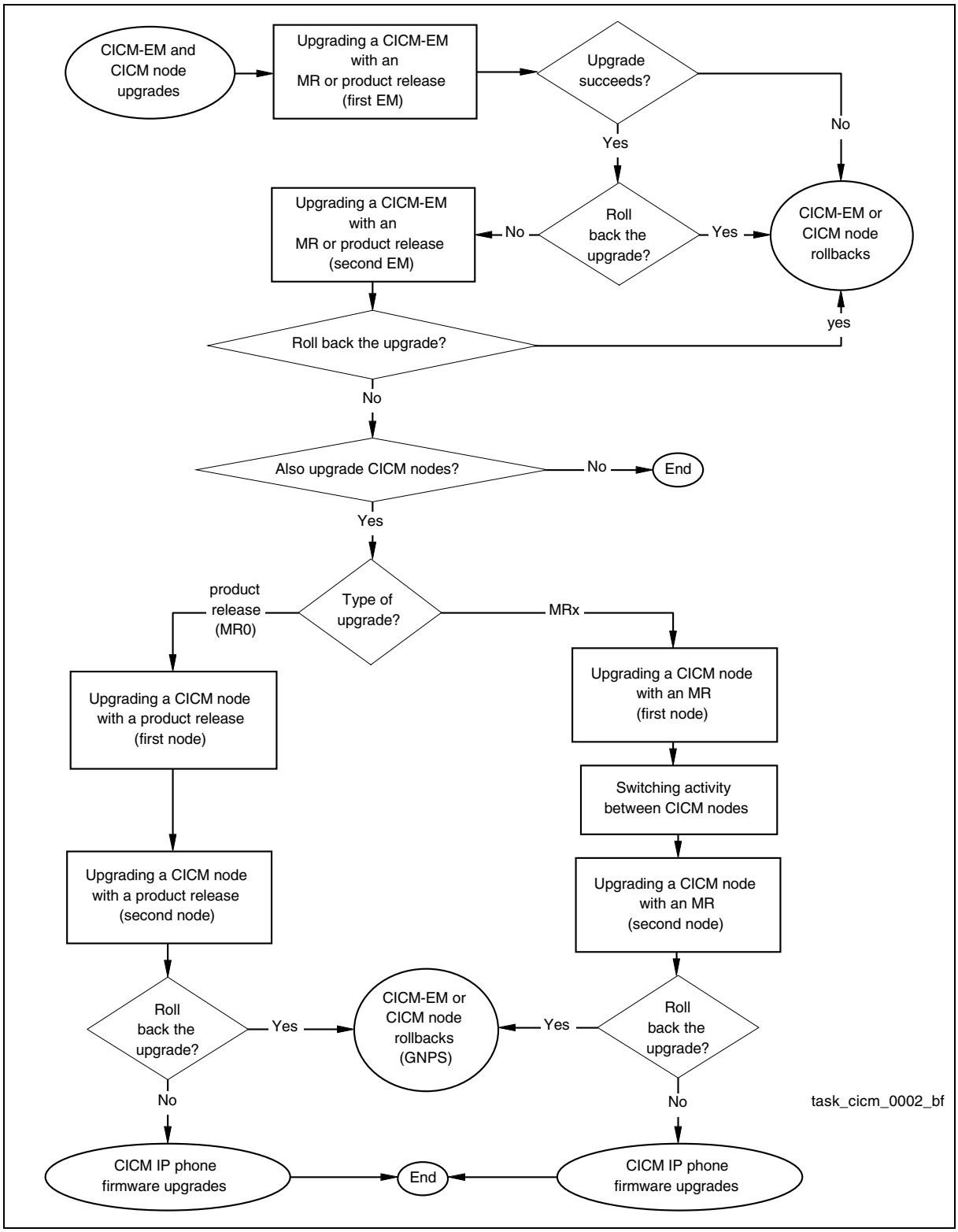
Task flow of CICM-EM and CICM node upgrades

The task flow shows the sequence of procedures and other task flows that are required to prepare for applying an upgrade to a redundant pair of CICM-EMs and a redundant pair of CICM nodes. Follow the figure Task flow of CICM-EM and CICM node preparation.

To link any procedure or imbedded task flow, go to Navigation immediately following the figure.

Note: Some of the rollback decision points do not appear in the upgrades task flow because they are included within various procedures.

Task flow of CICM-EM and CICM node upgrades



Navigation

The procedures and tasks in the task flow are listed alphabetically.

- “CICM-EM and CICM node roll backs” in *Upgrading CICM*, NN10230-461
- “CICM IP phone firmware upgrades” in *Upgrading CICM*, NN10230-461
- Switching activity between CICM nodes
- Transferring terminals for an upgrade
- Upgrading a CICM node with a product release
- Upgrading a CICM node with an MR
- Upgrading a CICM-EM with an MR or product release

Upgrade procedures for CICM-EM and CICM nodes

The procedures for upgrading the software of a CICM-EM pair and its CICM node pairs are listed alphabetically following this section. The actions you must do or understand prior to starting the task flow are identified in Prerequisites to the task flow of CICM-EM and CICM node preparation. The sequence of doing the procedures is identified in Task flow of CICM-EM and CICM node preparation.

Note: You must follow the prerequisites and sequence of procedures identified in the task flow in order to properly complete upgrading.

Accessing a CICM-EM through the IEMS

Access a CICM-EM through the Integrated Element Management System (IEMS) to upgrade the CICM-EM or CICM nodes or both with a maintenance release (MR) or a product release.

Prerequisites to accessing a CICM-EM through the IEMS

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node preparation for an upgrade.
- To access IEMS, you must know the IP address of the IEMS server and be able to access it through a web browser.
- You need to know the administrator userid and password to log into the CICM-EM from IEMS. Otherwise your access is determined by whatever authentication structure you have configured.

Procedure steps to accessing a CICM-EM through the IEMS

At a web browser

1 Access the IEMS by entering the command:

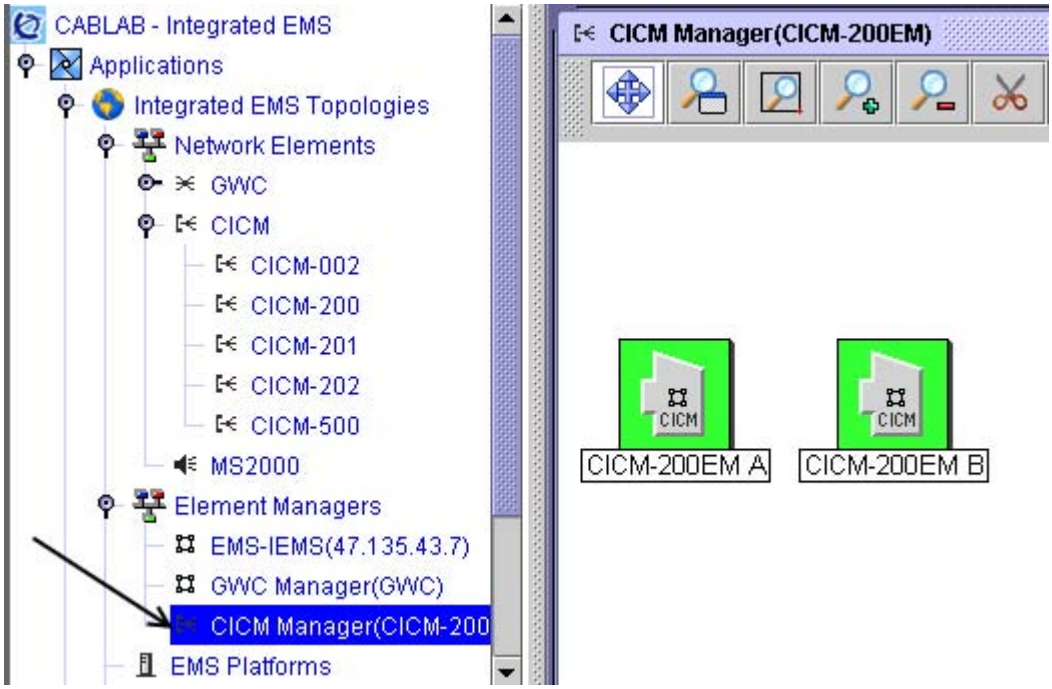
```
https://<iems_ip_address>:9091/LoginPage.do
```

2 Once connected, click option Web Start Client (which uses JAVA rather than HTML).

Unless already installed, you must install the version of JAVA that is provided at the Web Start Client link.

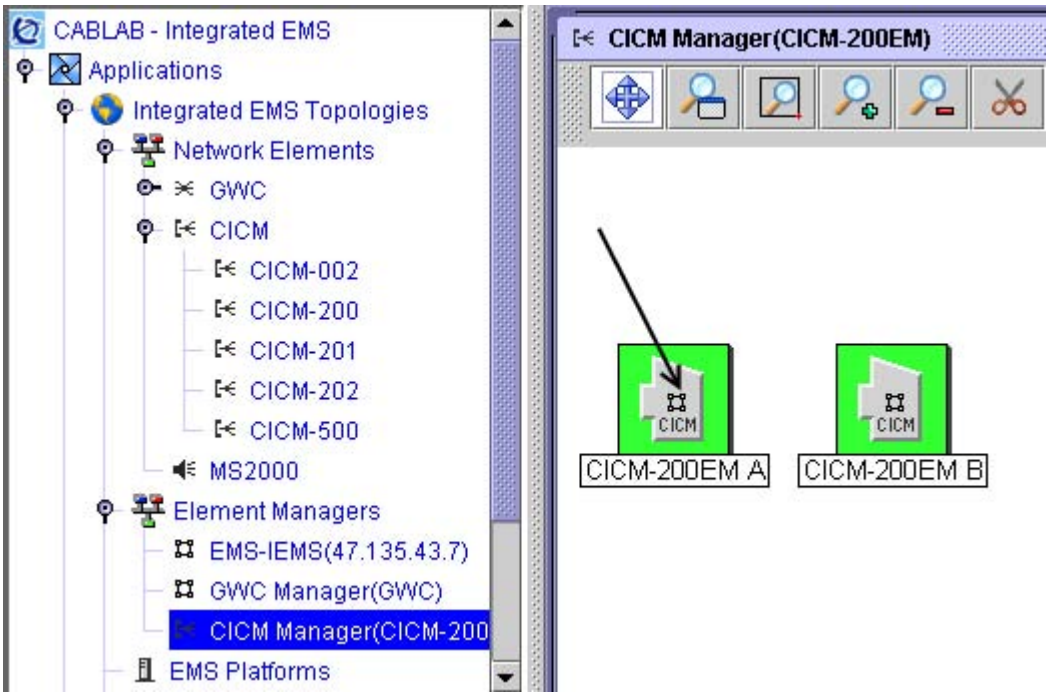
At the IEMS GUI

3 At the IEMS menu of components, locate the item for the CICM-EM to undergo an upgrade. Ensure that the static IP address of the CICM-EM is for the one to be upgraded.



4 Right click the icon of the CICM-EM to undergo an upgrade, and select **Launch CICM Manager**.

A prompt occurs for the userid and password.



5 Enter the CICM-EM administrator userid and password.

The CICM-EM web page opens.

6 Ensure that the node you selected is in-service.

7 To upgrade a pair of CICM-EM or CICM nodes, follow the other procedures in the task flow.

8 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

Backing up a pair of CICM nodes

Back up each node of a redundant CICM pair to prepare for restoring a former software configuration when you want a more recent snap-shot than the scheduled back-up file.

Prerequisites to backing up a pair of CICM nodes

Address the prerequisites before starting the procedure.

- Ensure that you have read and understood Backing up the CICM-EM and CICM node software configuration.
- Back up each node of a CICM pair. The back-up file can only be applied to the node it was taken from.
- Each back-up file name must remain the same as the copied file.
- The back-up files must be used only with the identical software release that they were created from.
- The duration of backing up varies according to the amount of datafill configured on the CICM node. The back-up application runs at a low level of software priority to minimize the impact on the service provided (call processing).
- Backup files for CICM nodes are stored on the CICM-EM in subdirectories at:

  d:\centrexip\support\backups\<cicm-nnn>
- Automated daily backups are stored on alternate CICM-EM nodes.

Procedure steps to backing up a pair of CICM nodes

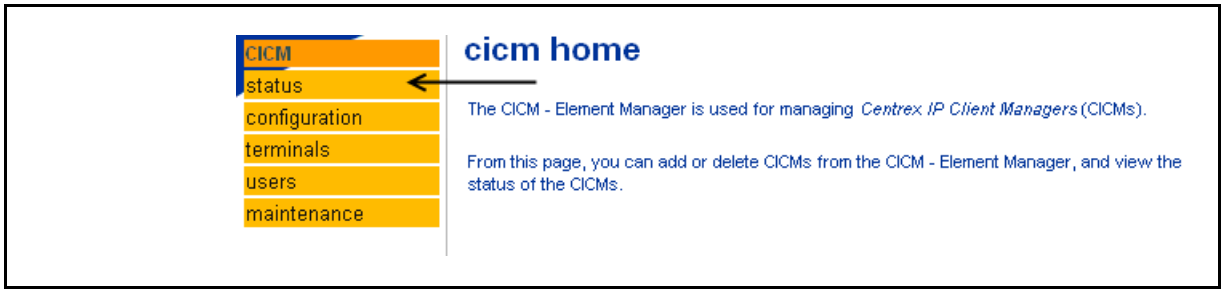
At the PC desktop for remote access to the CICM-EM

1 Access the CICM-EM of the CICM node being backed up from your PC through a web interface by entering:

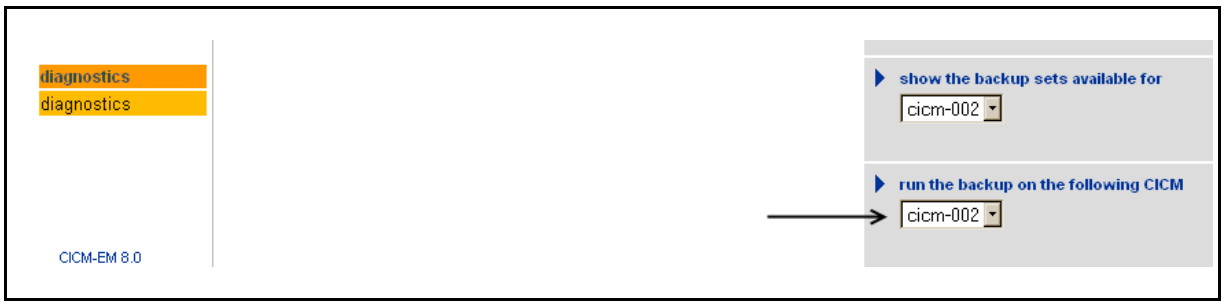
https://<unique_admin_ip_address_of_cicmem>/centrexip

At any CICM-EM web page

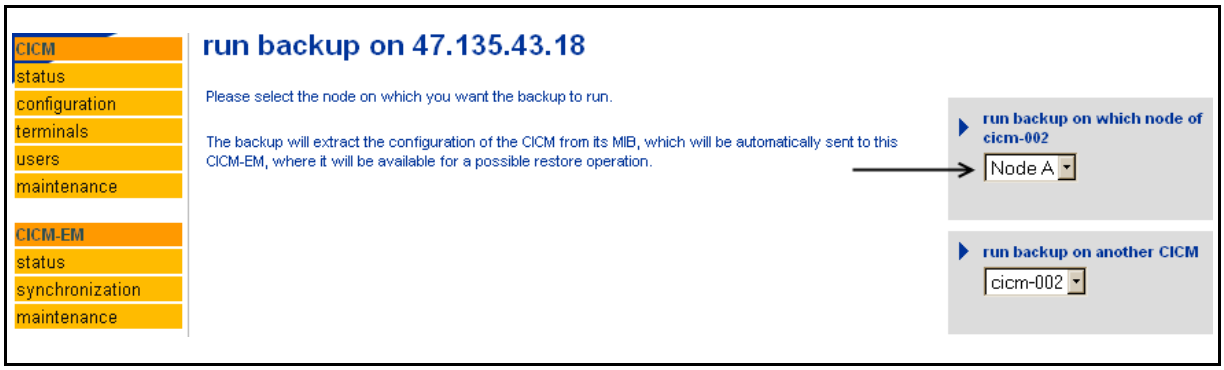
2 In the menu CICM, click on **status**.



3 Select the CICM to be backed up on the drop-down menu and click on **run the backup on the following CICM**.



4 From the pull-down menu, select the CICM *Node A* or *Node B* from which you want to run the backup.



5 Click on **run backup on which node of cicm-nnn**, where nnn echoes the node you selected.

6 Wait for this message which indicates the backup was successful:

```
The backup of the configuration for
<cicm_node_IP_addr> completed successfully.
```

7 Copy the back-up file called *backupconfig_<day_number>.xml* from the CICM-EM folder called *D:\CentrexIP\support\backups\<cicm-nnn>* to your location for storing such files, for example, in the Carrier Voice over IP (VoIP) server platform foundation (SSPS) server. The storage location must be off the CICM-EM. Use a secure FTP session (such as WinSCP) to transfer the file.

Note: Ensure that the copied back-up file ends up with the same name as the original.

8 Repeat the backing up for the mate node starting at step 3.

9 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node preparation.

Backing up a pair of CICM-EMs

Back up each node of a redundant CICM-EM pair to prepare for restoring a former software configuration when you want a more recent snap-shot than the scheduled back-up file.

Prerequisites to backing up a pair of CICM-EMs

Address the prerequisites before starting the procedure.

- Ensure that you have read and understood Backing up the CICM-EM and CICM node software configuration.
- Back up each node of a CICM-EM pair. The back-up file can only be applied to the node it was taken from.
- The back-up file name must remain the same as the copied file. Manual (on-demand) backup files have the form *EMDUMP_CICMEM-<node>_<day_number>.xml*. Scheduled backup files have the form *backupconfig_<day_number>_em.xml*, where <day_number> is the day of the month. In the procedure at step 6 you can use the scheduled back-up file instead of the manual back-up file.
- The duration of backing up varies according to the CICM-EM configuration and your access to the CICM-EM. The back-up application runs at a low level of software priority to minimize the impact on the CICM-EM.
- Backup files for CICN-EMs are stored on the CICM-EM in subdirectories at:

  d:\centrexip\support\backups\<cicmem-nnn>

- Automated daily backups are stored on alternate CICM-EM nodes.

Procedure steps to backing up a pair of CICM-EMs

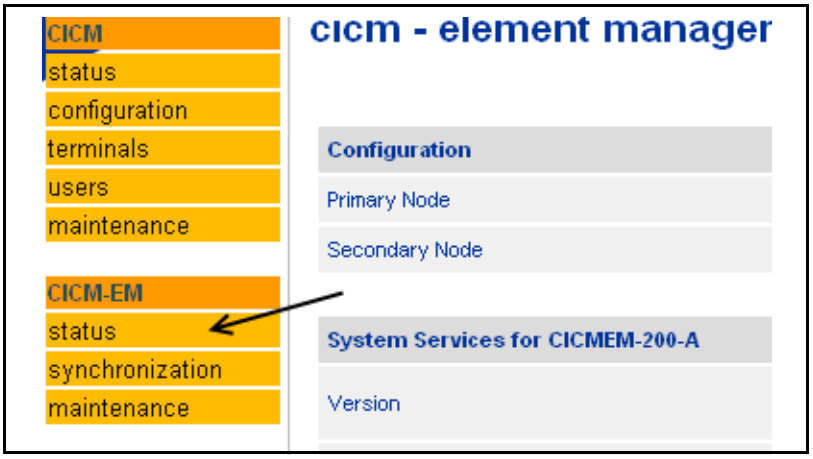
At the PC desktop for remote access to the CICM-EM

1 Access the CICM-EM that iis being backed up from your PC through a web interface by entering:

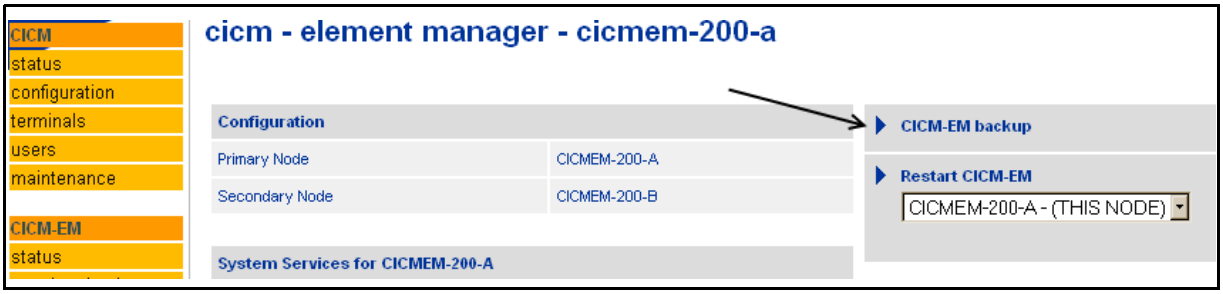
https://<unique_admin_ip_address_of_cicmem>/centrexip

At any CICM-EM web page

2 In the menu CICM-EM, click on **status**.



3 Click on **CICM-EM backup** to start backing up the file.



4 From the response, record the folder path under *Creating file* and the name under *secondary file* (see the example below).

5 Wait for this message indicating a successful backup:

```
Backup of configuration data from CICMEM-<node>
is complete.
```

6 Copy the on-demand back-up file called

EMDUMP_CICMEM-<node_number>_<day_number>.xml

for example,

EMDUMP_CICMEM-200-A_TueFeb151826582005.xml

from the CICM-EM folder called

D:\CentrexIP\support\backups

to your location for storing such files, for example, in the Carrier Voice over IP (VoIP) server platform foundation (SSPS) server. The storage location must be off the CICM-EM. Use a secure FTP session (such as WinSCP) to transfer the file.

Note: Ensure that the copied back-up file ends up with the same name as the original.

7 Access the CICM-EM mate node from your PC through a web interface by entering:

https://<unique_admin_ip_address_of_mate_cicem> /centrexip

8 Repeat this procedure from step 2 to step 6 to back up the mate node.

9 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node preparation.

Copying upgrade files to and from an SPFS server

Copy the upgrade files onto a Server Foundation Platform Software (SPFS) server from a Nortel CD and then onto a redundant pair of CICM-EMs to make the files available for upgrading the CICM-EMs and their CICM nodes.

Prerequisites to copying upgrade files to and from an SPFS server

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node preparation for an upgrade.
- You must understand and be familiar with Sources of software files for CICM, especially regarding access to the upgrades source files.
- You must know the unique Administration IP addresses of each CICM-EM of the pair.
- Both CICM-EMs must be in-service to enable accepting the files.
- You must use a secured FTP (SFTP) session to copy files to or from a CICM-EM (but not from a CICM node to its EM). You are responsible for providing your own software for an SFTP, for example, WinSCP.
- An equivalent to the SPFS server can also be used, in which case, use the procedure as a guide to indicate directories and file names. For example, the SPFS login steps in the procedure will likely be different for a PC.
- Each upgrade file name ends with a file extension. Refer to Recognizing the type of source file for an upgrade.
- You need a working knowledge of UNIX.

Procedure steps to copying upgrade files to and from an SPFS server

At the UNIX-based SPFS server

1 Load the CD with the upgrade files into the CD-ROM drive.

2 Log into the SPFS server by using a secure telnet session:

ssh <ip_address_SPFS> -l <username>

3 At the prompt, confirm the RSA fingerprint is correct and when prompted, enter the user's password.

4 Become the root user by entering:

su root

5 Go to the top level directory of the CDROM by entering:

cd /cdrom/cdrom0

The last character of *cdrom0* is a zero.

6 List the files at the directory by entering:

ls -al

Refer to Recognizing the type of source file for an upgrade.

7 Go to the directory containing the upgrades files by entering, for example:

cd "Upgrade Files"

8 SFTP to the master CICM-EM and log into it by entering:

sftp Administrator@<ip_address>

where <ip_address> is the static IP address of the CICM-EM (as opposed to the floating IP address).

As logging in begins, the response is:

```
Connecting to <ip_address>...
The authenticity of host '<ip_address>
(<ip_address>) can't be established.
DSA key fingerprint is <string>
Are you sure you want to continue connecting
(yes/no)?
```

9 Confirm the prompt:

yes

Logging in continues with:

```
Warning: Permanently added '<ip_address>' (DSA)
to the list of known hosts.
Administrator@<ip_address>'s password:
```

10 Enter the Administrator password:

<admin_password>

A successful password is indicated by the command prompt for SFTP:

```
sftp>
```

11 Identify the directory you are at:

pwd

The home directory of the server is always indicated after login:

```
Remote working directory: /HOME
```

12 Go to the directory on the CICM-EM where the EM upgrade files are to be copied:

cd /firmware/elementmgrs_mrs

The command prompt for SFTP re-appears:

```
sftp>
```

13 Set the FTP mode to binary (this is the default with SFTP):

bin

14 Confirm you have reached the directory:

pwd

The directory is echoed:

```
Remote working directory:
/D:/firmware/elementmgrs_mrs
```

15 Copy each EM_ MR upgrade file to the CICM-EM directory */elementmgrs_mrs*:

put EM_<release>.cab

Example
EM_8.10.183.upg

The progression of copying is indicated by:

```
Uploading <file_name> to
/D:/firmware/elementmgrs_mrs
<file_name> <pertage_loaded> <file_size>
<loading_rate> <time>
```

16 Repeat step 15 for each other file at the directory.

17 Confirm all EM_ MR upgrade files are present:

ls -al

At this directory, obsolete CICM-EM MR .cab files from previous releases should be removed or archived elsewhere to ensure there is enough space for the new software.

18 Go to the directory on the CICM-EM where the CICM node (gateway) MR upgrade files are to be copied:

cd /firmware/gateway_mrs

The command prompt for SFTP re-appears:

```
sftp>
```

19 Confirm you have reached the directory:

pwd

The directory is echoed:

```
Remote working directory:
/D:/firmware/gateway_mrs
```

20 Copy each GW_ MR upgrade file to the CICM node directory */gateway_mrs*:

put GW_<release>.cab

The progression of copying is indicated by:

```
Uploading <file_name> to
/D:/firmware/gateway_mrs
<file_name> <pertage_loaded> <file_size>
<loading_rate> <time>
```

21 Repeat step 20 for each other file at the directory.

22 Confirm all GW_ MR upgrade files are present:

ls -al

At this directory, obsolete gateway .cab files from previous upgrades should be removed or archived elsewhere to ensure there is enough space for the new software.

23 Repeat the copying onto the second CICM-EM, starting from step 7. Use the static IP address of the second CICM-EM.

24 Repeat the copying of each additional CD with required files, starting from step 1. Repeat until all the files are copied.

25 Close the FTP session:

quit

or

bye

26 Release the CD from the server:

cd /
eject cdrom

27 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

Copying upgrade files to and from your PC

Copy the upgrade files onto your remote PC from a CD of Nortel and then onto a redundant pair of CICM-EMs to make the files available for upgrading the CICM-EMs and their CICM nodes.

Prerequisites to copying upgrade files to and from your PC

Address the prerequisites before starting the procedure.

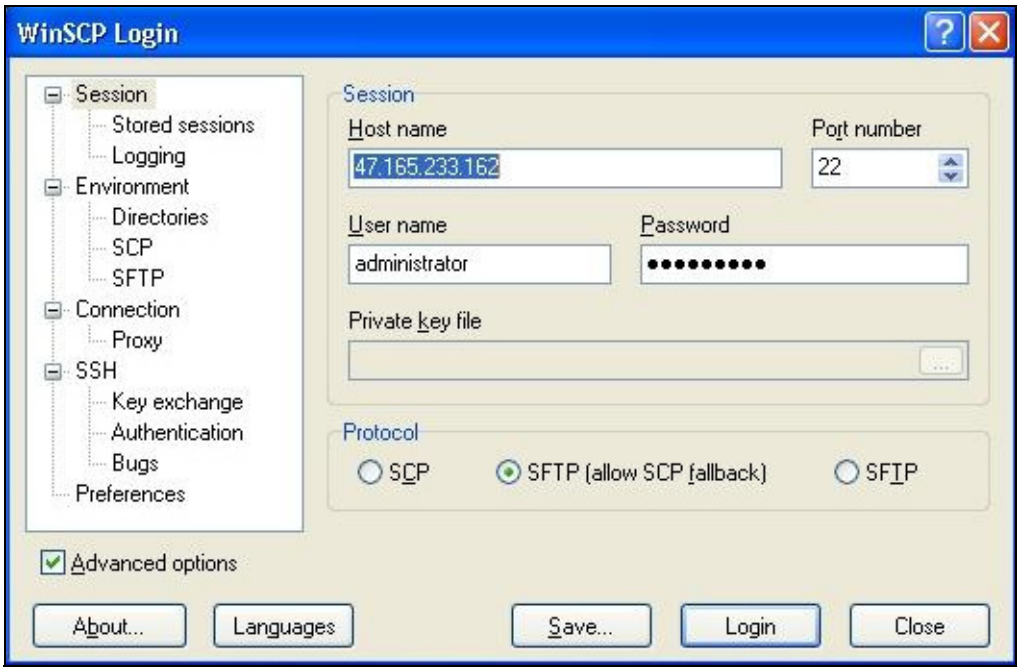
- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node preparation for an upgrade.
- Understand Sources of software files for CICM, especially regarding access to the upgrades source files.
- You must know the unique Administration IP addresses of each CICM-EM of the pair.
- Both CICM-EMs must be in-service to enable accepting the files.
- You must use a secured FTP (SFTP) session to copy files to or from a CICM-EM (but not from a CICM node to its EM). You are responsible for providing your own software for an SFTP, for example, WinSCP.
- Each upgrade file name ends with a file extension. Refer to Recognizing the type of source file for an upgrade.
- The specifications of hardware and software for your personal computer (PC) must comply with the criteria identified in *CICM Basics*, NN10044-111.
- A PC is remote in context of not necessarily being located on the same site as the SAM16 or SAM21 hardware that runs the CICM software.
- You need a working knowledge of secure FTP and Microsoft Windows. The procedure uses WinSCP software as an example of a secure FTP.

Procedure steps to copying upgrade files to and from your PC

At your remote PC

1. Create folders on your PC to copy the source files into. For simpler file management create separate folders for CICM-EMs and CICM nodes. Within those folders, the file names distinguish which files are for CICM-EMs or CICM nodes. Do not rename the files.
2. Access the source files of the upgrade files by inserting the Nortel CD of upgrade files into your PC's CD-ROM and opening the folders.

3 Start a Secure FTP (SFTP) session on the CICM-EM that is to receive copies of the files. For example, on your PC Desktop double-click the icon for the WinSCP application.



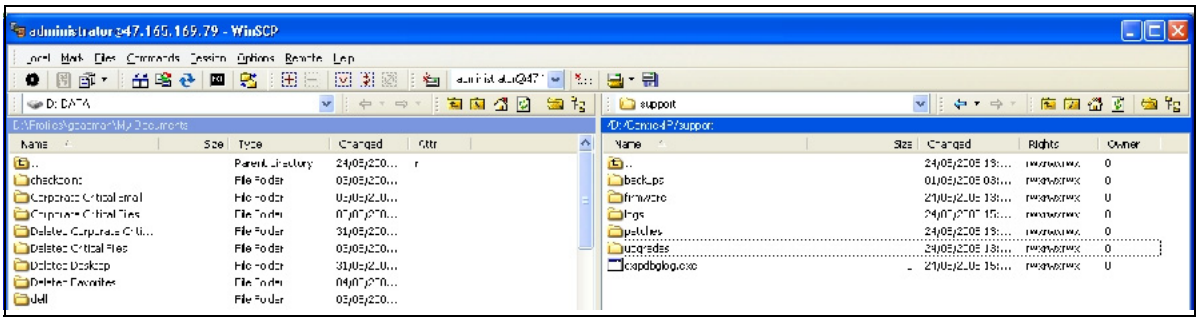
4 Navigate from the remote directory to the directory on the CICM-EM where the upgrade files are to be copied.

The directories for the CICM-EM upgrade files are:

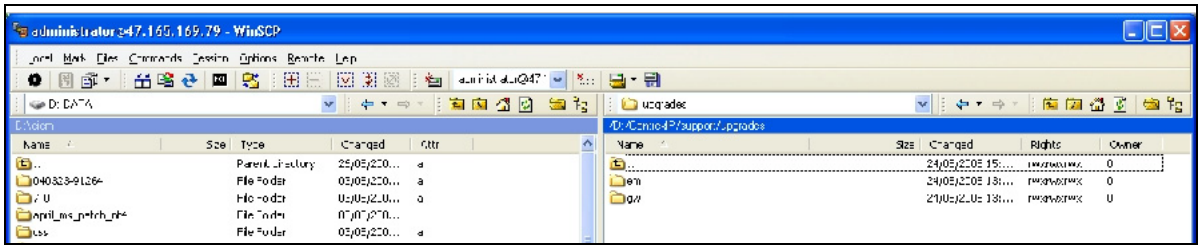
d:\firmware\elementmgrs_mrs

The directories for the CICM node upgrade files are:

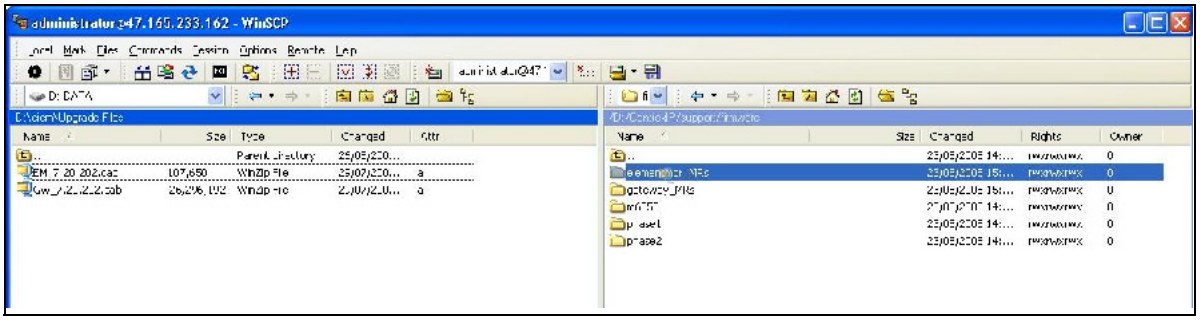
d:\firmware\agteway_mrs



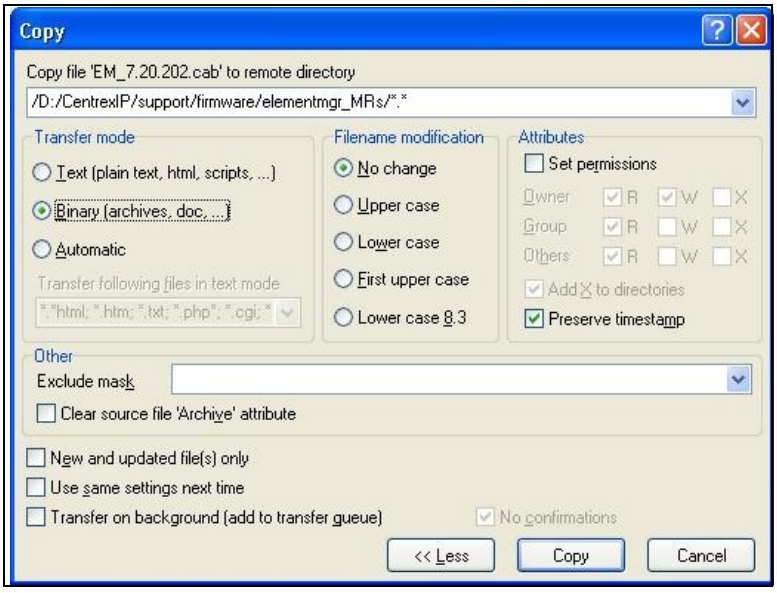
5 Open a local directory.



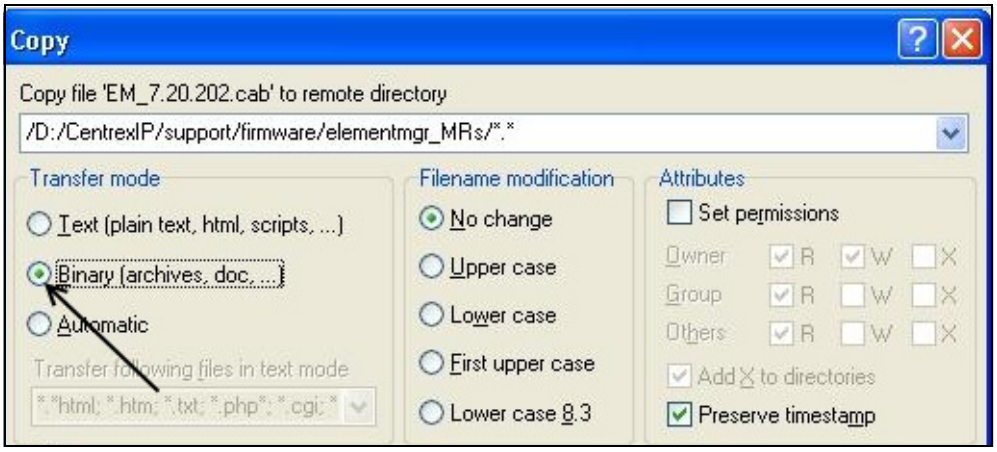
6 Drag each file from the local PC directory to the appropriate CICM-EM or CICM node remote directory. Refer to Recognizing the type of source file for an upgrade.



The box *Copy* appears.

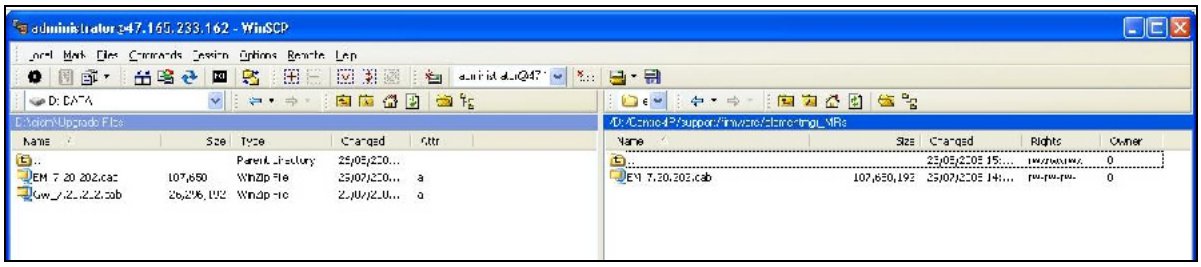


7 Since the upgrade files are executable files, ensure that the transfer mode is set to binary.



8 Press enter to copy the files.

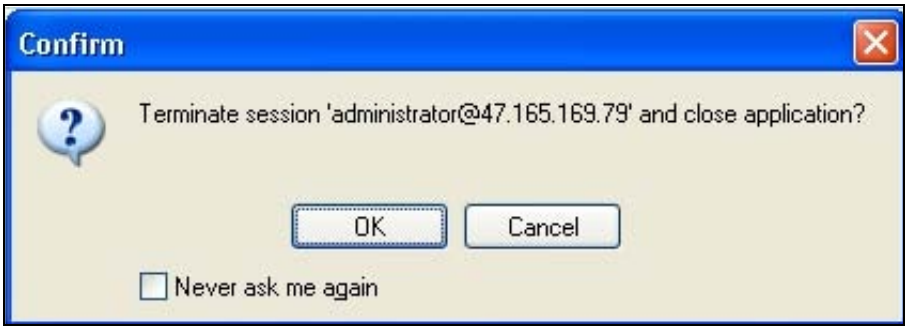
9 Refresh the directory display and confirm that all files have been copied.



10 Repeat from step 4 to step 9 to copy all upgrade files to each appropriate CICM-EM directory.

11 When all upgrades files are copied to the first CICM-EM, repeat step 10 for the mate CICM-EM.

12 Quit the SFTP session. For WinSCP, click the upper right-hand X of the window and click **OK** of the confirmation prompt.



13 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

Switching activity between CICM nodes

Switch the activity from the master CICM node to the slave node of the redundant pair.

Prerequisites to switching activity between CICM nodes

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node preparation for an upgrade.
- Both CICM nodes must be in-service to enable the switch of activity (SWACT) to occur.
- After the upgrade and before the SWACT, Node A is the slave with status running and with no terminals connected to it.
- When upgrading with an MR for SN08 or later, the CICM terminals are automatically transferred during the switch of activity.
- If you did step 15 in the procedure Upgrading a CICM node with an MR to enable testing calls, then do not repeat this procedure to upgrade the mate node. The mate node is already the slave.

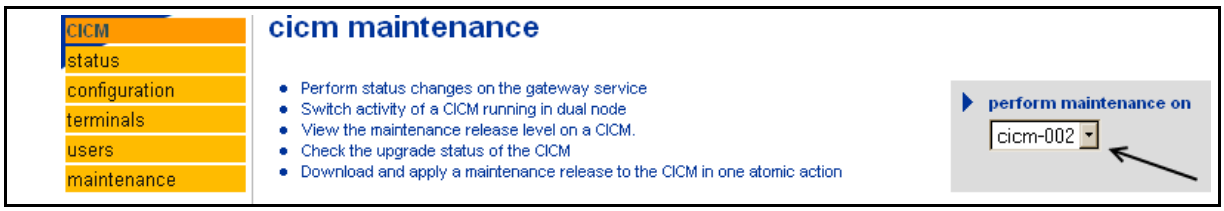
Procedure steps to switching activity between CICM nodes

At any CICM web page

1 In the menu *CICM*, click **maintenance**.

At the page cicm maintenance

2 From the pick-list under **perform maintenance on**, select the CICM node identifier.



3 Click **perform maintenance on**.

4 Observe from the *Node Maintenance status* of each node which ones are master and slave.

5 Click **switch activity**.

The duration of the switchover varies according to the number of users configured on the nodes and the volume of calls being sustained in the node at the time of the SWACT.

When both nodes are not available for a SWACT, the command button is tinted grey and disabled. Ensure that both nodes are in service.

6 Click **confirm switch of activity**.

7 Confirm from the *Node Maintenance status* whether the master and slave have switched successfully:

- the *Node status* is *master*
- the *Node Maintenance status* is *system idle*

If not, then contact your next level of support to determine why.

8 This procedure is complete.

When this procedure was invoked for applying an MR or a product release, return to the task flow Task flow of CICM-EM and CICM node preparation or the step in the procedure Upgrading a CICM node with a product release from where you came:

- step 4 (before applying the upgrade file)
- step 18 (after applying the upgrade file)

Otherwise, return to the task flow or the step in the procedure that sent you to this one.

Transferring terminals for an upgrade

Transfer the terminals (clients) from one CICM node to another to ensure that service is maintained or can be restored.

Prerequisites to transferring terminals for an upgrade

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node preparation for an upgrade.
- When upgrading from SN07 to SN08 or later and Node A is already upgraded, transferring terminals from Node B to Node A means the command **terminal transfer** can only be found at the page *maintenance release*. When both CICM nodes have SN08 or later, the command **terminal transfer** no longer appears.
- When upgrading from SN07, a transfer of terminals must be done manually, as indicated in the procedure. A transfer process:
  - transfers terminals that are not in-call (handling a call)
  - notifies the users of in-call terminals that a maintenance activity is pending and asks them to terminate their session as soon as possible
  - after a telco-defined timeout period, forces the in-call terminals to transfer (thereby dropping all calls in progress)
- Have a working CICM terminal (for example, an m6350 or IP Phone 200x) available to test the operation of an upgraded node.
- The section “Terminal transfers” and the procedure “Perform a terminal transfer” have additional information in *CICM Security and Administration*, NN10252-611.

Procedure steps to transferring terminals for an upgrade

At the page CICM maintenance status (cicm-nnn)

1 On the right menu, ensure that **start auto refresh** is showing, but do not click on it.

If **stop auto refresh** is shown, click it to show **start auto refresh**.

2 When upgrading the first CICM node, which is always node A, transfer its terminals to the mate by clicking **from node A to node B** at the Node pick-list.

When upgrading the second CICM node, which is always node B, transfer its terminals to the mate by clicking **from node B to node A**.

3 From the pick-list *Terminal Shutdown Timeout*, select the minutes. The minutes are to allow CICM clients time to log off themselves before they are automatically dropped by the transfer.

4 Click **transfer terminals**.

5 When the confirmation screen appears, click **confirm terminal transfer**.

The terminal transfer will commence immediately upon confirmation, and will terminate when the selected timeout interval has expired.

6 Click **start auto refresh** on the page *maintenance status (cicm-nnn)*.

The button **stop auto refresh** appears.

During a transfer when Node A has SN08 or later and Node B has SN07, the statuses shown for *Terminal service* (SN07) and *Terminal status* (SN08 or later) indicate temporary transitional hybrid combinations. Since terminal transfers are handled differently between SN07 and SN08 and later, ignore the transitional terminal statuses.

7

CAUTION
Risk of service interruption
Wait until the terminal transfer has completed before proceeding. If the transfer does not complete, discontinue the procedure and contact your next level of technical support to determine your next actions.

When the terminals have transferred, all should be hosted on CICM Node A. Completion of the transfer is indicated by *stopped* or *inactive* or appearing for *Terminal service* (SN07) or *Terminal status* (SN08 or later).

8 This procedure is complete. Return to the step in the procedure Upgrading a CICM node with a product release from where you came:

- step 6 (before applying the upgrade file)
- step 20 (after applying the upgrade file)

Upgrading a CICM node with a product release

Upgrade the CICM slave node with a product release as part of upgrading all CICM components in a network.

Prerequisites to upgrading a CICM node with a product release

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node preparation for an upgrade.
- When upgrading from SN07, you must determine the new unique static UNIStim IP address for Node A.
- Both CICM nodes must be in service before attempting the upgrade.
- You must know the administrator userid and password to log into the CICM-EM from a remote PC for this upgrade.
- During the upgrade to a CICM node, the node restarts several times.
- When upgrading from SN07, at the CICM-EM maintenance page when the status field of the node indicates `awaiting external step`, refer to the debug logs for details about what to do next.
- A CICM node fails an upgrade when it does not return to service and the version of the upgrade does not appear beside the Version status. Before re-attempting to upgrade the node, you must determine from the debug logs why it failed. If the upgrade was aborted, it will return to a pre-upgrade idle state with the previous software. If the upgrade was started and failed, you will need to roll back from the upgrade to restore service.
- Always upgrade node A first. A node must be the slave before it can be upgraded. When Node A is the master, it must be made the slave as indicated in the procedure.

CAUTION
Risk of service outage
It is critical to upgrade Node A first since the upgrade results in the use of Node A's pre-upgrade (SN07) static UNIStim address as the floating UNIStim address for the post-upgrade (SN08 or later) operation.

Procedure steps to upgrading a CICM node with a product release

At the page CICM home through the web interface

1 When upgrading the second CICM node of a redundant pair, start this procedure from step 22. Do not repeat the procedure a third time for the same upgrade to the same pair of nodes.

At the PC desktop for remote access to the CICM node

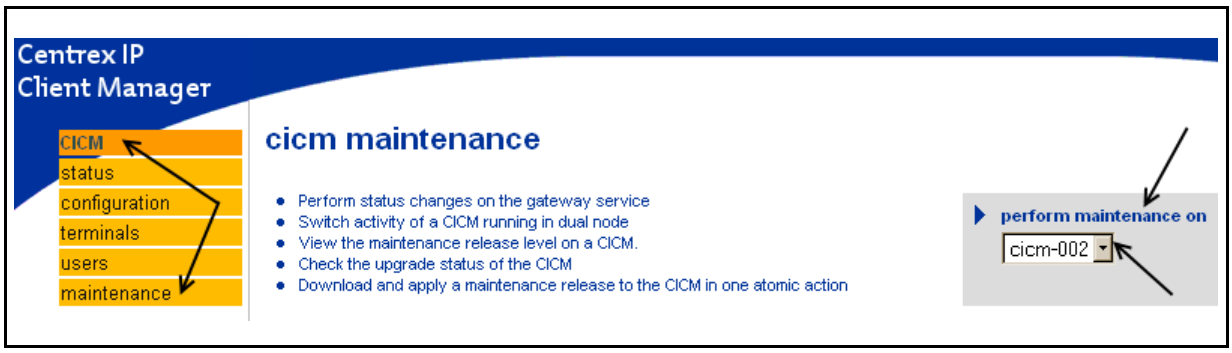
2 Access the CICM node from your PC through a web interface by entering:

https://<unique_admin_ip_address_of_cicmem>/centrexip

At the page welcome to the CICM

3 In the menu *CICM*, click **maintenance**.

The page *cicm maintenance* opens.



At the page cicm maintenance

4 From the pick-list under **perform maintenance on**, select the CICM node to upgrade.

When you select the node other than the one that is showing, the page *maintenance status* automatically opens.

When the displayed Node is the slave, click **perform maintenance on**.

The page *maintenance status* opens.

5 From the display *Node Maintenance Status*, determine the statuses of Nodes A and B.

When upgrading Node A, Node B must be the master. When Node A is the master, do the procedure Switching activity between CICM nodes and return to this step.

When upgrading Node B, Node A must be the master. When Node B is the master, do the procedure Switching activity between CICM nodes and return to this step.

At the page cicm maintenance status (cicm-nnn)

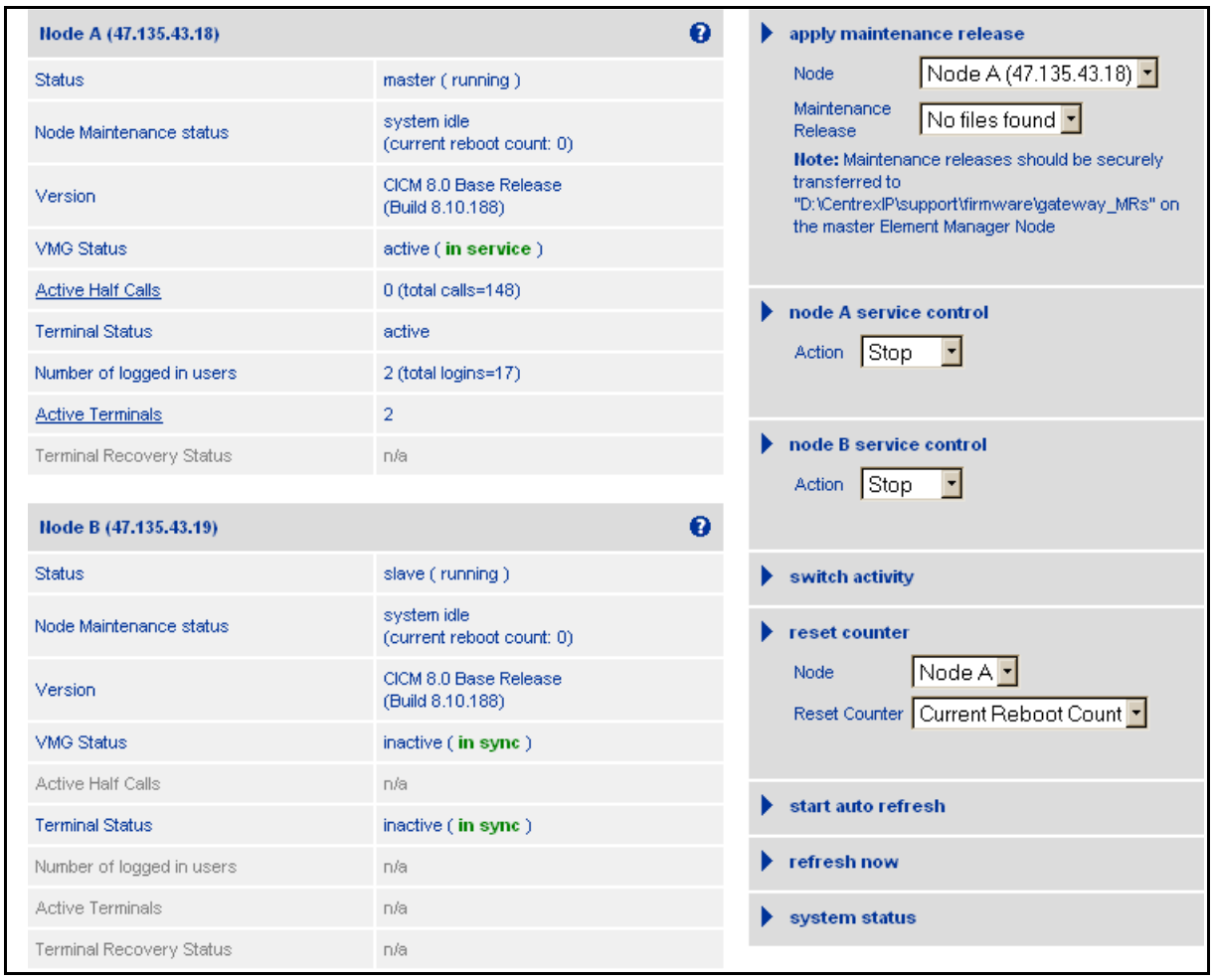
6 When upgrading the first or second CICM node of a redundant pair from SN07, transfer all terminals from the node being upgraded to its mate using the procedure Transferring terminals for an upgrade.

When upgrading from SN08 and later, terminals are automatically transferred.

7 On the right menu, ensure that *start auto refresh* is showing, but do not click it.

If **stop auto refresh** is shown, click it to show **start auto refresh**.

8 From the pick-list under **apply maintenance release** beside *Nodes*, select **Node A** or **Node B**, whichever is the slave.



9 From the pick-list beside *Maintenance Release*, select the appropriate upgrade file. Refer to Recognizing the type of source file for an upgrade.

When *No files found* is showing, the upgrades files have not been copied to the CICM-EM or were copied to the wrong directory. You have not followed the task flow.

10 Click **apply maintenance release**.

11 Confirm applying the upgrade by clicking **confirm maintenance release application**.

12 Wait 10 seconds then track the progress of the upgrade to the slave CICM node by clicking **start auto refresh**.

13 Monitor Node A (or B) as it goes through a series of restarts as part of the upgrade process.

When upgrading from SN07 and the status of the node indicates `awaiting external step`, refer to the debug logs for details about what to do next.

At the PC desktop for remote access to the CICM node

14

CAUTION
Risk of service prevention
Take extreme care when entering preboot data. Errors may result in unexpected and undesirable behavior when the node later attempts to return to service.

Telnet to the admin IP address of the node being upgraded to enter the following commands.

Note: Preboot will collect a new static UNIStim IP address for one on Node A. This step will modify the routing tables to match the required new configuration.

a At the CLI prompt (shown as *C:\temp>*), enter the command **preboot**, for example: **preboot/upgrade**

b Enter the floating UNIStim IP address for this CICM, for example: 47.165.76.180.

Note: When upgrading from SN07, the floating UNIStim address must be identical to the existing static UNIStim address of Node A. You must use the existing 7.xx Node A

static UNIStim IP address as the new 8.xx or later floating UNIStim IP address.

c Enter the new static UNIStim IP address for Node A, for example: 47.165.76.181

d Enter the existing static UNIStim IP address for Node B, for example: 47.165.76.185

e Enter the existing network mask for the UNIStim IP network, for example: 255.255.255.0

f Enter the existing default route for the UNIStim IP network, for example: 47.165.76.1

or for *no route* (for the clients to communicate only within the same subnet instead of to the gateway), enter: **0.0.0.0**

Enter a no route only if you do not have a default and you understand the consequences of not having one.

```
[SC] ChangeServiceConfig SUCCESS
The DHCP Client service is starting.
The DHCP Client service was started
successfully.

Applying IP Address and Subnet Mask: The
ReturnValue is 96 (4 byte int)
The DHCP Client service is stopping.
The DHCP Client service was stopped
successfully.

[SC] ChangeServiceConfig SUCCESS

Correcting H248 routing...
Deleting old defunct routes...
Marking the upgrade step as run...
Preboot /upgrade completed successfully.
```

15 At the last step to the **preboot**, you will receive a prompt to restart the node to complete the upgrade. Enter **Y** to confirm.

16 Wait for the reboot to occur. The duration depends upon the number of configured users for the CICM node.

After the reboot, the final changes will be applied to the node, then the node will be brought into service as a CICM slave running the new release.

At the page maintenance status (cicm-nnn)

17 Monitor the status of Node A until it is running as slave before proceeding.

> ***Note:*** When upgrading from SN07 and Node A is the slave, it is bound to its new static UNIStim IP address but not the floating UNIStim IP address. At this point in an upgrade, terminals cannot be connected to Node A while it is a slave. When upgrading from SN08 and later, the floating address is always bound to the master node.

At this point you can choose to roll back the upgrade as described in “CICM-EM or CICM node rollbacks” with no SWACT and no terminal transfers.

18 Do the procedure Switching activity between CICM nodes.

When upgrading from SN07, following the switch of activity (SWACT), Node A becomes the master and is bound to the UNIStim floating address. Node B continues to be running version 7.xx, so it continues to be bound to its static UNIStim address.

19 Verify that Node A is working properly, which means:

- the *Node status* is *master*
- the *Node Maintenance status* is *system idle*
- the Version is *w.xx.yyy* of the target upgrade version, for example, 8.10.183

If Node A is not working properly, you must discontinue this procedure and follow the rollback path indicated in the task flow “CICM-EM or CICM node rollbacks”.

At this point you can choose to roll back the upgrade as described in “CICM-EM or CICM node rollbacks” with a SWACT and no terminal transfers.

20 When upgrading from SN07, prior to upgrading the second CICM node of a redundant pair, transfer all terminals from the node being upgraded to its mate using the procedure Transferring terminals for an upgrade.

When upgrading from SN08 and later, terminals are automatically transferred.

21

CAUTION
Risk of service prevention
This is the last chance to roll back a node. Once an upgrade to the second node is attempted, a rollback then becomes a re-installation of the base software and upgrades for each node. Nortel' GNPS must be requested to do the re-installation.

At this point you can choose to roll back the upgrade as described in the task flow "CICM-EM or CICM node rollbacks" with a SWACT and terminal transfers.

22 When upgrading from SN07, with Node B in slave mode and hosting no terminals, begin the upgrade of Node B by repeating step 8 to step 16 and then do Switching activity between CICM nodes.

When upgrading from SN08 and later, with Node B in slave mode and hosting no terminals, begin the upgrade of Node B by repeating step 8 to step 13 and then do Switching activity between CICM nodes.

Note: While Node B is starting, you can monitor its status. On start-up of the slave node, there is a delay before the load achieves a state of synchronization with the master. Only when this data synchronization is achieved is it possible to initiate a switch of activity.

23 Verify that Node B is working properly, which means:

- the *Node status* is *master*
- the *Node Maintenance status* is *system idle*
- the Version is *w.xx.yyy* of the target upgrade version, for example, 8.10.183

If Node B is not working properly, you must contact your next higher level of technical support to determine what to do next.

The command button for **terminal transfer** is no longer present.

At the IEMS interface

24 Edit the object properties in the IEMS for the CICM network elements you just upgraded to reflect the new software version.

Refer to either of the procedures that follow to update the software version in the field *Device Version*:

- Editing and viewing object properties using Java Web Client on page 1841
- Editing and viewing object properties using Web Client on page 1846

With the Java Web Client, CICM uses *v2c* for the *Version* in the *SNMP Details* page.

25 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

Also address After an upgrade from CICM SN07 to SN08 or later. These are to be done as part of the upgrade, but independently from the task flow.

After an upgrade from CICM SN07 to SN08 or later

After the CICM upgrade from SN07 to SN08 or later has been completed, address the following.

- Node B's static UNIStim address is no longer valid for use by terminals in the network. Once the upgrade is complete, it is recommended that the operator take the necessary steps to update all terminals in their network so that they do not attempt to contact the CICM on this (now) invalid address.

  If using DHCP, its configuration must be changed. Refer to DHCP documentation for information on configuration DHCP servers.
- Leaving terminals configured with the old B UNIStim address will not cause harm to the network. However, it can cause individual terminals to take longer to locate the CICM following a terminal reboot, since it can use the invalid address for its search.
- If a survivable remote gateway (SRG) is to be deployed, this can safely be done once the CICM has been upgraded. In doing so, the terminal must be reconfigured such that S1 is set to the CICM's floating UNIStim address, and S2 is set to the SRG's address. These must not be reversed. The SRG uses S2.
- For those terminals in the network not serviced by an SRG, it is recommended that both their S1 and S2 entries be set to the CICM's floating UNIStim address.

Upgrading a CICM node with an MR

Upgrade a CICM node with a maintenance release (MR) upgrade to CICM nodes already running the same software release (for example, both have release 8.10 MR2).

Prerequisites to upgrading a CICM node with an MR

Address the prerequisites before starting the procedure.

- For MR zero (MR0), you must follow instead the procedure Upgrading a CICM node with a product release.
- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node preparation for an upgrade.
- Both nodes of a CICM pair must operate with the same version of software prior to and after the upgrade. Operating within three MRs applies only during the transition of upgrading two nodes one at a time. The nodes are updated one at a time using the same procedure as indicated by the task flow.
- Always upgrade the slave node first and one node at a time.
- Both CICM nodes must be in service for an upgrade to complete successfully.
- You must know the administrator userid and password to log into the CICM-EM for this upgrade.
- Terminals connected to the node being upgraded will maintain service while they locate the mate node.
- Active calls using resources on the node being upgraded are maintained.
- When the system detects an invalid software release or corrupt file for an upgrade, the CICM node does not apply the upgrade and will resume activity at its current software release.
- A CICM node fails an upgrade when it does not return to service and the version of the upgrade does not appear beside the Version status. Before re-attempting to upgrade the node, you must determine from the debug logs why it failed. If the upgrade was aborted, it will return to a pre-upgrade idle state with the previous software. If the upgrade was started and failed, you will need to roll back from the upgrade to restore service.

Procedure steps to upgrading a CICM node with an MR

At the page CICM home through the web interface

1 When upgrading the second CICM node of a redundant pair, start this procedure from step 4. Do not repeat the procedure a third time for the same upgrade to the same pair of nodes.

At the PC desktop for remote access to the CICM

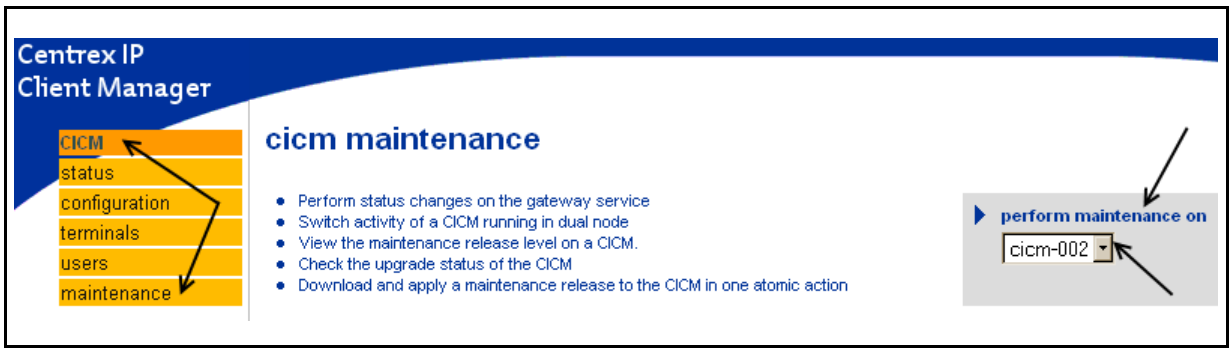
2 Access the CICM node from your PC through a web interface by entering:

https://<unique_admin_ip_address_of_cicmem>/centrexip

At any CICM web page through the web interface

3 In the menu *CICM*, click **maintenance**.

The page *cicm maintenance* opens.



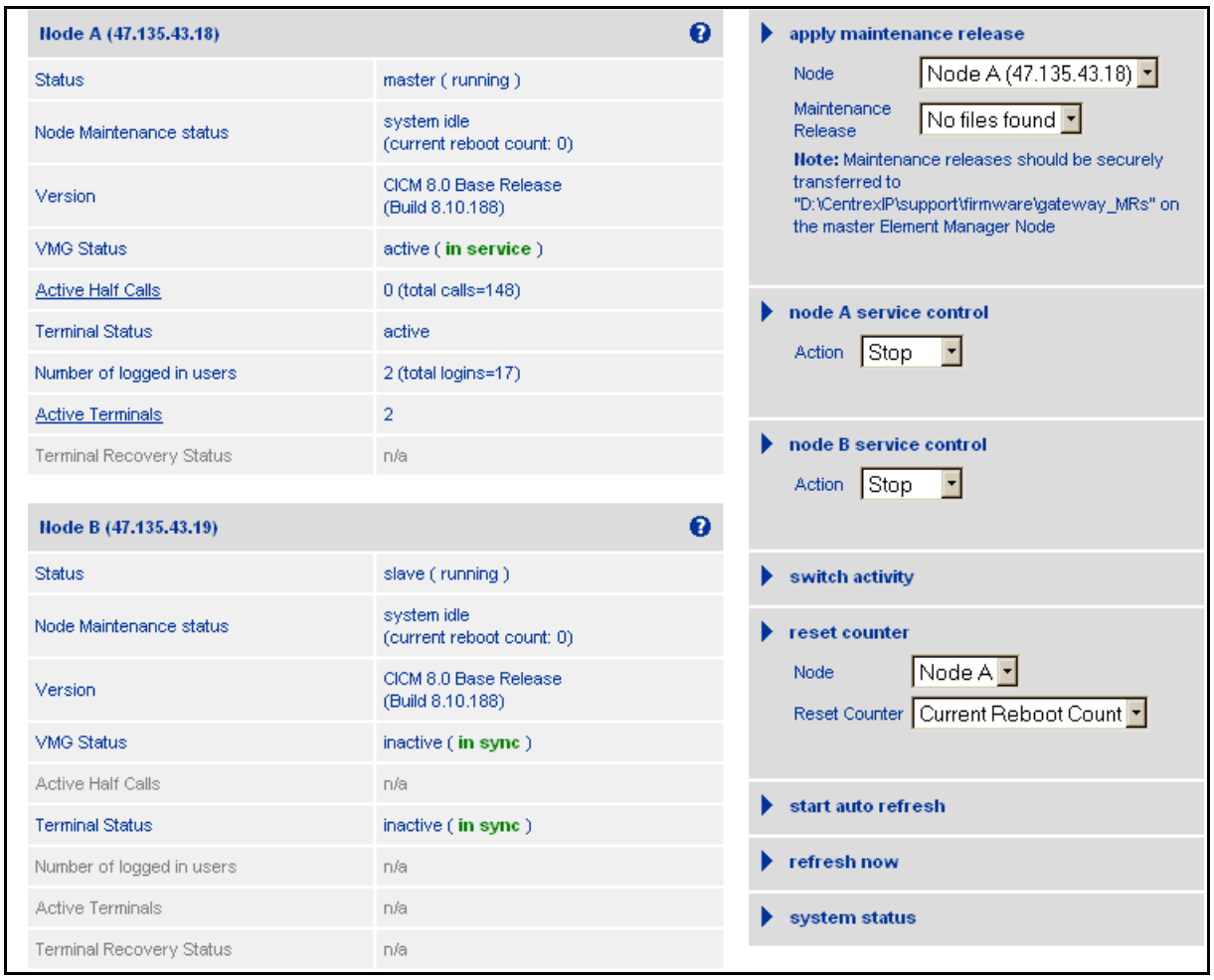
4 From the pick-list under **perform maintenance on**, select the CICM node to upgrade.

When you select the node other than the one that is showing, the page *maintenance status* automatically opens.

When the displayed Node is already the slave, click **perform maintenance on**.

The page *maintenance status (cicm-nnn)* opens. The current software version for each node is displayed.

The display *Node maintenance status* indicates 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, it displays *system idle* or *system running*.



At the page maintenance status (cicm-nnn)

5 Ensure that **start auto refresh** is showing. If **stop auto refresh** is displayed, click it. Stopping the auto refresh will stabilize the pick-lists used.

6 From the pick-list of *Node* under **apply maintenance release**, select **Node A** or **Node B**, whichever is the slave.

7 From the pick-list beside *Maintenance Release*, select the appropriate upgrade file. Refer to Recognizing the type of source file for an upgrade.

When *No files found* is showing, the upgrades files have not been copied to the CICM-EM or were copied to the wrong directory. You have not followed the task flow.

8 Click **apply maintenance release**.

9 Confirm applying the upgrade by clicking **confirm maintenance release application**.

10 Wait 10 seconds, then to aid in monitoring the progress of the update, click **start auto refresh** for a periodic automatic refresh of the status pages.

To stop automatic refresh when monitoring is complete, click **stop auto refresh**.

The auto refresh option toggles between start and stop.

11 To monitor the progress of the upgrade, click **system status**.

The page *<cicm-nnn> cicm status* opens and displays the status details of the CICM.

At the page <cicm-nnn> cicm status

12 Monitor the <cicm-nnn> status until *Service* shows *running*.

A manual restart of the node is not required.

13 Upon successful completion of the upgrade, click **perform maintenance on <cicm-nnn>** to return to the maintenance status.

At the page maintenance status (cicm-nnn)

14 Check the new CICM node version as displayed beside *Version* of the Node A and B status.

15 To enable performing test calls, use the procedure Switching activity between CICM nodes to make the new MR active.

16 Perform test calls on the upgraded node to verify that the upgraded node is working.

If calls cannot occur on the first upgraded node, you must roll back the upgrade as described in the task flow “CICM-EM or CICM node rollbacks”.

17

CAUTION
Risk of service prevention
After upgrading the first CICM node, this is the last chance to roll back the upgrade. Once an upgrade to the second node is attempted, a rollback then becomes a re-installation of the base software and upgrades for each node. Nortel’ GNPS must be requested to do the re-installation.

If the tests pass for the first upgraded node, you can choose to roll back the upgrade as described in the task flow “CICM-EM or CICM node rollbacks”.

At the IEMS interface

18 Edit the object properties in the IEMS for the CICM network elements you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the field *Device Version*:

- Editing and viewing object properties using Java Web Client on page 1841
- Editing and viewing object properties using Web Client on page 1846

With the Java Web Client, CICM uses *v2c* for the *Version* in the *SNMP Details* page.

19 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

Upgrading a CICM-EM with an MR or product release

Upgrade a CICM element manager (CICM-EM) of a redundant pair with a maintenance release (MRx) or a product release (MR0).

Prerequisites to upgrading the CICM-EM with an MR or a product release

Prerequisites to upgrading the CICM-EM with an MR or a product release include the following.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node preparation for an upgrade. The first occurrence of a procedure is for the slave CICM-EM, and the second occurrence is for the master after it becomes the slave.
- The CICM-EM node-pair can support CICM node-pairs running either the same version or one previous version (for example, the EMs running 8.0 while a pair of nodes run 7.0 or 8.0).
- You need a PC or equivalent to remotely access the CICM-EM web pages. Upgrading is not done locally to a CICM-EM.
- Both CICM-EMs must be in service before attempting the upgrade.
- You must know the administrator userid and password to log into the CICM-EM for this upgrade.
- A failed CICM-EM upgrade is indicated by one of the following.
  - The upgrade aborts and the system stays at the pre-upgrade idle state.
  - The upgraded CICM-EM hangs and remains out of service.

  Review debug logs to determine why the failure occurred.

CAUTION
Risk of service prevention
Before upgrading the first CICM-EM of a redundant pair to a different version of software, both must be running the same software version, including the same MR incremental version. For example, version 8.10.001 is the same release as 8.10.200 but not the same version.

Procedure steps to upgrading the CICM-EM with an MR or a product release

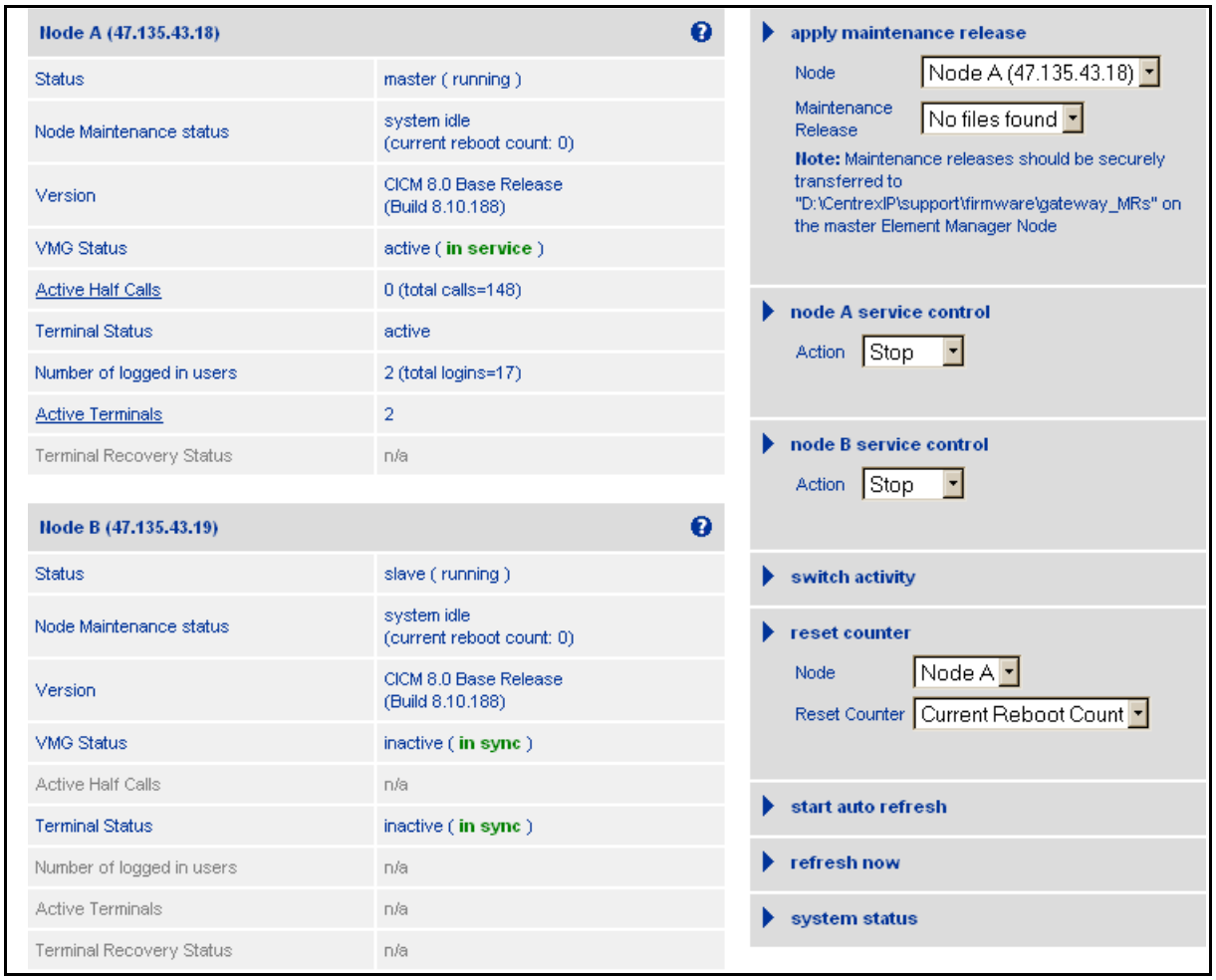
At the PC desktop for remote access to the CICM-EM

1 Access the CICM-EM from your PC through a web interface by entering:

https://<floating_http_ip_address_of_cicmem>/centrexip

At the page maintenance status (cicmem-nnn)

2 Identify from the display Node status whether Node A or B is the slave CICM-EM.



3 From the pick-list of *Node* under **apply maintenance release**, select **Node A** or **Node B**, whichever is the slave.

4 From the pick-list beside *Maintenance Release*, select the appropriate upgrade file. Refer to Recognizing the type of source file for an upgrade.

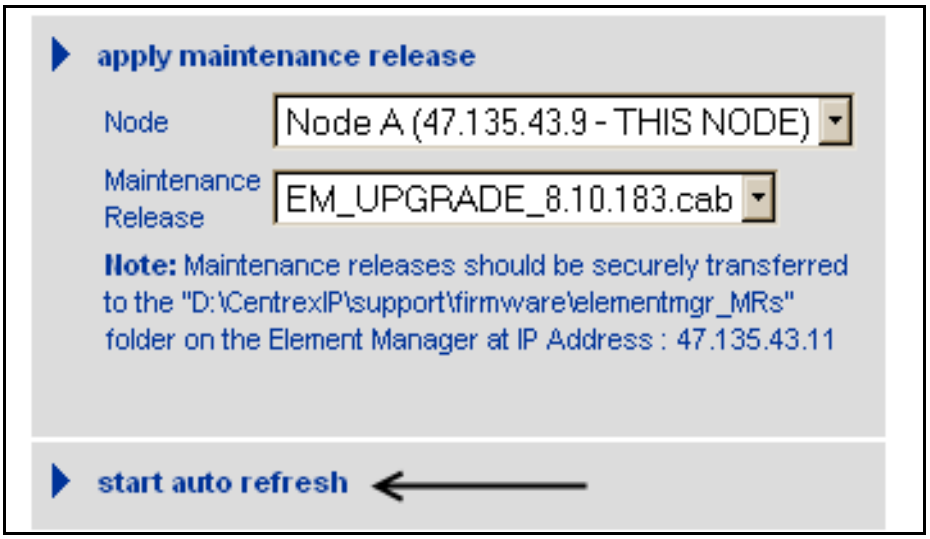
When *No files found* is showing, the upgrades files have not been copied to the CICM-EM or were copied to the wrong directory. You have not followed the task flow.

5 Click **apply maintenance release**.

6 Confirm applying the upgrade by clicking **confirm maintenance release application**.

At the page maintenance release management (cicmem-nnn)

7 Wait 10 seconds then track the progress of the upgrade to the slave EM by clicking **start auto refresh**.



The refresh button toggles to show **stop auto refresh**.

8 Wait until the CICM-EM being upgraded shows the following combination:

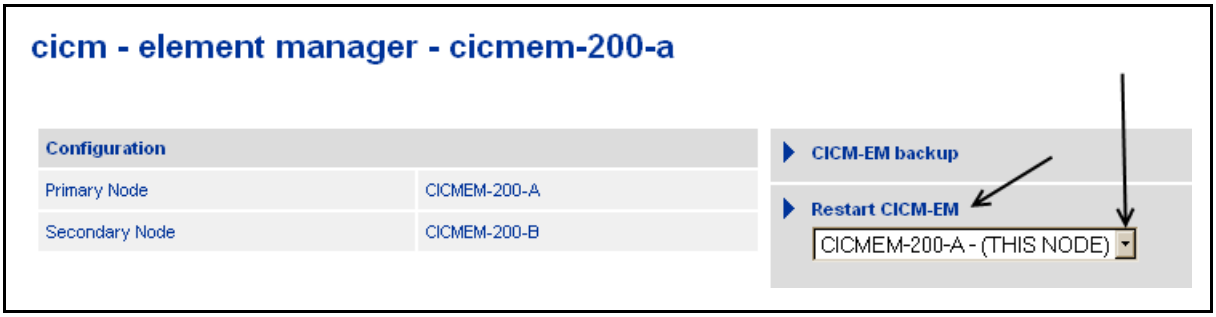
- the *Node Maintenance status* is *system idle*
- the Version is *w.xx.yyy* of the target upgrade version, for example, 8.10.183

If the EM is not in service and idle within 30 minutes, abort the upgrade. Review the debug logs to determine the cause of failure. Refer to the task flow in Task flow of CICM-EM and CICM node preparation for the procedures to roll back from an upgrade.

At the page status (cicmem-nnn)

9 Switch activity between the CICM-EM pair by restarting the active node. From the pick-list under **Restart CICM EM**, select the active mate node.

Click **Restart CICM EM**.



The page changes to show the confirmation prompt.

10 Click **Confirm restart of CICM-EM (CICMEM-nnn-x)** where x is the node A or B you selected.

Monitor the progress of the restart by clicking **maintenance** in the menu CICM-EM.

11

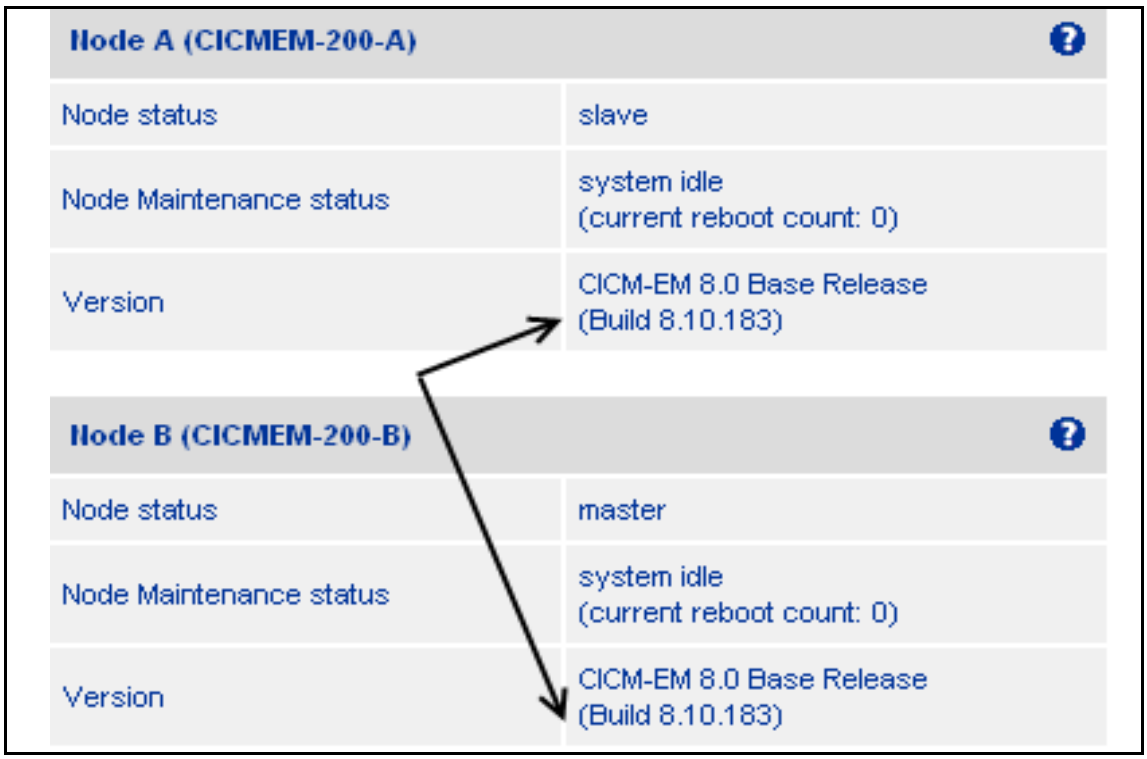
CAUTION
Risk of service prevention
Do not repeat step 3 when both CICM-EMs have been upgraded.

Upgrade the master CICM-EM by repeating the procedure from step 3. Do not repeat this step when both EMs have been upgraded.

12 Wait until the second CICM-EM of the redundant pair being upgraded shows it is in service (*system idle* or *system running*).

If the second EM fails the upgrade, refer to the rollback task flow in Task flow of CICM-EM and CICM node preparation.

13 When both EMs of a redundant pair are in service and running with identical versions of software (for example, 8.10.183), the upgrade is complete.



At the IEMS interface

14 Edit the object properties in the IEMS for the CICM network elements you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the field *Device Version*:

- Editing and viewing object properties using Java Web Client on page 1841
- Editing and viewing object properties using Web Client on page 1846

With the Java Web Client, CICM uses *v2c* for the *Version* in the *SNMP Details* page.

15 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

Verifying the software version of the CICM-EM and CICM nodes

Verify the software version of a CICM-EM and its CICM nodes.

Prerequisites to verifying the software version of the CICM-EM and CICM nodes

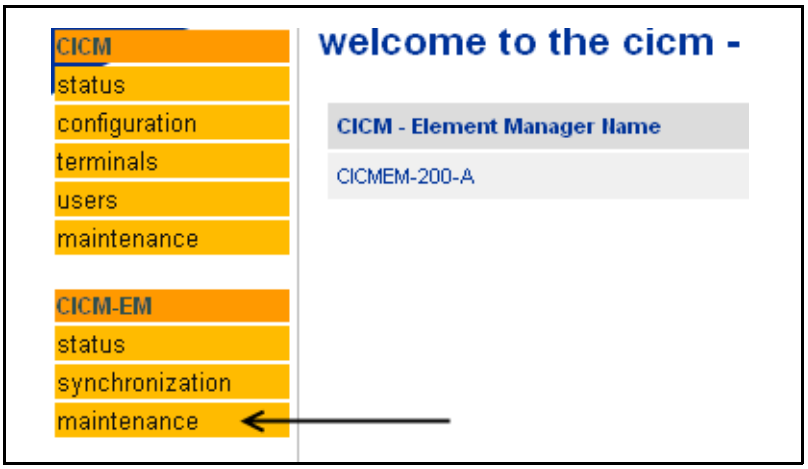
Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node preparation for an upgrade.
- You must know the administrator userids and passwords to login to the CICM-EM.

Procedure steps to verifying the software version of the CICM-EM and CICM nodes

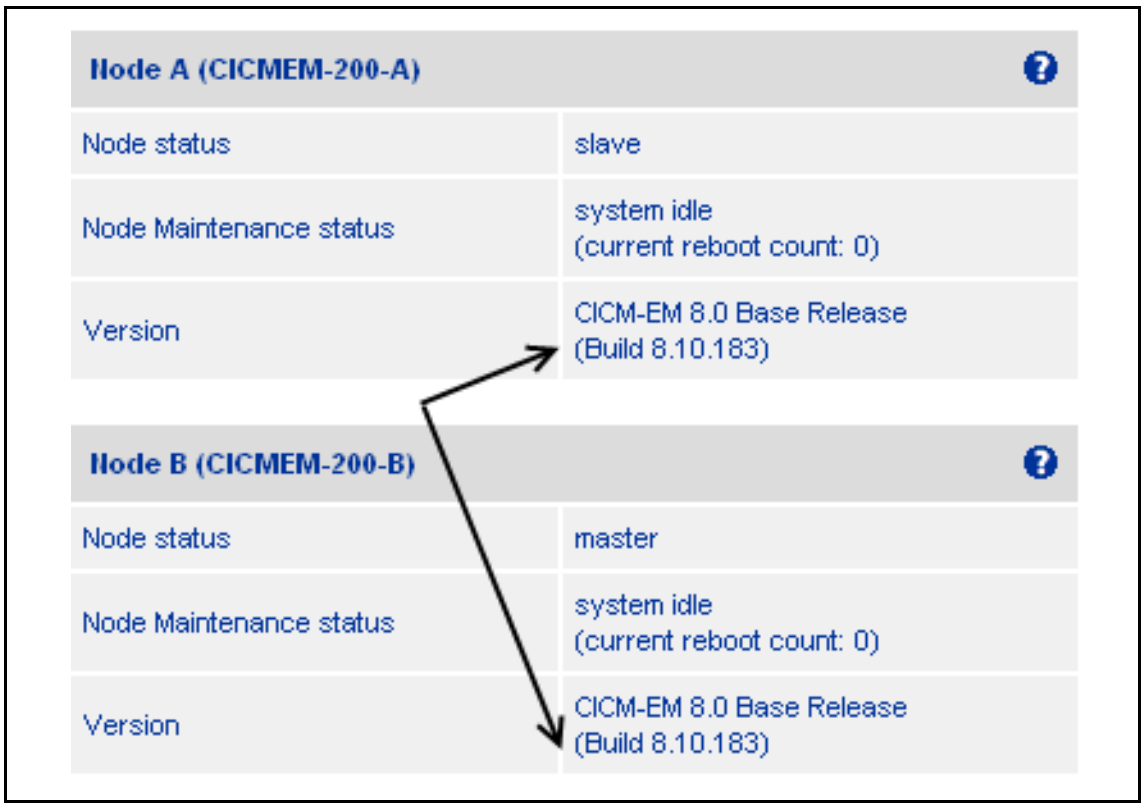
At the page CICM-EM home

1 Click **maintenance** in the menu *CICM-EM*.



At the page maintenance status (cicmem-nnn)

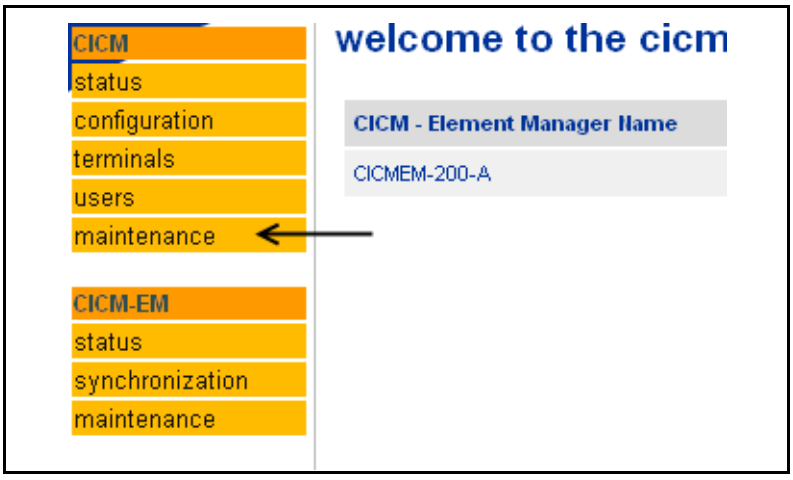
2 View the versions of each CICM-EM beside *Version* under the status of each Node.



If the versions are identical, proceed with the upgrade.

If the versions are different, you must match them by applying whatever product release (MR0) or MRx is required. Both nodes must be in service and running the same version of software before an upgrade is attempted.

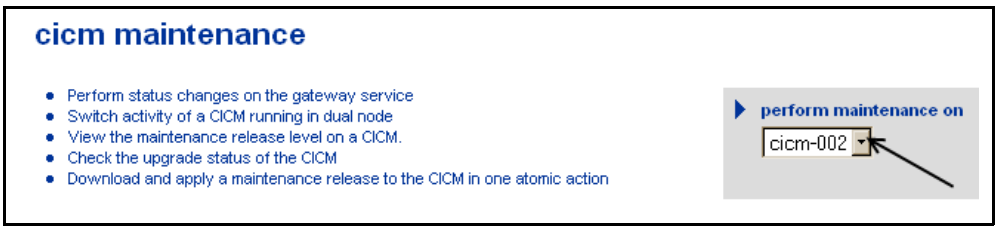
3 Compare the CICM nodes versions by clicking **maintenance** in the menu *CICM*.



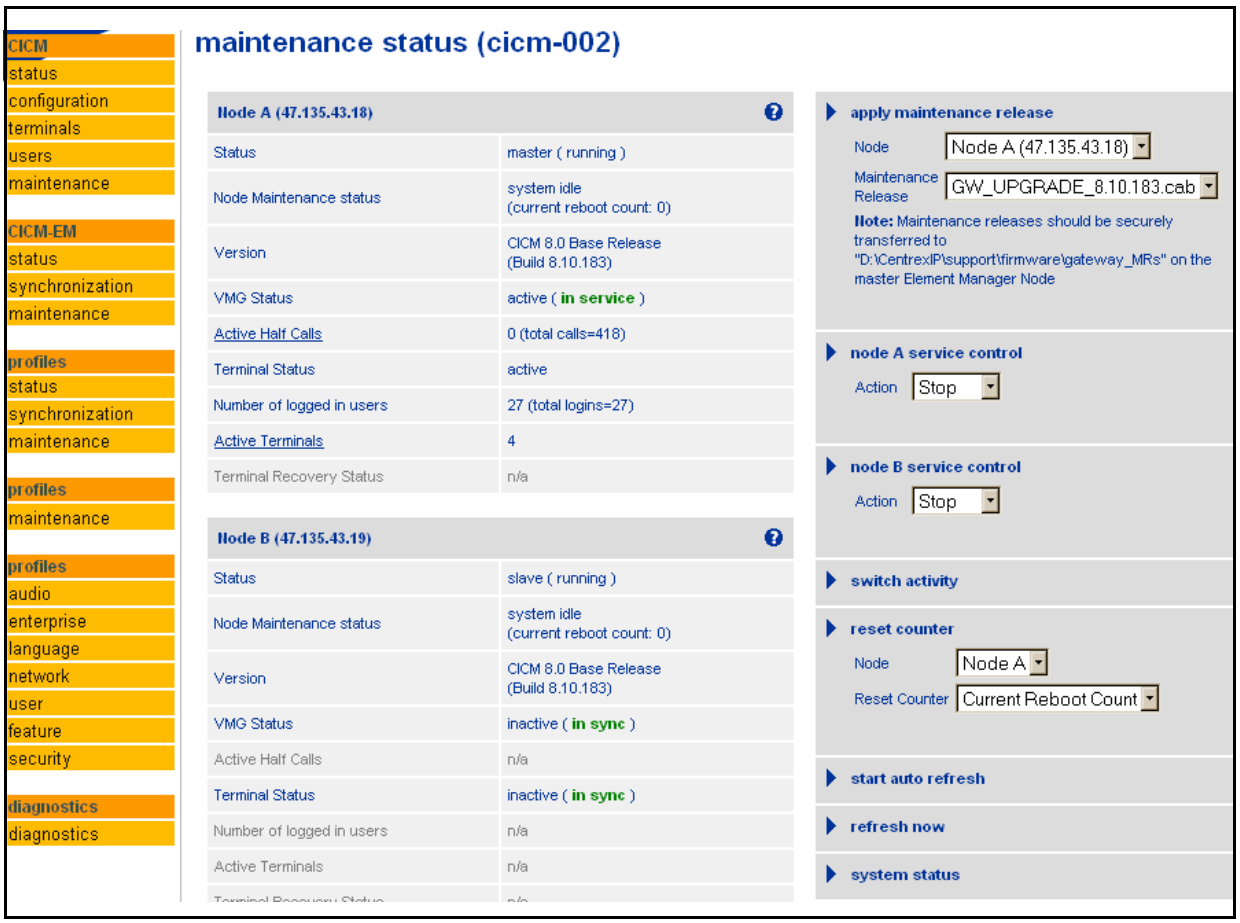
4 From the pick-list under **perform maintenance on**, select the CICM to view.

When you select the node other than the one that is showing, the page *maintenance status* automatically opens.

When the displayed *Node* is already the one you want, click **perform maintenance on**.



The page *maintenance status (cicm-nnn)* opens.



5 The software version for each CICM node is shown beside Version of the Node A and B status windows.

The software of the CICM-EM and CICM nodes should all be the same version for optimal performance. For acceptable different versions, refer to CICM software versions.

6 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

Original Equipment Manufacturer (OEM) gateways and gateway managers

Before upgrading Original Equipment Manufacturer (OEM) gateways and gateway managers

Perform the required prerequisite upgrade as follows:

Network	OEM gateways and gateway managers apply to:	Previous Upgrade
ATM	not applicable	not applicable
IP	CHS and IAC[1]	Centrex IP Client Manager (CICM) on page 1771
	IAW	Media Gateway 7400/15000/20000 on page 1769
Tri-Modal	not applicable[2]	not applicable

1.Includes IP International: CHS and IAC.
2.Carrier Hosted Services introduced to Tri-Modal in the SN08 release. Only CHS conversions and new installations are supported for the Trii-Modal SN08 applications.

After upgrading Original Equipment Manufacturer (OEM) gateways and gateway managers

Perform the next required upgrade as follows:

Network	OEM gateways and gateway managers apply to:	Next Upgrade
ATM	not applicable	not applicable
IP	CHS[1] and IAW	MCS Management Server upgrade on page 1835
	IAC[2]	upgrade is complete
Tri-Modal	not applicable	not applicable

1.Includes IP International: CHS.
2.Includes IP International: IAC.

About the Original Equipment Manufacturer (OEM) gateways and gateway managers

Refer to OEM/third-party media gateway upgrade documentation. 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. 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.

MCS Management Server upgrade

ATTENTION

Due to the complexity of the upgrade for the MCS Management Server and RTP Media Portal product, Nortel requires that all customers contact their Nortel Customer Service representative to engage the appropriate Nortel Software Delivery team to perform this upgrade.

There will be no service charges incurred for this activity.

RTP Media Portal upgrade

ATTENTION

Due to the complexity of the upgrade for the MCS Management Server and RTP Media Portal product, Nortel requires that all customers contact their Nortel Customer Service representative to engage the appropriate Nortel Software Delivery team to perform this upgrade.

There will be no service charges incurred for this activity.

Post Upgrade Procedures

After completing a network upgrade a series of additional procedures can be required. The following table contains a summary of optional post-upgrade procedures that can be required after a network upgrade.

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. Refer to Modifying a plan using the NPM on page 1985
Remove or update DCE	IP solutions only: PT-IP PT-AAL2 IAW	Distributed Computing Environment (DCE) CAUTION on page 11 *CS 2000 Core Manager Security and Administration*, NN10170-611
Cutover USP messaging from core bounce to direct messaging	IP solutions only	USP core bounce to direct messaging cutover on page 1626

Table 1 Post-upgrade procedures

Requirement	Applicable Solutions	Documentation
Complete any required post-upgrade tasks for each component	All solutions	Refer to the individual component upgrade procedures for post upgrade tasks.
Clean up old data in the NPM database	All solutions	Refer to Cleaning up old data in the NPM database on page 2014
Add required components to the IEMS topology	All solutions except PT-AAL1	Refer to Editing and viewing object properties using Java Web Client on page 1841 and Editing and viewing object properties using Web Client on page 1846

Editing and viewing object properties using Java Web Client

Application

Use this procedure to edit or view the properties of objects that are displayed in the IEMS topology using Java Web Client.

Prerequisites

None

Action

At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to Launching IEMS Java Web Start Client in *Integrated EMS Basics*, NN10329-111.

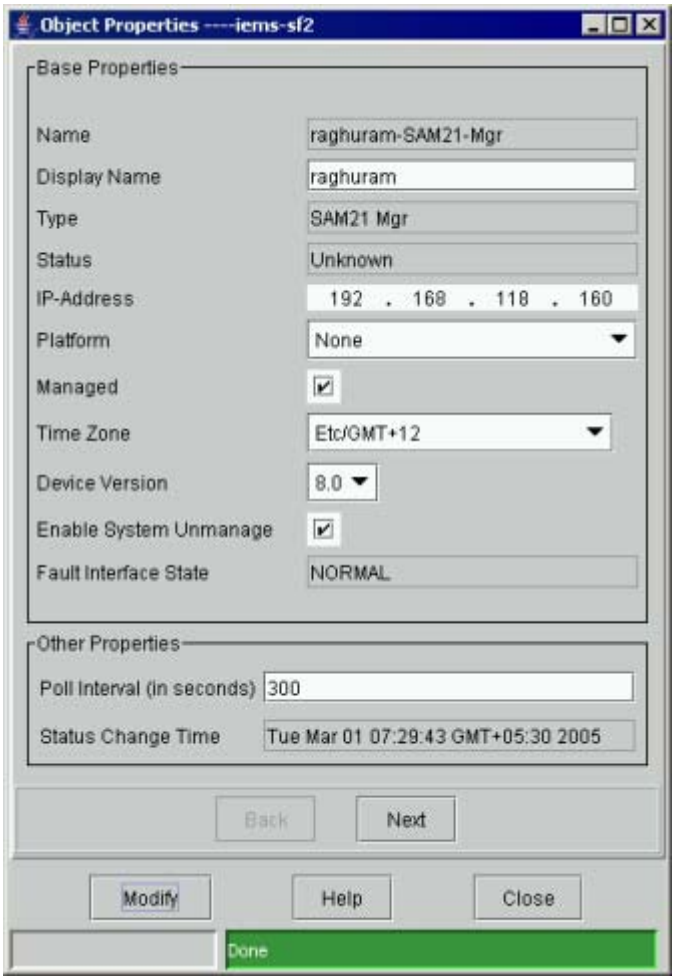
2 Select the required object in the Integrated EMS Topologies tree under Applications.

Note: The properties of an object from the Inventory panel of Integrated EMS tree can also be viewed. To view the Inventory object properties, select the object in the Integrated Topologies tree under Applications to open the Inventory view. Double-click the required row in the Inventory view.

3 Right-click the map symbol and select the **Managed Object Properties** menu item or double-click the map symbol to open the Object Properties window.

Note: The object properties displayed can differ for each component.

A window similar to the following figure opens.



4 Modify the object properties listed in the table below if required.

Managed object properties in Java Web Client

Field	Description
Name	Displays a unique name for the object
Display Name	Edit the name displayed in the topology for the object
Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
IP-Address	Edit the IP address of the object

Managed object properties in Java Web Client

Field	Description
Platform	Select the platform where the object resides from the drop-down list
Managed	Indicates whether the object is managed or unmanaged
Time Zone	Select the time zone of the geographical location where the object exists from the drop-down list
Device Version	Select the device version of the managed object from the drop-down list
Enable System Unmanage	Enable or disable the System_Unmanaged state. Refer to the System_Unmanaged state section of Configuring the Message Overload Controller parameters in *Integrated EMS Fault Management*, NN10334-911.
Poll Interval	Edit the Poll Interval for status updates
Status Change Time	Displays the last status change time of the object
Note: For the following objects, only the Display Name and the Managed field can be modified. • SDM platform, APS EMS application, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Proxy, Media Gateway 7480/15000, MSS 15000	

5 Select your next step.

If	Do
you do not want to modify any other properties	go to step 6
you want to view or modify the fault interface or performance interface properties	go to step 8

6 Click the **Modify** button to update the changes.

7 Go to step 16.

8 Click the **Next** button to proceed to the Fault Interface window.

A window similar to the following figure opens.

9 Edit or view the fault interface properties of the object as required.

Note: The Details panel dynamically changes according to the fault interface of the EMS/NE.

10 Select your next step.

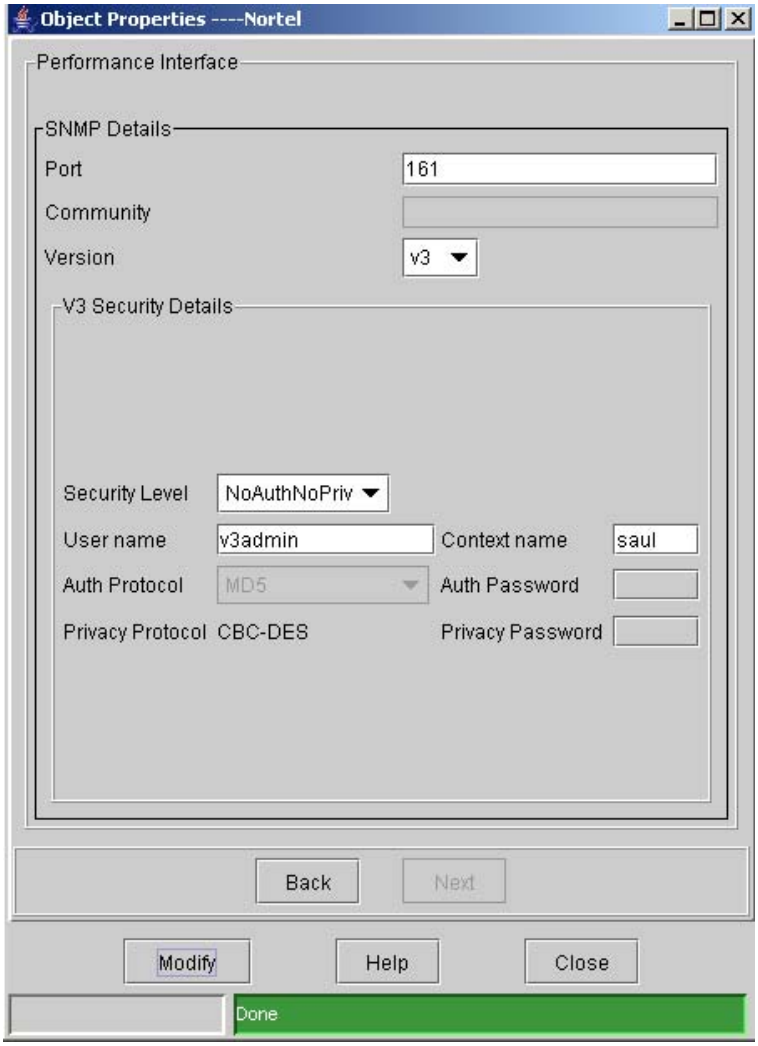
If	Do
you do not want to modify any other properties	step 11
you want to view or modify the performance interface properties	step 13

11 Click the **Modify** button to update the changes.

12 Go to step 16.

13 Click the **Next** button to proceed to the Performance Interface window.

A window similar to the following figure opens.



14 Edit or view the performance interface properties of the object as required.

15 Click the **Modify** button to update the changes.

16 You have completed this procedure.

Editing and viewing object properties using Web Client

Application

Use this procedure to modify or view the properties of an object in the IEMS topology using Web Client.

Prerequisites

None

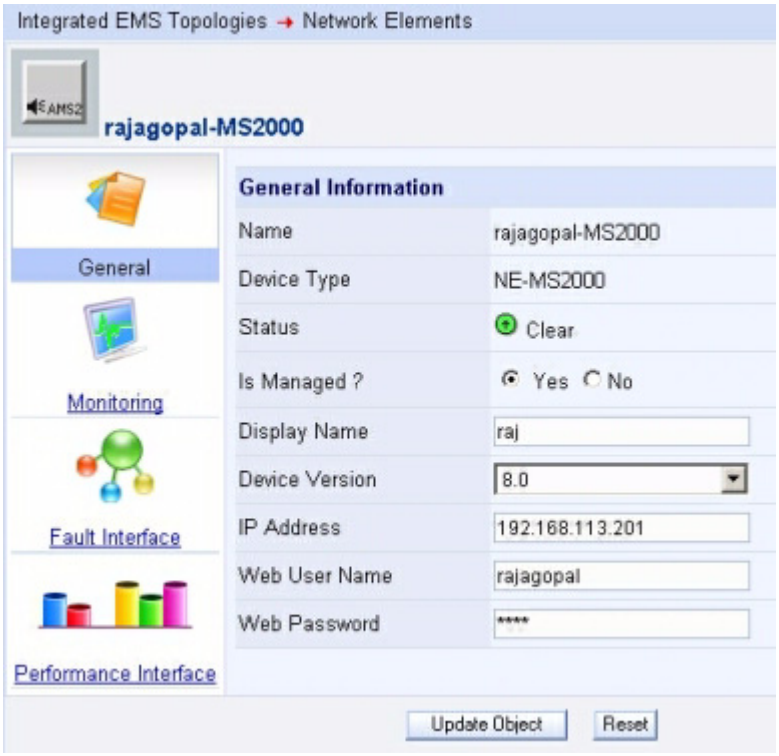
Action

At the IEMS workstation

1. Launch the IEMS Web Client. Refer to Launching the IEMS Web Client in *IEMS Basics*, NN10329-111.
2. Select the **Integrated EMS Topologies** tab.
3. Navigate to the required topology node in the Integrated EMS Topologies tree.
4. Click the map symbol label to open the **General Information** window.

   Note: The object properties displayed can differ for each component.

   A window similar to the following figure opens.



5 Select each vertical tab and modify the object properties listed in the table below if required.

Managed object properties in Web Client

Field	Description
General	
Name	Displays the unique object name of the managed object
Device Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
Is Managed?	Indicates whether the object is managed or unmanaged
Display Name	Displays the name or label displayed in map symbol
Device Version	Select the version of the device from the drop-down list

Managed object properties in Web Client

Field	Description
IP Address	Modify the IP address of the object
Web User name	Enter your web user name
Web Password	Enter your web password
Monitoring	
Last Status Update Time	Displays the time when the status of the managed object last changed
Last Status Change Time	Displays the time when the status of the managed object last changed
Status Polling Interval (secs)	Modify the Poll Interval for status updates

Managed object properties in Web Client

Field	Description
Fault Interface	
If the details are present for the selected object, the details can be modified.	
Performance Interface	
If the details are present for the selected object, the details can be modified.	

6 Click the **Update Object** button to update the changes.

7 You have completed this procedure.

Carrier Voice over IP Network 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 Carrier Voice over IP components that support the patching capability:

- core manager
- Succession Server Platform Foundation Software (SSPFS)
- Integrated Element Management System (EMS)
- Integrated EMS security component
- Core Element Manager (COREM)
- 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
- Multiservice Switch 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.nortel.com. Patches are located under "Support & Training> Software Downloads > Succession Communication Server 2000> 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 & Training> Software Downloads > Succession Communication Server 2000> 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 Carrier Voice over IP 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: • CS 2000 • MG 4000 • IW SPM • DPT SPM • Legacy peripherals, for example, the Spectrum Peripheral Module (SPM) ***Note:*** Patches are also referred to as Post-Release Software Updates (PRSUs).

Tool/utility	Description
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: • GWC • CS 2000 SAM21 Manager • MG 9000 • MG 9000 Manager • PSE • NPM • SESM • QCA • SSPFS • Integrated EMS • Integrated EMS security component • Core Element Manager (COREM) ***Note:*** You can obtain help information on the NPM through the Help menu of the GUI or by typing “help” in the CLUI.
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: • Preside MDM • Multiservice Switch 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 on page 1855
- Succession Server Platform Foundation Software on page 1855
- IEMS, COREM, and IEMS security components on page 1856
- Patching Server Element on page 1857
- CS 2000 Management Tools components on page 1857
  - CS 2000 SAM21 Manager
  - SESM
  - QCA
- Media Gateway 9000 Manager on page 1859
- Network Patch Manager on page 1860
- Preside Multi-service Data Manager on page 1860
- Multiservice Switch 15000 on page 1860
- Gateway Controller on page 1860
- Multi-service Gateway 4000 on page 1861
- Media Gateway 9000 on page 1861
- Interworking Spectrum Peripheral Module on page 1862
- Dynamic Packet Trunking Spectrum Peripheral Module on page 1862
- Legacy Peripheral Modules on page 1862
- Communication Server 2000 on page 1862

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.

Patching procedures checklist for the SSPFS

	Activities	√	Procedures
1	Retrieve the patch files from CD or electronically, and copy into the NPM database.		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
2	Apply the patches to the SSPFS.		Perform procedure Applying patches using the NPM on page 1895.

IEMS, COREM, and IEMS security components

The table below lists the procedures you must perform to patch the Integrated Element Management System (IEMS), the Core Element Manager (COREM), and the IEMS security components (IEMSCSS and IEMSCSS_DS). 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.

Patching procedures checklist for the IEMS, COREM, and IEMS security components

	Activities	√	Procedures
1	Apply the patches to the Integrated EMS.		Perform procedure Applying patches using the NPM on page 1895.
2	Restart the IEMS to enable the applied patches.		Perform procedure Restarting a device using the NPM on page 1943.
3	Apply the patches to the COREM.		Perform procedure Applying patches using the NPM on page 1895.
4	Restart the COREM to enable the applied patches.		Perform procedure Restarting a device using the NPM on page 1943.
5	Apply the patches to the IEMS security components as follows: • IEMSCSS • IEMSCSS_DS		Perform procedure Applying patches using the NPM on page 1895.
6	Restart the IEMS security components to enable the applied patches.		Perform procedure Restarting a device using the NPM on page 1943.

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.

Patching procedures checklist for the PSE

	Activities	√	Procedures
1	Retrieve the patch files from CD or electronically, and copy into the NPM database.		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
2	Apply the patches to the Patching Server Element (PSE).		Perform procedure Applying patches using the NPM on page 1895.
3	Restart the PSE to enable the applied patches.		Perform procedure Restarting a device using the NPM on page 1943.

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.

Patching procedures checklist for the CS 2000 Management Tools components

	Activities	√	Procedures
1	Audit the devices for existing patch activity.		Perform procedure Performing a device audit using the NPM on page 1879.
2	Retrieve the patch files from CD or electronically, and copy into the NPM database.		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
3	Apply the patches to the CS 2000 SAM21 Manager.		Perform procedure Applying patches using the NPM on page 1895.
4	Restart the CS 2000 SAM21 Manager to enable the applied patches.		Perform procedure Restarting a device using the NPM on page 1943.
5	Apply the patches to the Succession Element and Sub-network Manager (SESM).		Perform procedure Applying patches using the NPM on page 1895.
6	Restart the SESM to enable the applied patches.		Perform procedure Restarting a device using the NPM on page 1943.
7	Apply the patches to the QoS Collector Application (QCA).		Perform procedure Applying patches using the NPM on page 1895.
8	Restart the QCA to enable the applied patches.		Perform procedure Restarting a device using the NPM on page 1943.

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.

Patching procedures checklist for the MG 9000 Manager

	Activities	√	Procedures
1	Retrieve the patch files from CD or electronically, and copy into the NPM database.		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
2	Apply the patches to the MG 9000 Manager components as follows: • mg9kemserver • mg9kemmidtier • mg9kemomcollector		Perform procedure Applying patches using the NPM on page 1895.
3	Restart the MG 9000 Manager components to enable the applied patches.		Perform procedure Restarting a device using the NPM on page 1943.

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.

Patching procedures checklist for the NPM

	Activities	√	Procedures
1	Retrieve the patch files from CD or electronically, and copy into the NPM database.		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
2	Apply the patches to the Network Patch Manager (NPM).		Perform procedure Applying patches using the NPM on page 1895.
3	Restart the NPM to enable the applied patches.		Perform procedure Restarting a device using the NPM on page 1943.

Preside Multi-service Data Manager

Refer to section “Downloading the Preside MDM software and patches” in *Upgrading Preside MDM PT-AAL1/UA-AAL1*, NN10085-461.

Multiservice Switch 15000

Refer to section “Installing and downloading Multiservice Switch 15000 software and patches” in the U*pgrading Nortel Networks Multiservice Swtich 15000 PT-AAL1/UA-AAL1*, 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.

Patching procedures checklist for the GWC

	Activities	√	Procedures
1	Audit the GWC unit for existing patch activity.		Perform procedure Performing a device audit using the NPM on page 1879.
2	Retrieve the patch files from CD or electronically, and copy into the NPM database.		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
3	Apply the patches to the standby GWC unit.		Perform procedure Applying patches using the NPM on page 1895.
4	Activate the applicable patches.		Perform procedure Activating patches using the NPM on page 1911.
5	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.

Patching procedures checklist for the MG 9000

	Activities	√	Procedures
1	Audit the devices for existing patch activity.		Perform procedure Performing a device audit using the NPM on page 1879.
2	Retrieve the patch files from CD or electronically, and copy into the NPM database.		Perform one of the following procedures: • Transferring patches delivered on CD to the NPM database on page 1884 • Transferring patches delivered through ESD to the NPM database on page 1889
3	Apply the patches to the MG 9000.		Perform procedure Applying patches using the NPM on page 1895.

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 1863 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.

Patch management procedures

Procedure	Page
Defining sets using the NPM	1951
Defining a task using the NPM	1957
Setting field values using the NPM	1962
Defining reports using the NPM	1968
Defining a plan using the NPM	1977
Modifying a plan using the NPM	1985
Deleting a plan using the NPM	1997
Prioritizing a patching maintenance request using the NPM	2000
Performing a device image using the NPM	1904

To automate a task, perform procedure Defining a task using the NPM on page 1957 to define the task, for example autoimaging, then perform procedure Modifying a plan using the NPM on page 1985 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 and NPM client applications on page 1866.

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-based server” in the ATM/IP Security and Administration document, NN10402-600.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server where NPM resides

2 When prompted, enter your user ID and password.

3 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

4 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode: Enter 'npm' commands, help
or quit to exit.

npm>
```

You have completed this procedure.

Launching CS 2000 Management Tools and NPM client applications

Application

Use this procedure to launch any one of the following client applications:

- Trunk Maintenance Manager (TMM)
- CS2000 Management Tools
- Line Maintenance Manager (LMM)
- SAM21 Element Manager
- Batch Configuration Monitor
- Network Patch Manager (NPM), when installed and enabled on the same server as the CS 2000 Management Tools

  Note: The NPM also has a command line user interface (CLUI). Refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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

- Launching applications from a web browser on page 1868. You must use this method when launching an application for the first time.
- Launching applications from the JWS Application Manager on page 1871.

  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 1874.

  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 1877.

Note: You can also launch applications from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to the Integrated Element Management System Basics document, NN10329-111.

Prerequisites

Ensure the client workstation meets the minimum requirements. Refer to section “Client workstation requirements” under "CS 2000 Management Tools" in the Basics document, NN10320-100 (ATM solution) or NN10300-100 (IP solution).

ATTENTION

If you have an ATI Raedon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you can experience the “blue screen of death” in your Windows environment. You can obtain information on this issue at the following website:

http://developer.java.sun.com/developer/bugParade/bugs/4713003.html

A workaround for this issue is to download the latest ATI graphics driver from the following web site:

http://mirror.ati.com/support/driver.html

Contact your IT support team if you need assistance.

You need the IP address or host name of the server where the CS 2000 Management Tools are installed, and a valid user name and password to launch an application.

Note: Users of the CS 2000 Management Tools client applications must belong to the primary user group “succssn” for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure “Setting up local user accounts on a Sun server” in the ATM/IP Security and Administration document, NN10402-600.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_05 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the following applications:

- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

Note: JWS 1.2.0_02 is included as part of JRE 1.4.2_05.

Action

Launching applications from a web browser

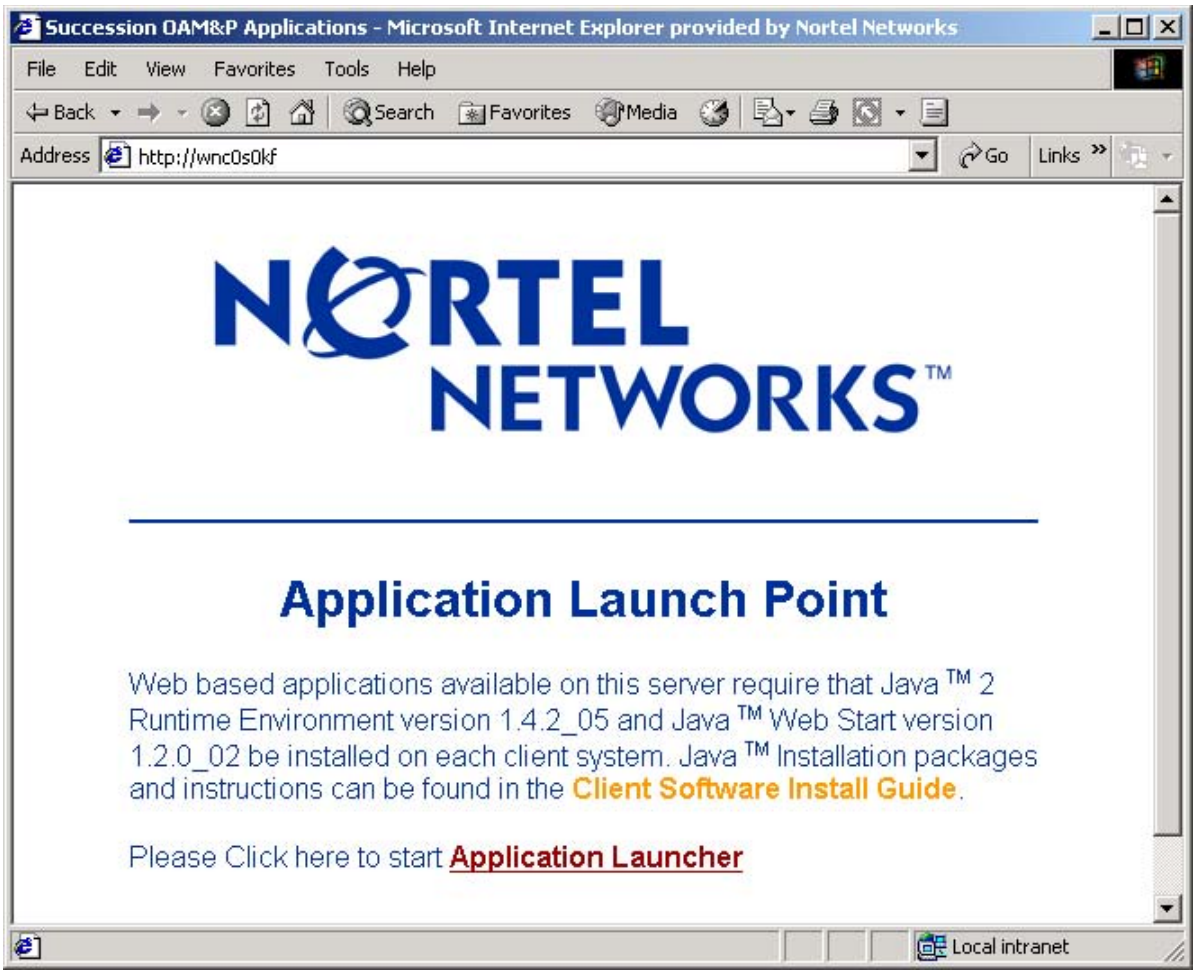
At your workstation

1 Launch your web browser.

2 In the Address field, enter the name or IP address of the CS 2000 Management Tools server.

Example
http://47.142.89.70

The “Application Launch Point” page appears.



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

If	Do
you have JRE 1.4.2_05 and JWS 1.2.0_02 installed	step 9
you do not have JRE 1.4.2_05 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 1.4.2_05 and JWS 1.2.0_02 installed	step 8
you do not have JRE 1.4.2_05 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.

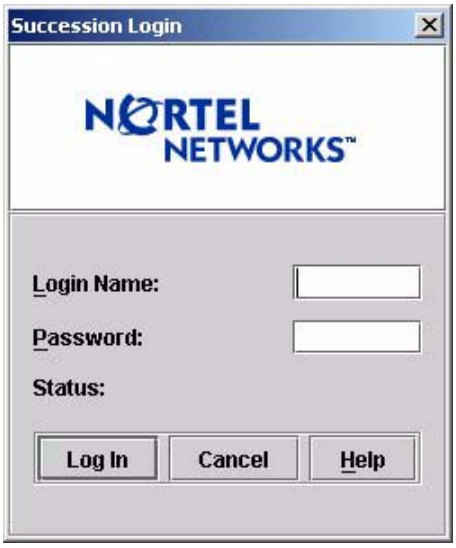
7 Click **Java 2 Runtime Environment Software Download** under *Microsoft Windows* or *Sun Solaris* to download and install the software.

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 the link for the application you want to launch.

The interface for the application you launched, is displayed.

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

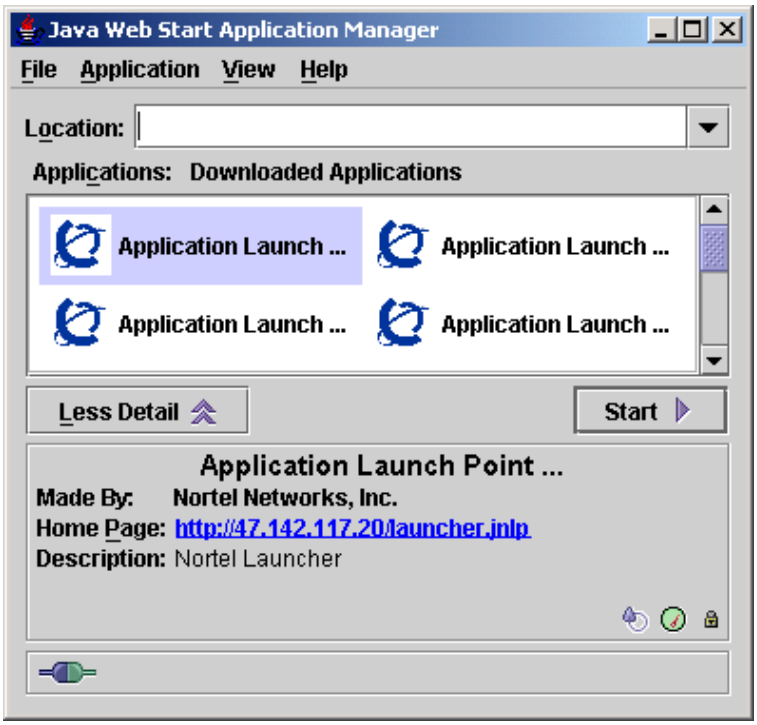
You have completed this procedure.

Launching applications from the JWS Application Manager

ATTENTION
You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Launch the Java Web Start Application Manager.

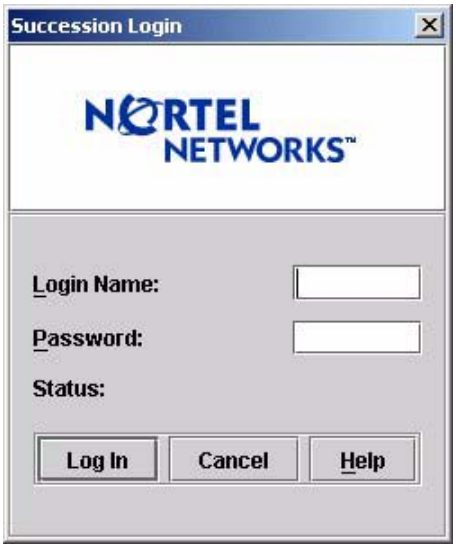


Note: If you do not see the downloaded applications as shown in the example above, on the **View** menu, click **Downloaded Applications**.

2 Double click on the Application Launch Point you want to access, or select the Application Launch Point and click **Start**.

The Login window appears.

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



The Application Launch Point, similar to following, appears.

4 Click the link for the application you want to launch.

The interface for the application you launched, is displayed.

You have completed this procedure.

Launching applications from a desktop icon or Start menu (Windows only)

ATTENTION
You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Perform step a to launch an application from a desktop icon, or step b to launch an application from the Start menu.

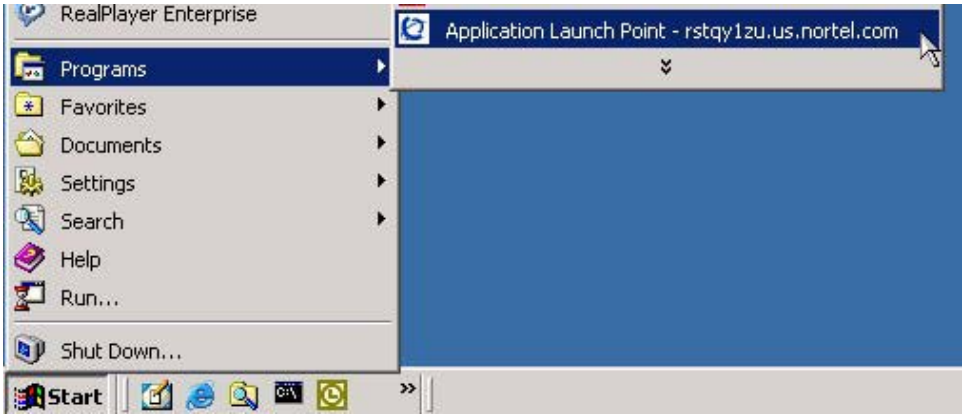
a To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double click on it to start the application.

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

The Login window appears.

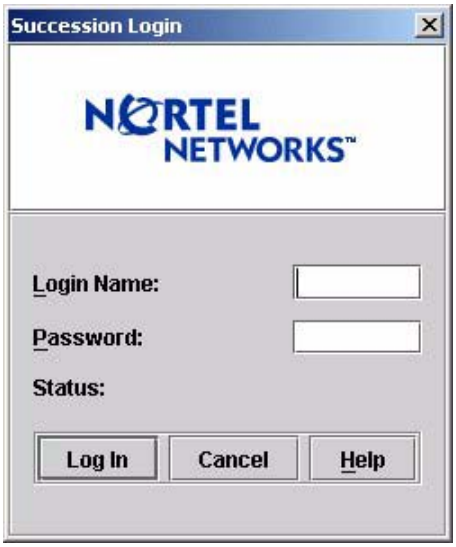
Proceed to step 2.

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



The Login window appears.

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



The Application Launch Point, similar to following, appears.

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

The interface for the application you launched, is displayed.

You have completed this procedure.

Launching specific applications using a URL

ATTENTION

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_05 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in this procedure Launching applications from a web browser on page 1868.

At your workstation

1 Launch your web browser.

2 In the Address field, enter one of the following URLs for the application you want to launch:

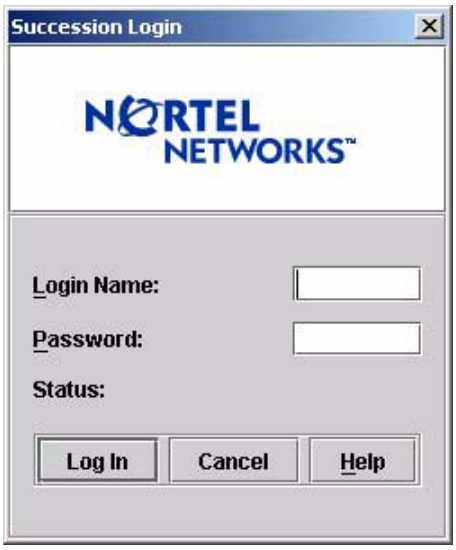
Application	URL
CS2000 Management Tools	http://<host>:8080/launch/servlet/Launch?app=sesm
Line Maintenance Manager	http://<host>:8080/launch/servlet/Launch?app=lmm
Trunk Maintenance Manager	http://<host>/sesm/tmm.html
Batch Configuration Monitor	http://<host>/sesm/bpt.html
CS2000 SAM21 Manager	http://<host>:8080/launch/servlet/Launch?app=sam21em
Network Patch Manager	http://<host>:8080/launch/servlet/Launch?app=npm

Where

host
is the host name or IP address of the server where the application resides

The Login window appears.

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



The interface for the application you launched, is displayed.

You have completed this procedure.

Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and SAM21 Element Manager) connect to their corresponding server-side application through a Socks proxy.

Note: The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

If, when you launch a client application that connects through a Socks proxy, you receive an error message indicating that the Socks connection to the server has failed, the server is down and needs to be rebooted. Once the server has rebooted, you can relaunch the client application.

Performing a device audit using the NPM

Application

Use this procedure to perform a device audit using the Network Patch Manager (NPM).

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 one of the following procedures to transfer the patches to the NPM database:

- Transferring patches delivered on CD to the NPM database on page 1884
- Transferring patches delivered through ESD to the NPM database on page 1889

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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

Action

Perform the steps under one of the following headings to complete this procedure:

- Using the NPM CLUI on page 1879
- Using the NPM GUI on page 1880

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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. If applicable, return to the high-level task or procedure that directed you to this procedure.

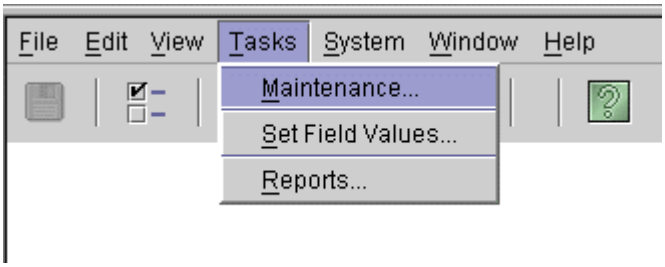
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

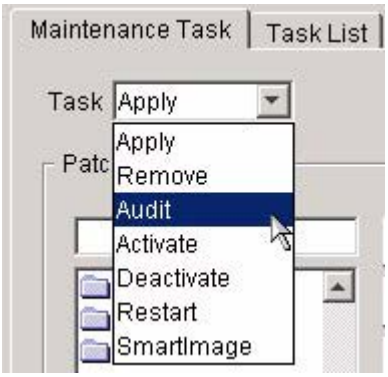
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.



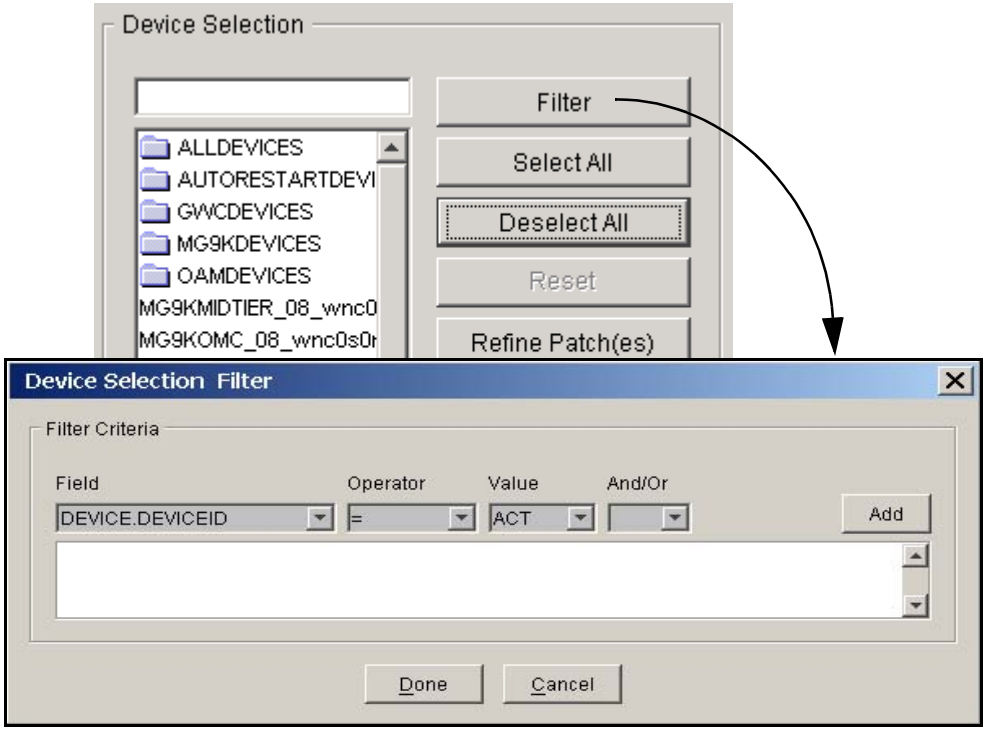
The Maintenance window is displayed.

3 In the **Task** list, click **Audit**.

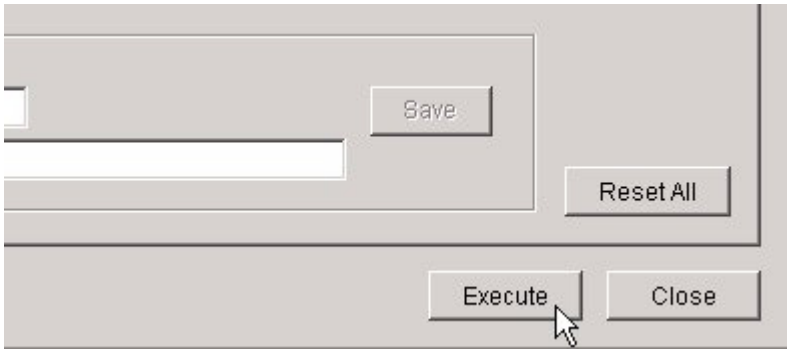


4 In the **Device Selection** list, select the devices or device sets to which you want to audit.

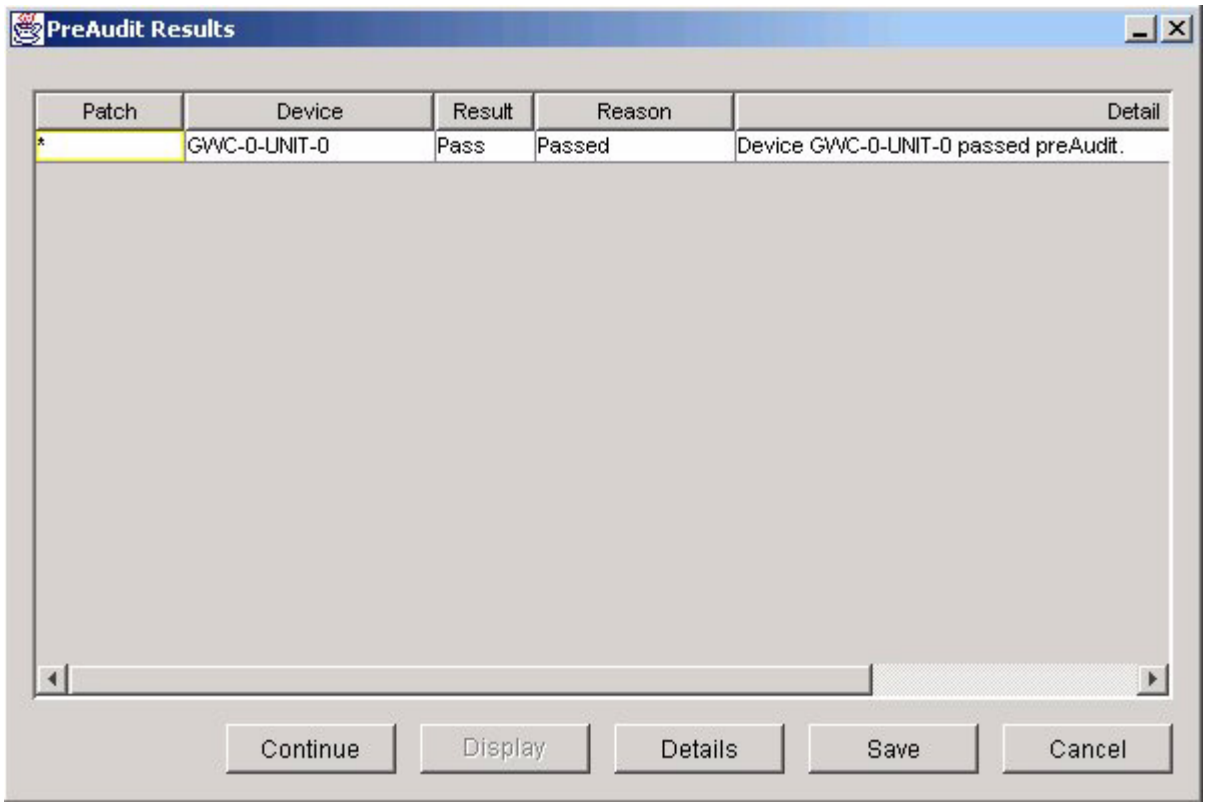
To limit the devices displayed in the **Device Selection** list, click **Filter** to configure a filtering criteria.



5 Click the **Execute** button to begin the audit process.



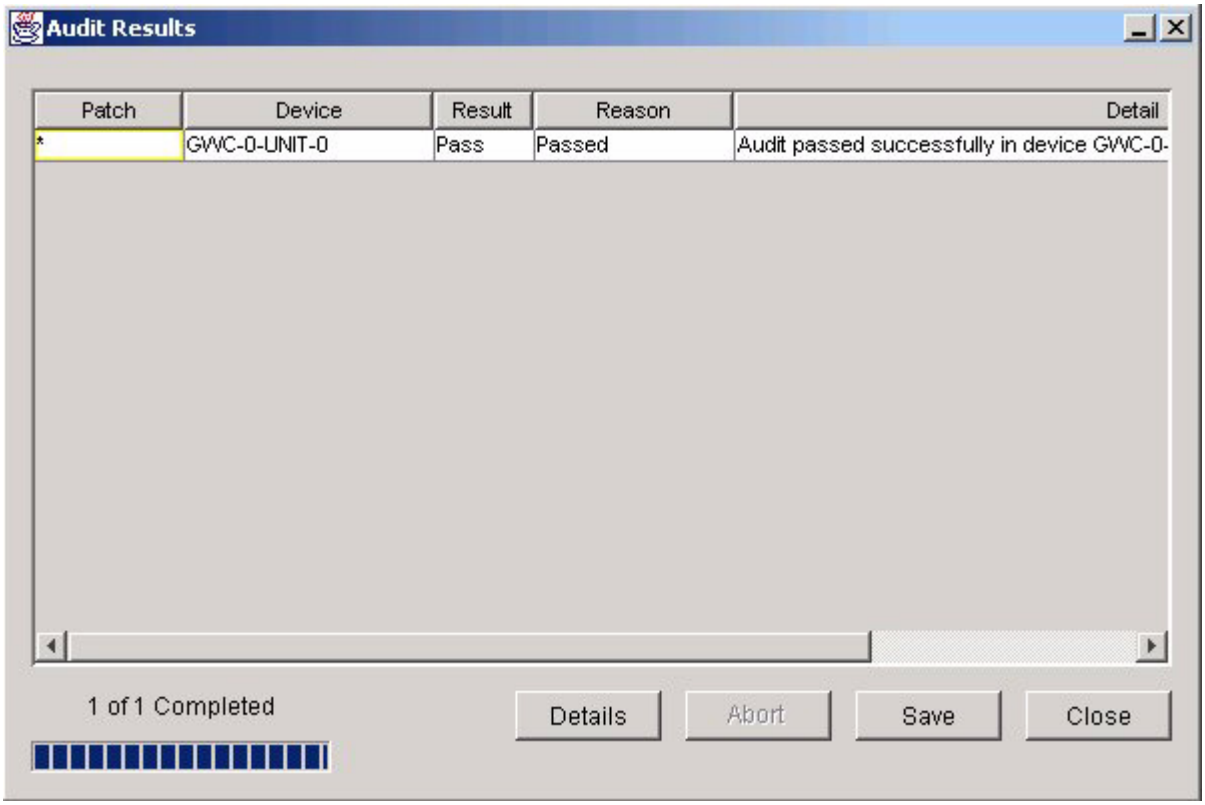
The results of the PreAudit phase are displayed.



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. If applicable, return to the high-level task or procedure that directed you to this procedure.

Transferring patches delivered on CD to the NPM database

Application

Use this procedure to manually transfer patches to the Network Patch Manager (NPM) database and retrieve them for processing. Use this procedure if the patches were delivered on CD.

Note: Once NPM is installed and configured, 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 *ATM/IP Solution-level Configuration Management*, NN10409-500, to enable PFRS or determine if it is already enabled.

Also use this procedure when you are either attempting to apply patches that have a blank patch category, or you are preparing for an HA cluster upgrade.

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" in *ATM/IP solution-level Security and Administration*, NN10402-600.

Action

Perform the steps that follow to complete this procedure.

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

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

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

b When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

At the server

4 Insert the CD that contains the patches into the drive of the SSPFS-based server where the NPM resides. In a two-server configuration, insert the CD into the drive of the active server.

At your workstation

5 Make a temporary directory for the patchlist file by typing

```
# mkdir /data/npm/tmp
```

and pressing the Enter key.

6 Change the permissions on the temporary directory by typing

```
# chmod 777 /data/npm/tmp
```

and pressing the Enter key.

7 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.

8 Access the directory you just created by typing

```
# cd /data/npm/tmp
```

and pressing the Enter key.

9 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 10
running	step 11

10 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

11 Access the NPM command line user interface (CLUI) by typing

```
# npm
```

and pressing the Enter key.

12 When prompted, enter your user ID and password.

Note: Do not change directories.

13 Retrieve the patch files copied from the CD by typing

```
npm> getpatch current.patchlist
```

and pressing the Enter key.

Note 1: The following error message may be received when executing this step:

```
Error: Patch file
/data/npm/patch_upgrade/lex83o9s.ptchoamp
cannot be verified. Copying to golden
directory.
```

This is acceptable behavior because the (I)SN07 load cannot verify the (I)SN08 patch. Ignore this error.

Note 2: The golden directory mentioned in the previous note is /data/npm/Au. The files are successfully placed here when the getpatch is done, even though it appears to fail.

14 Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

15 Eject the CD from the drive. Change to the root directory level by typing

```
# cd /
```

and pressing the Enter key.

16 Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

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

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

and pressing the Enter key.

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

and pressing the Enter key.

Then, press the eject button located on the front of the DVD drive.

17 Remove the CD or DVD from the drive.

If	Do
you have other patch CDs to install	insert the next CD and go to step 7
otherwise	close the cdrom tray and proceed to the next step

18 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Transferring patches delivered through ESD to the NPM database

Application

Use this procedure to obtain NPM patch files if you are using ESD. This procedure should be performed on the machine where the NPM application is resident. In an HA cluster configuration, this procedure should be run on the Active unit.

Prerequisites

None

Action

Perform the steps that follow complete this procedure.

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

Obtaining the NPM patch files from ESD

At your workstation

1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

> **`telnet <server>`**

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

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

b When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

4 Make a directory for the patch files you want to install by typing

```
# mkdir /<directory>
```

and pressing the Enter key.

where

directory
is a valid directory name

Example

```
# mkdir /esd_patches
```

5 Change the permissions on the newly created directory by typing

```
# chmod 777 /<directory>
```

and pressing the Enter key.

where

directory
is the directory name from step 4

Example

```
# chmod 777 /esd_patches
```

6 Access the newly created directory by typing

```
# cd /<directory>
```

and pressing the Enter key.

where

directory
is the directory name from step 4

Example

```
# cd /esd_patches
```

7 Log in to the ESD server through FTP by typing

```
# ftp <esd_server>
```

and pressing the Enter key.

where

esd_server
is the IP address of the ESD server

8 When prompted, enter your user ID and password for the ESD server.

9 Obtain a list of files and directories on the ESD server by typing

```
ftp> dir
```

and pressing the Enter key.

Note the name and timestamp of the .tar.gz file.

10 Set the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

11 Transfer all the patches from the ESD server to the NPM by typing

```
ftp> mget *.patch
```

and pressing the Enter key.

To transfer individual patch files, type

```
ftp> get <patchfilename>
```

where

patchfilename
is the name of the patch you are transferring

12 Exit FTP by typing

```
ftp> quit
```

and pressing the Enter key.

13 Verify the patches are on the server in the temporary directory that you created in step 4 by typing

```
# ls
```

and pressing the Enter key.

14 Change permissions for the patch files in the directory by typing

```
# chmod 777 *
```

and pressing the Enter key.

15 Use the following table to determine your next step:

If	Do
you have access to http://www.nortel.com	step 16
you do not have access to http://www.nortel.com	step 17

16 Retrieve the patches that have been released since the software was shipped by using the Pre Upgrade Patch Calculator. The Pre Upgrade Patch Calculator will require a label and a date. The label is the first eight characters of the .tar.gzip file associated with the software component being upgraded and the date is the date of the file shown in step 9 above.

Refer to Ensuring patch currency on page 50.

17 Create a patchlist file by typing

```
# ls *.patch > current.patchlist
```

and pressing the Enter key.

18 Verify the NPM server application is running by typing

```
# servquery -status -group NPM
```

and pressing the Enter key.

19 Use the following table to determine your next step:

If the NPM server is	Do
running	step 21
not running	step 20

20 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

21 Access the NPM command line interface (CLUI) by typing

```
# npm
```

and pressing the Enter key.

22 When prompted, enter your user ID and password.

Note: Do not change directories.

23 Retrieve the patch files for the NPM to process by typing

```
npm> getpatch current.patchlist
```

and pressing the Enter key.

Note 1: The following error message may be received when executing this step:

```
Error: Patch file
/data/npm/patch_upgrade/lex83o9s.ptchoamp
cannot be verified. Copying to golden
directory.
```

This is acceptable behavior because the current release cannot verify the patch for the new release. Ignore this error.

Note 2: The golden directory mentioned in the previous note is /data/npm/Au. The files are successfully placed here when the getpatch is done, even though it appears to fail.

24 Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

25 Access the directory that contains the downloaded patch files by typing

```
# cd /<directory>
```

and pressing the Enter key.

where

directory
is the directory you created in step 4 for the patch files

Example

```
# cd /esd_patches
```

26 Erase the downloaded patch files from the directory by typing

```
# rm *.patch
```

and pressing the Enter key.

27 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Applying patches using the NPM

Application

Use this procedure to apply patches using the Network Patch Manager (NPM).

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 one of the following procedures to transfer the patches to the NPM database:

- Transferring patches delivered on CD to the NPM database on page 1884
- Transferring patches delivered through ESD to the NPM database on page 1889

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

It is recommended that you perform an audit on the devices prior to patching. If required, refer to procedure Performing a device audit using the NPM on page 1879.

Action

Perform the steps under one of the following headings to complete this procedure:

- Using the NPM CLUI
- Using the NPM GUI

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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>

Example

```
npm> apply ACT02GAX in GWC-8-UNIT-1
```

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.

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 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:

- Patching Server Element (PSE)
- Integrated Element Management System (IEMS)
- IEMS security components (IEMSCSS_DS and IEMSCSS)
- CS 2000 SAM21 Manager (SAM21EM)
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
- Core Element Manager (COREM)
- Network Patch Manager (NPM)

To restart a device, refer to procedure Restarting a device using the NPM on page 1943 if required.

8 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

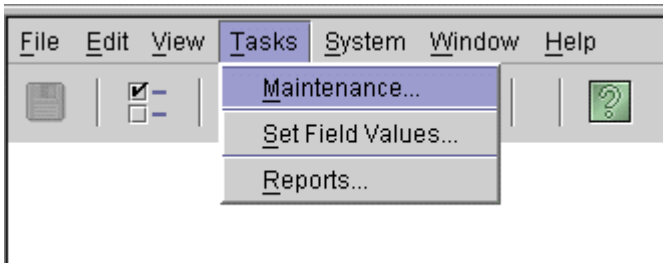
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

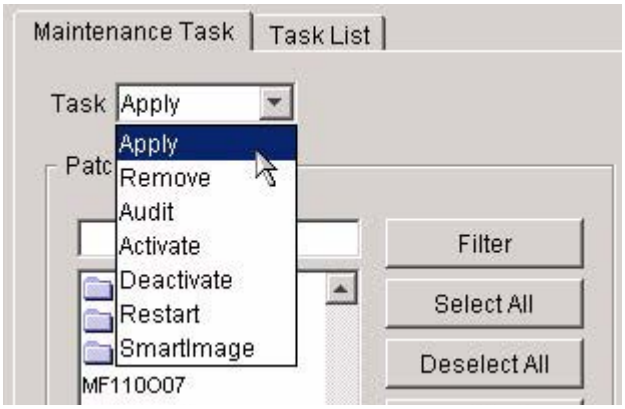
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.



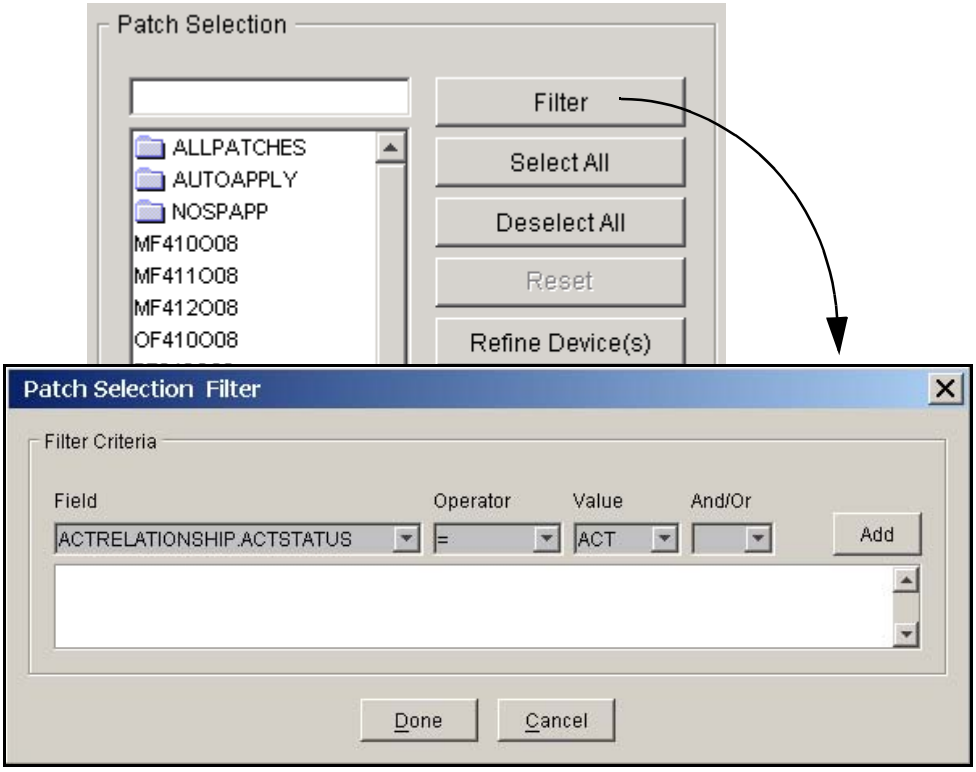
The Maintenance window is displayed.

3 In the **Task** list, click **Apply**.



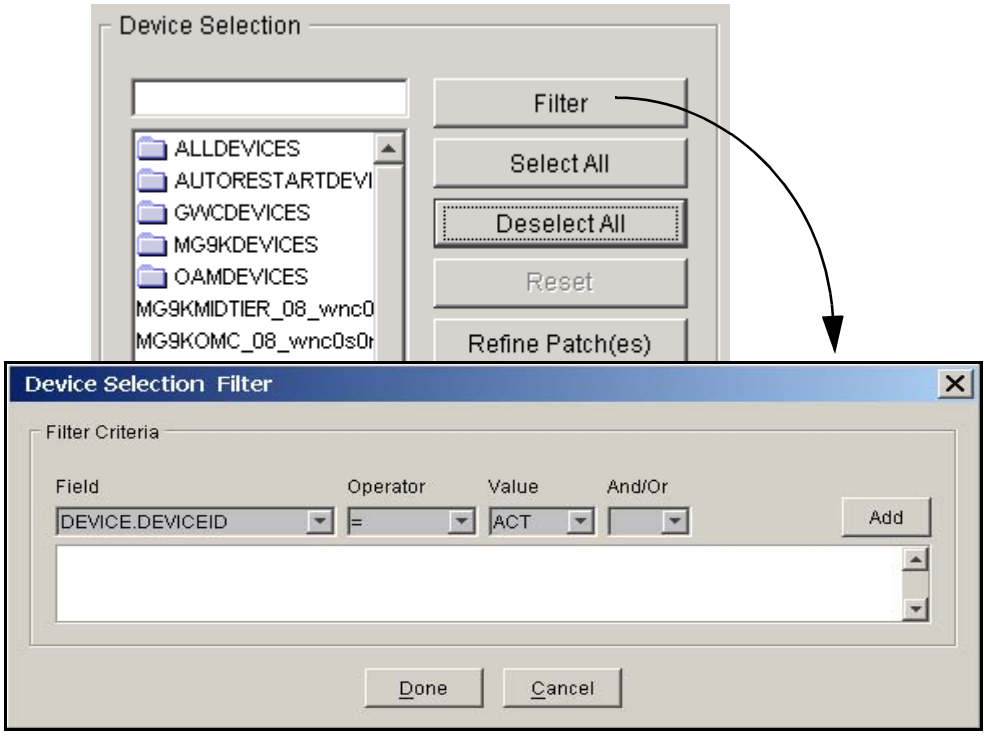
4 In the **Patch Selection** list, select the patch files or patch sets you want to apply, then click **Refine Device(s)** to display a list of devices to which the patches apply.

To limit the patches displayed in the **Patch Selection** list, click **Filter** to configure a filtering criteria.

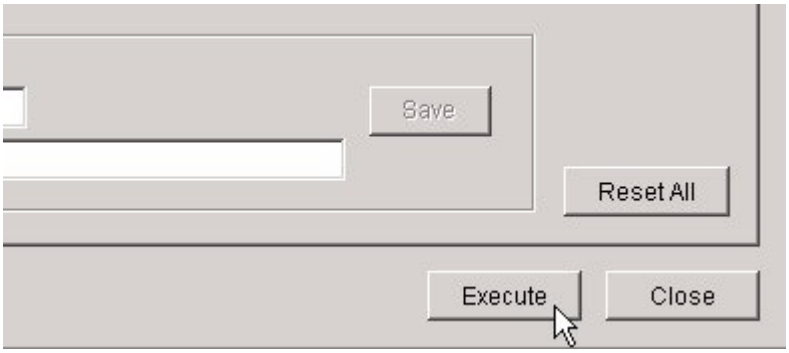


5 In the **Device Selection** list, select the devices or device sets to which you want to apply the patches.

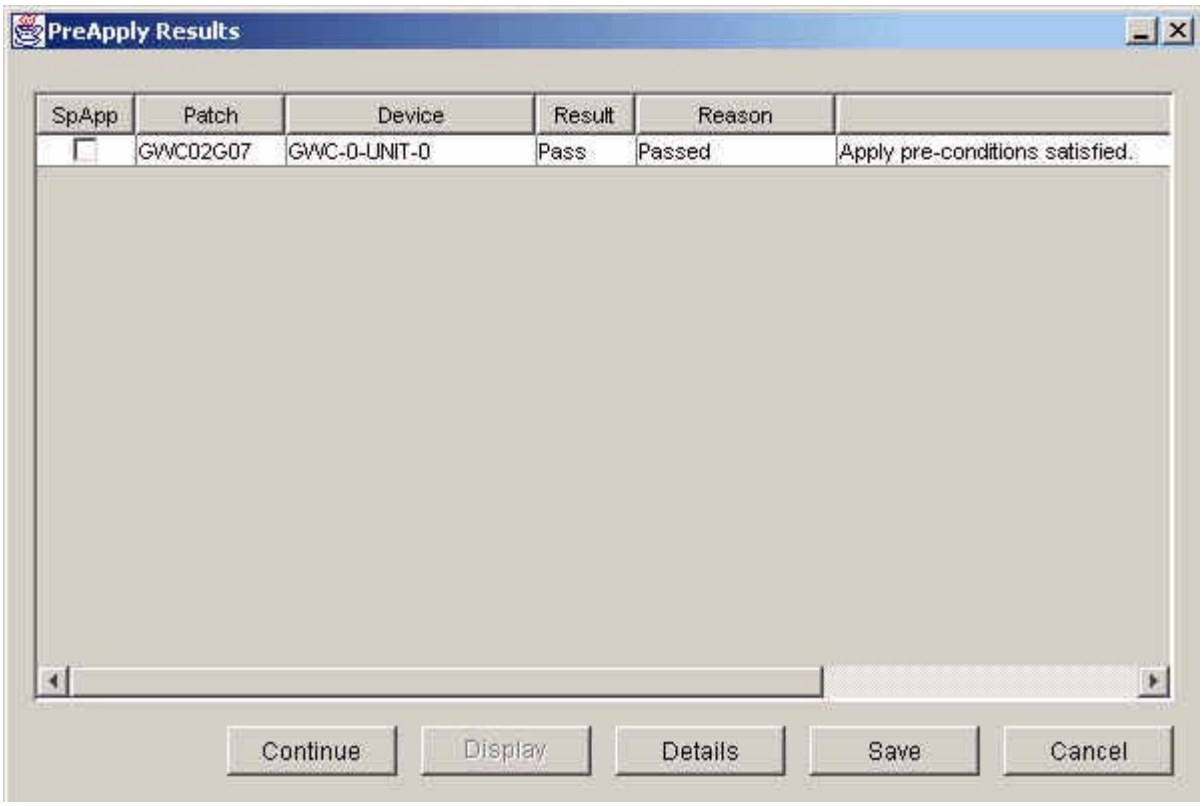
To limit the devices displayed in the **Device Selection** list, click **Filter** to configure a filtering criteria.



6 Click **Execute** to begin the patching process.



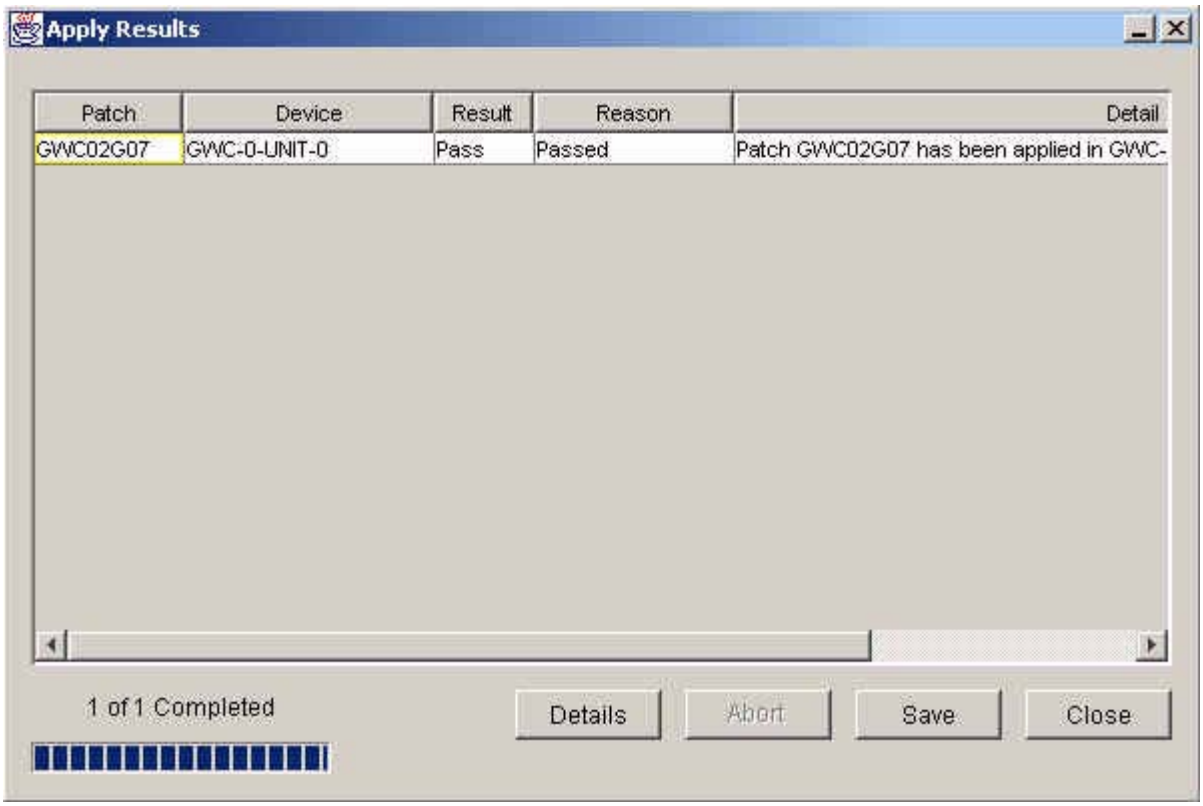
The results of the PreApply phase are displayed.



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 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:

- Patching Server Element (PSE)
- Integrated Element Management System (IEMS)
- IEMS security components (IEMSCSS_DS and IEMSCSS)
- CS 2000 SAM21 Manager (SAM21EM)
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
- Core Element Manager (COREM)
- Network Patch Manager (NPM)

To restart a device, refer to procedure Restarting a device using the NPM on page 1943 if required.

10 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

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 1905
- Using the NPM GUI on page 1907

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, must 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 Defining a task using the NPM on page 1957if required), and schedule that task as part of the NPM System Plan (refer to procedure Modifying a plan using the NPM on page 1985 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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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 using the following syntax

<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. If applicable, return to the high level task or procedure that directed you to this procedure.

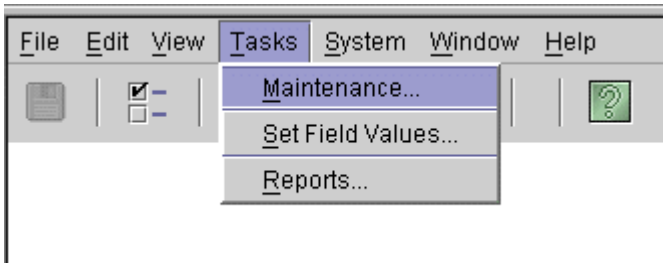
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

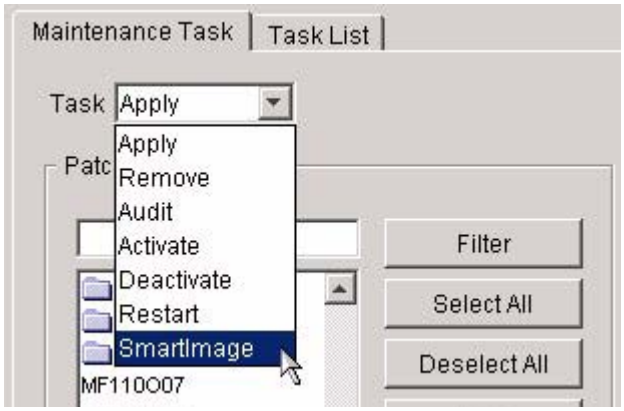
At the NPM GUI

2 On the Tasks menu, click **Maintenance...**.

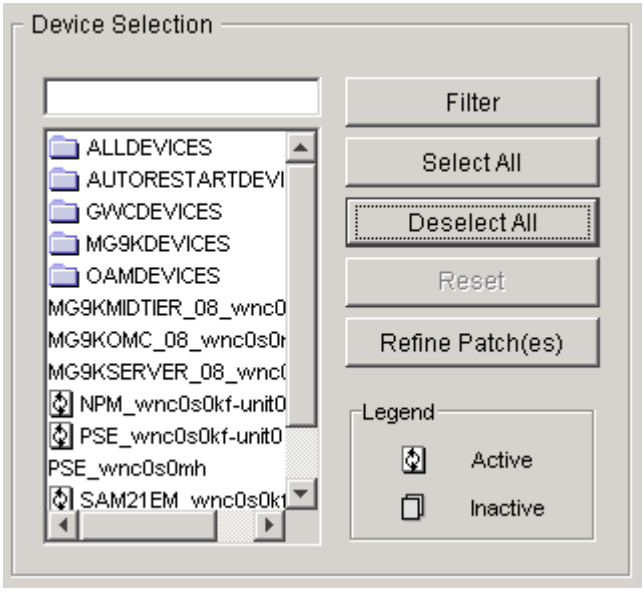


The Maintenance window is displayed.

3 In the Task list, click **SmartImage**.

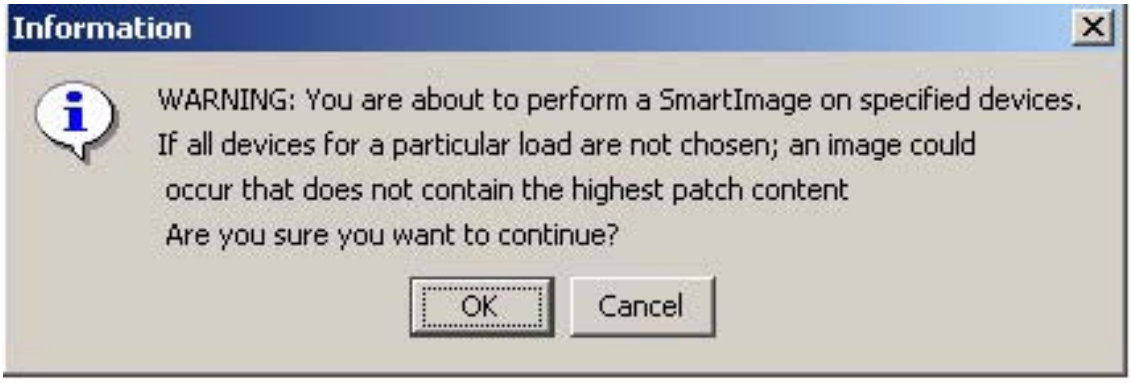


4 In the Device Selection list, select the device, device list, or device set that you want to image.



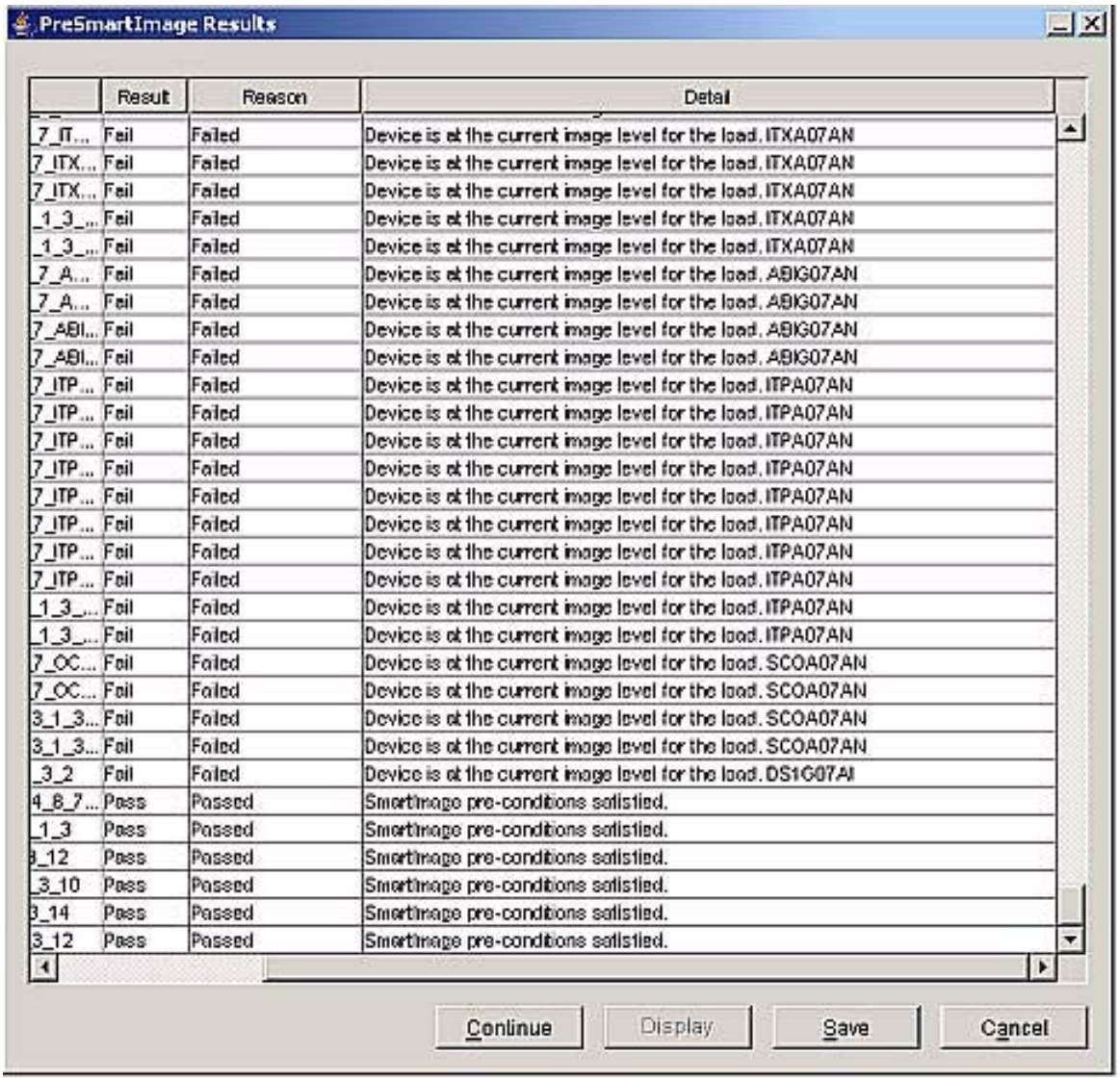
5 Click **Execute** to begin the restart.

The system returns the following warning.



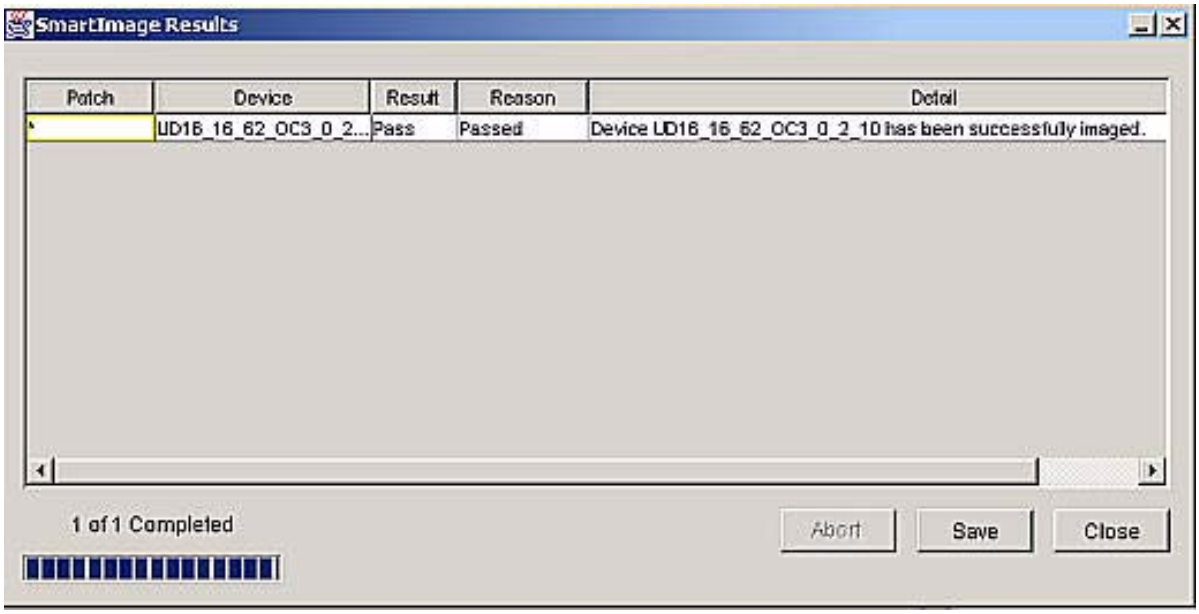
6 If you agree that the devices chosen are the ones you want evaluated, click **OK** to begin imaging.

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. If appicable, return to the high level task or procedure that directed you to 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 1912
- Using the NPM GUI on page 1913

Note: Currently, only GWC can have ACT category patches.

ATTENTION
Certain GWC patches are ACT category patches that require activation. It is important to note that not all ACT category patches require activating. The patches to be activated 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
Potential for partial loss of service
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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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 using the following syntax

<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 using the following syntax (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and activates them)

<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. If applicable, return to the high level task or procedure that directed you to this procedure.

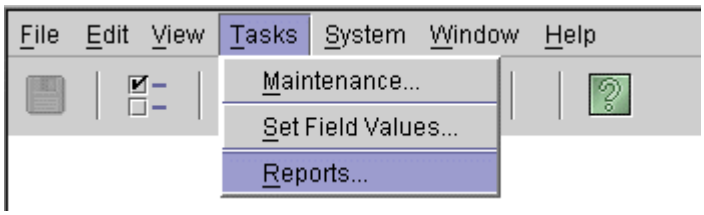
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

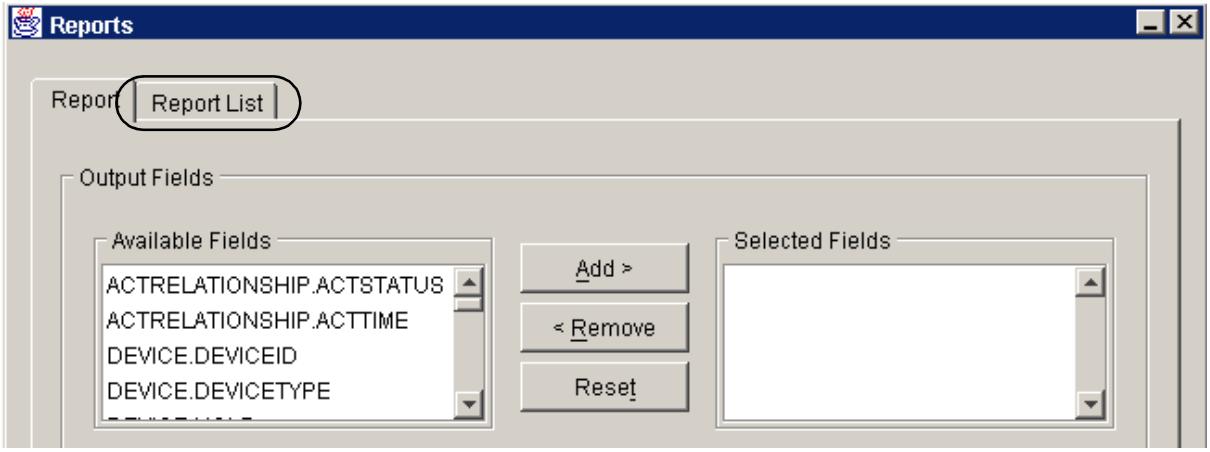
At the NPM GUI

2 On the Tasks menu, click **Reports...**.

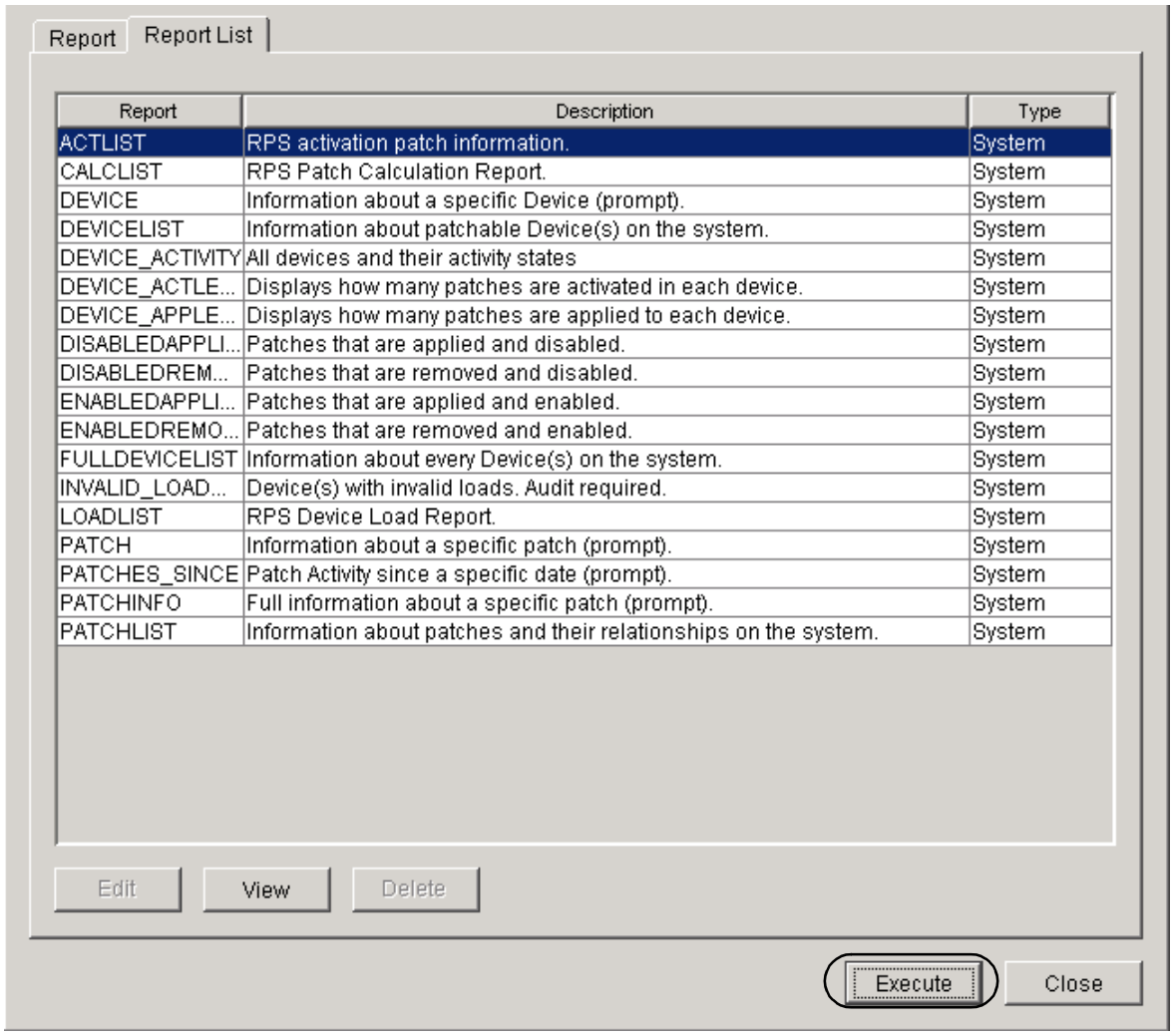


The Reports window is displayed.

3 Click the **Report List** tab.

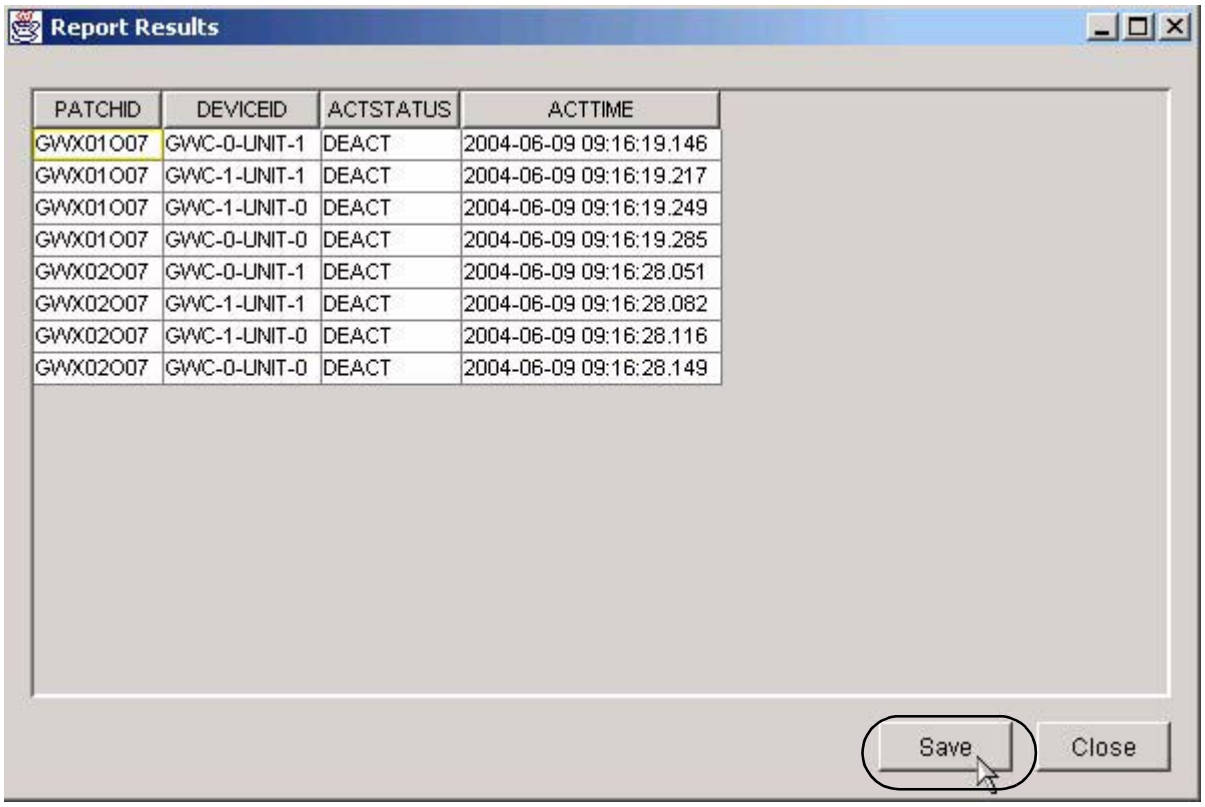


4 Click the **ACTLIST** entry in the Report field, then click **Execute**.



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 must be activated.

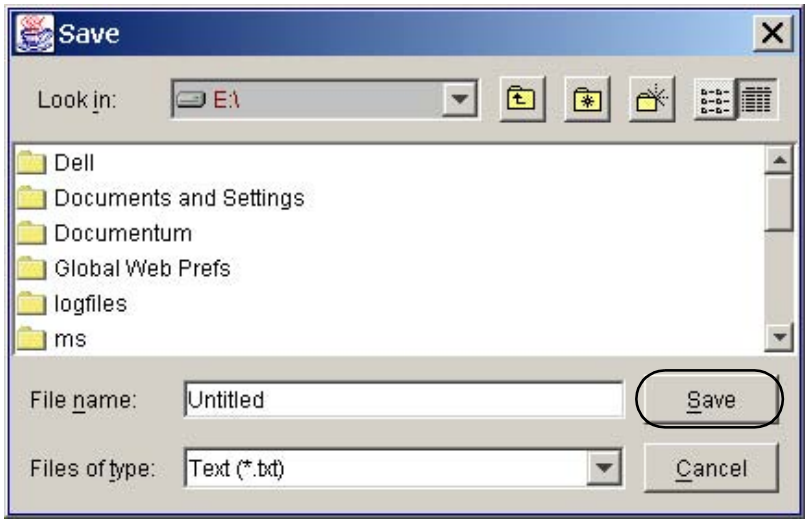
Note: If there are no patches to activate, the system returns a dialog box indicating that the report has “empty results”.



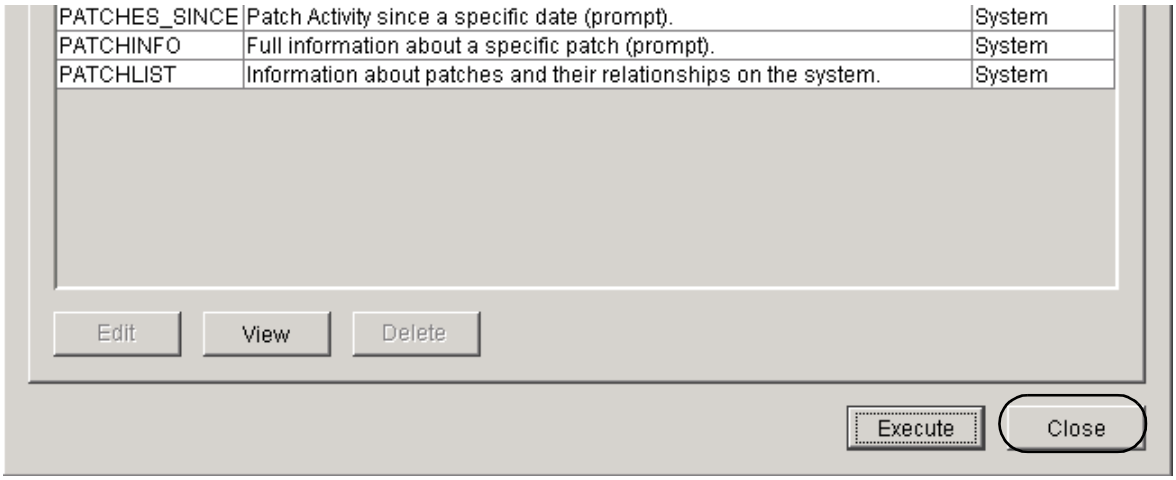
6 If necessary, save a copy of the report to a text file as follows:

a Click **Save**.

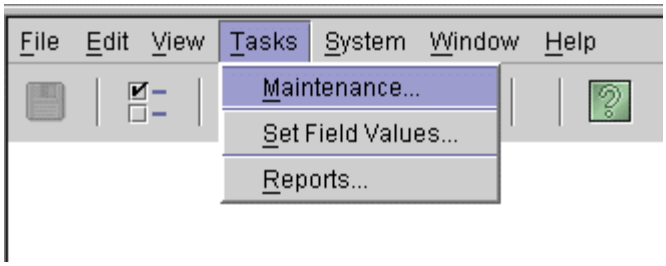
b Type a file name in the File name**:** box, and click **Save**.



7 Click **Close** to close the Reports window.

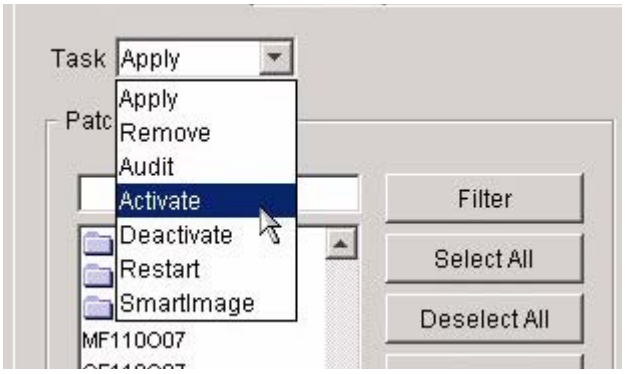


8 On the Tasks menu, click **Maintenance...**.



The Maintenance window is displayed.

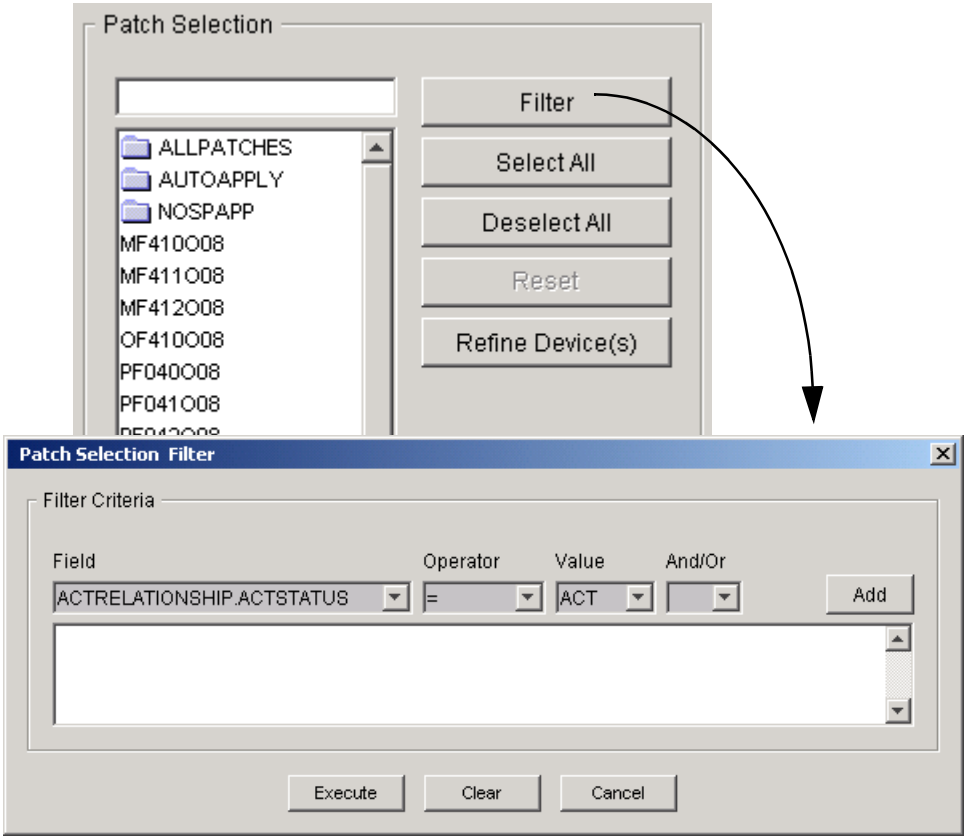
9 In the Task list, click **Activate**.



10 In the Patch Selection list, select the patch files or patch sets you want to activate, then click **Refine Device(s)** to display a list of devices to which the patches apply.

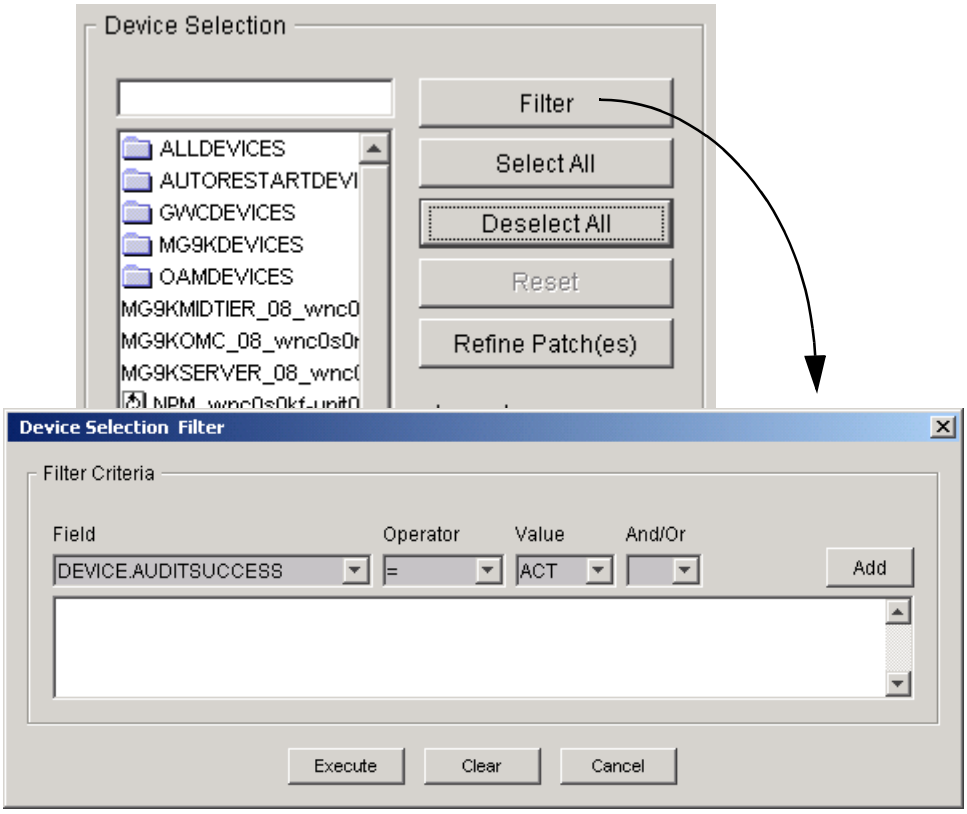
To limit the patches displayed in the Patch Selection list, click **Filter** to configure a filtering criteria.

Note: The patches must have a category of ACT.

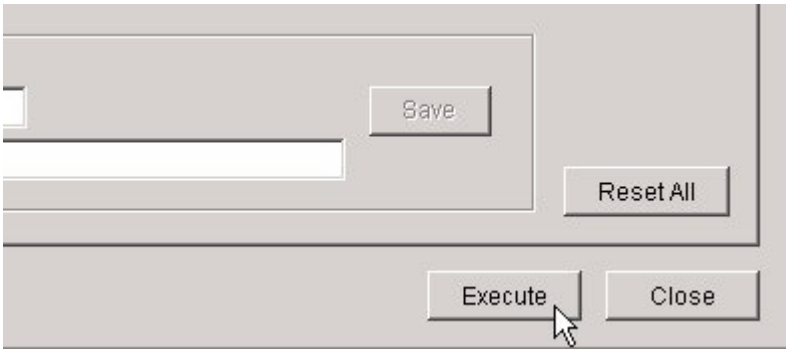


11 In the Device Selection list, select the devices or device sets that have the applied patches you want to activate.

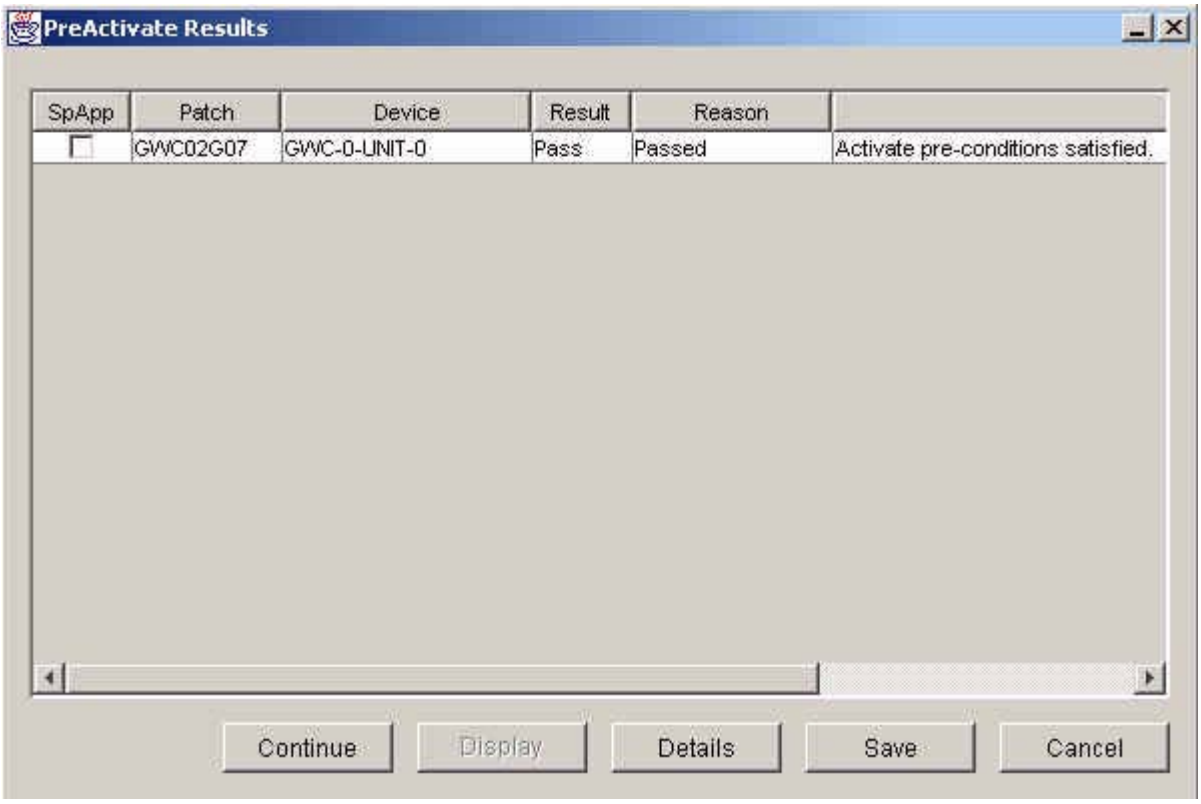
To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.



12 Click **Execute** to begin the patch activation process.



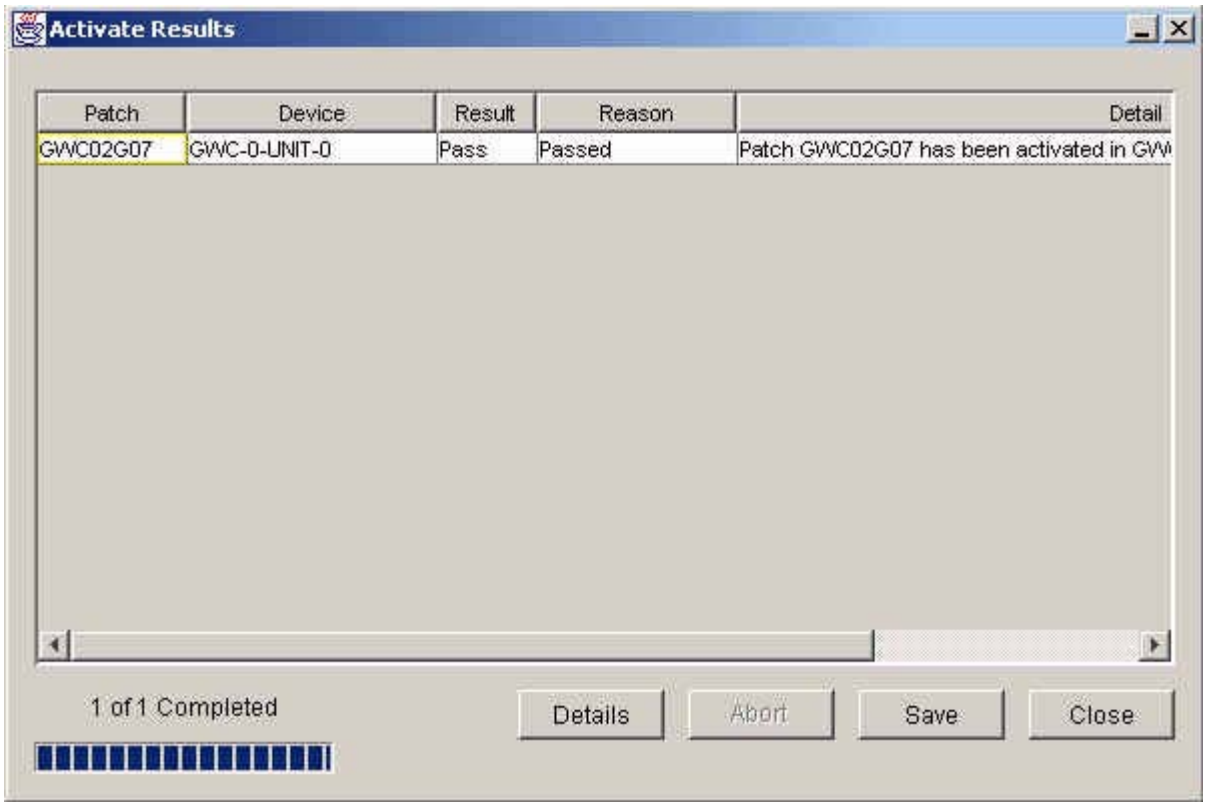
The results of the Pre-activate phase are displayed.



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. If applicable, return to the high level task or procedure that directed you to 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 1923
- Using the NPM GUI on page 1924

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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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.

You have completed this procedure.

Using the NPM GUI

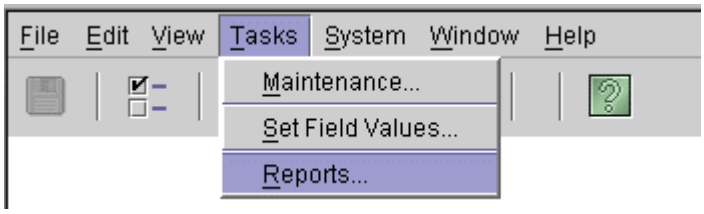
At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

At the NPM GUI

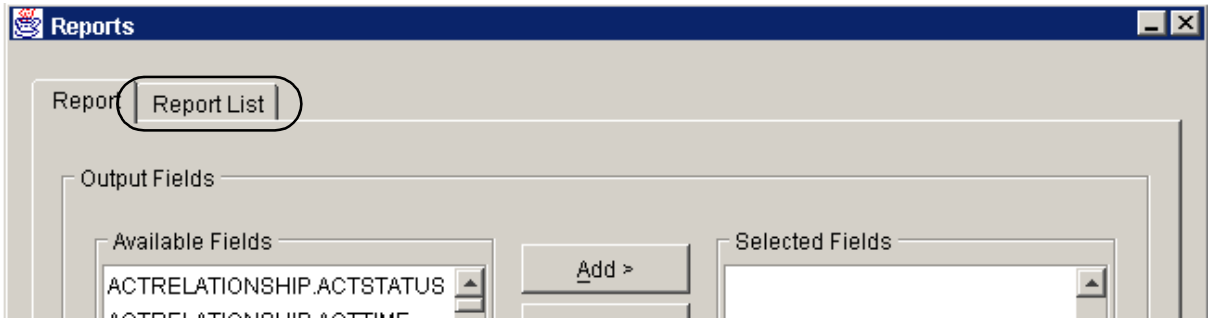
2 Query the NPM for a list of patches that are activated as follows:

a On the **Tasks** menu, click **Reports...**.

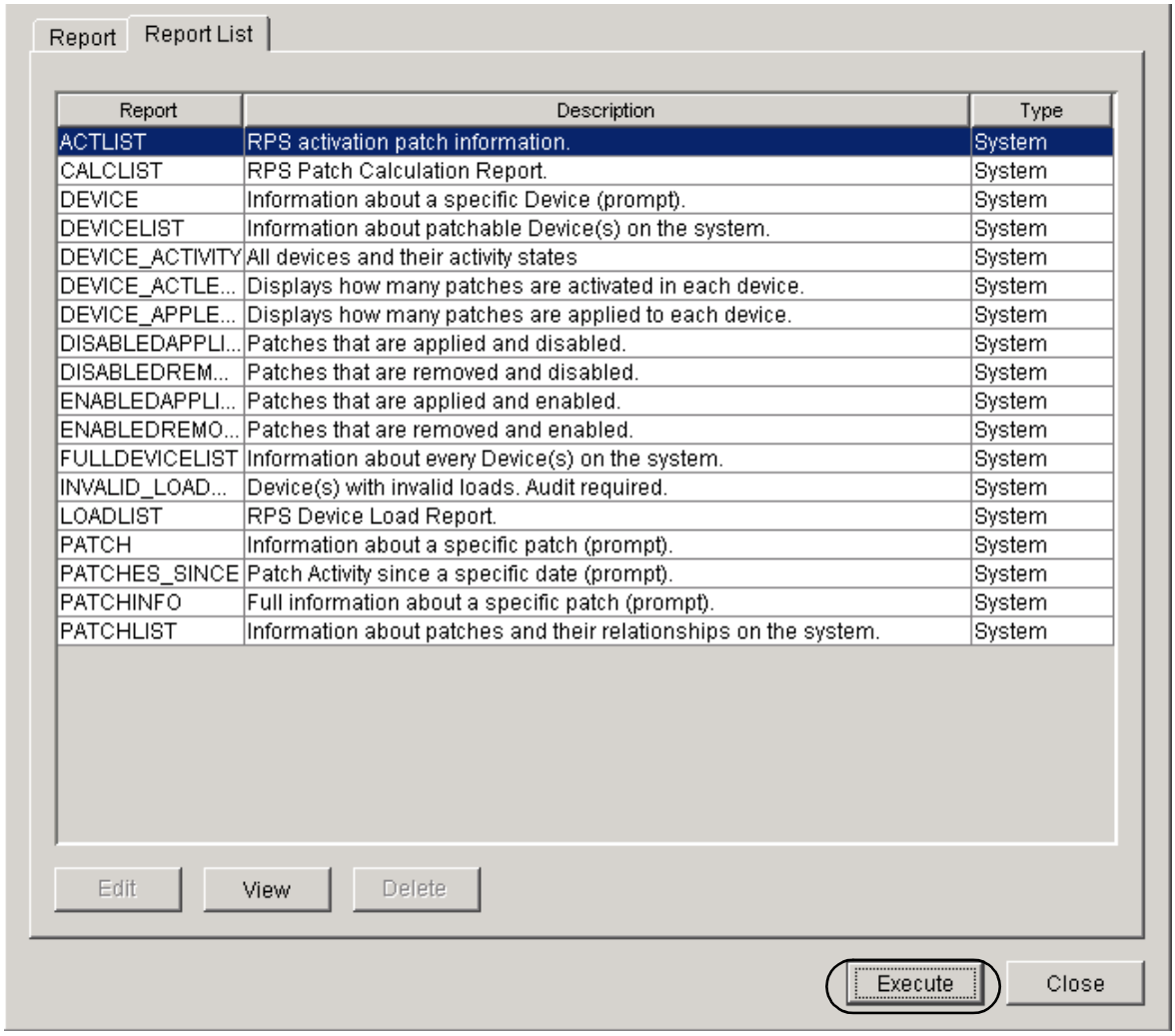


The Reports window is displayed.

b Click the **Report List** tab.

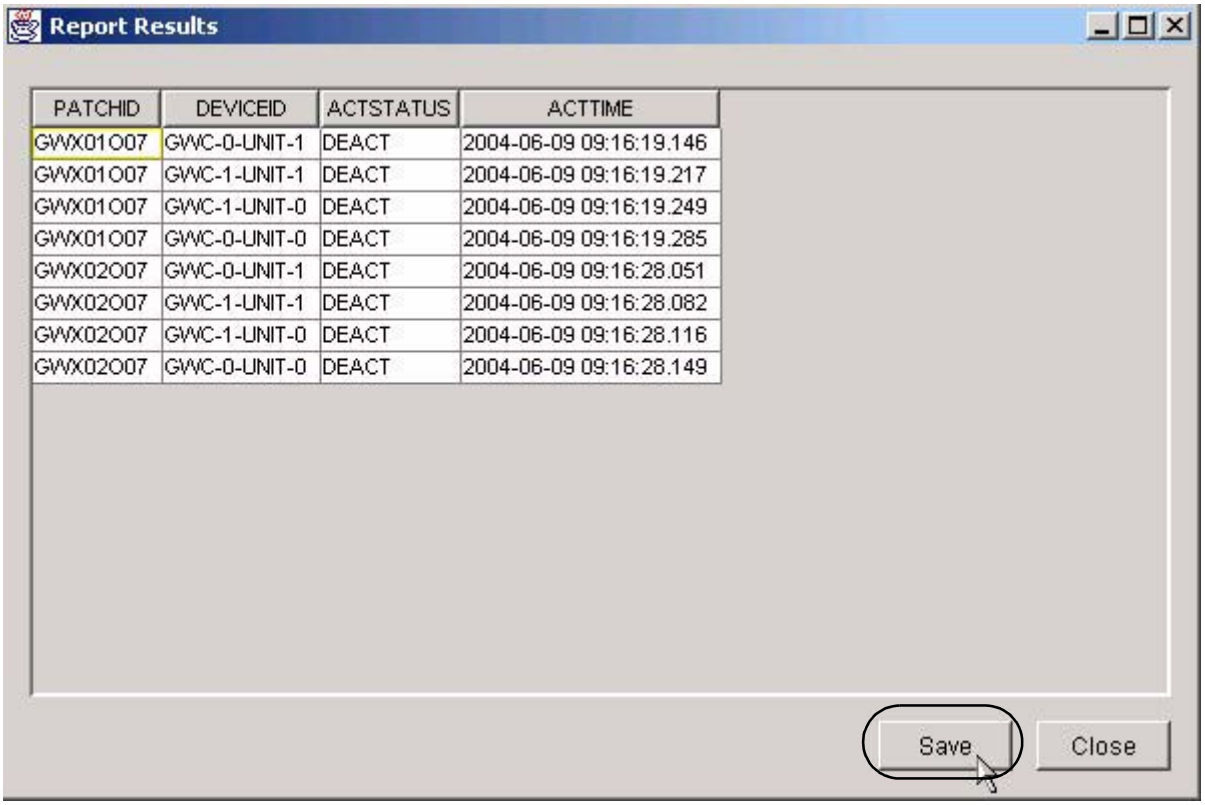


c Click the **ACTLIST** entry in the **Report** field, then click **Execute**.



d 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.

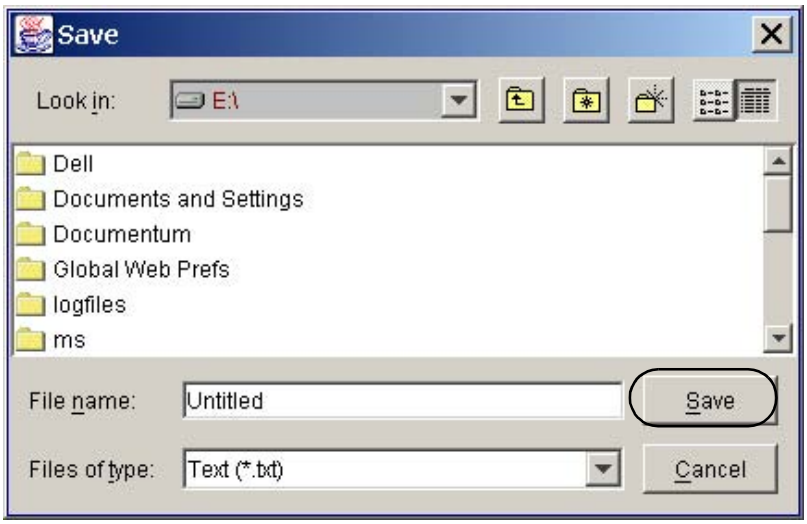
Note: If there are no patches to deactivate, the system returns a dialog box indicating that the report has “empty results”.



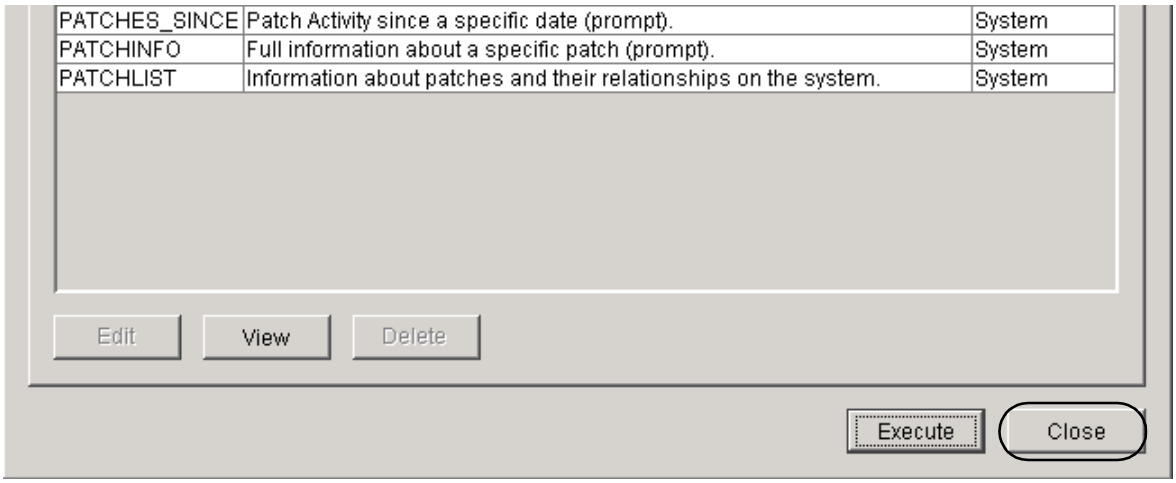
e If necessary, save a copy of the report to a text file as follows:

i Click **Save**.

ii Type a file name in the **File name:** box, and click **Save**.

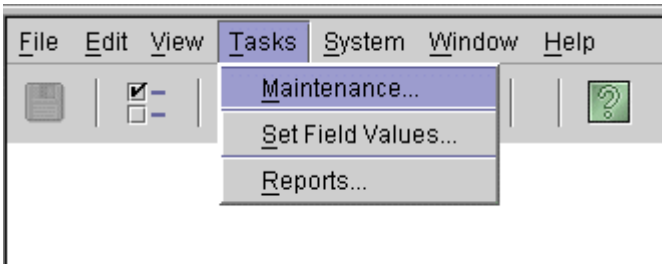


f Click **Close** to close the Reports window.



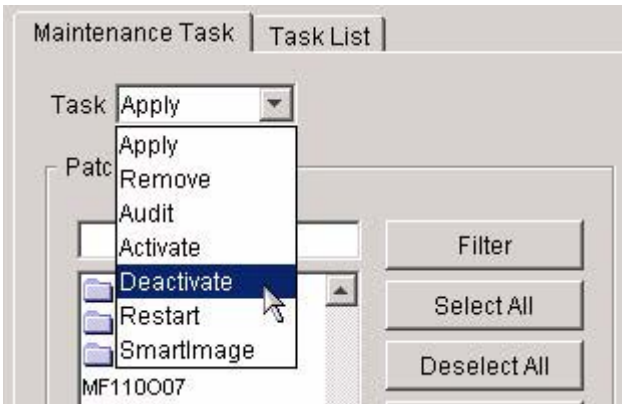
3 Deactivate one or more patches for one or more devices as follows:

a On the **Tasks** menu, click **Maintenance...**.



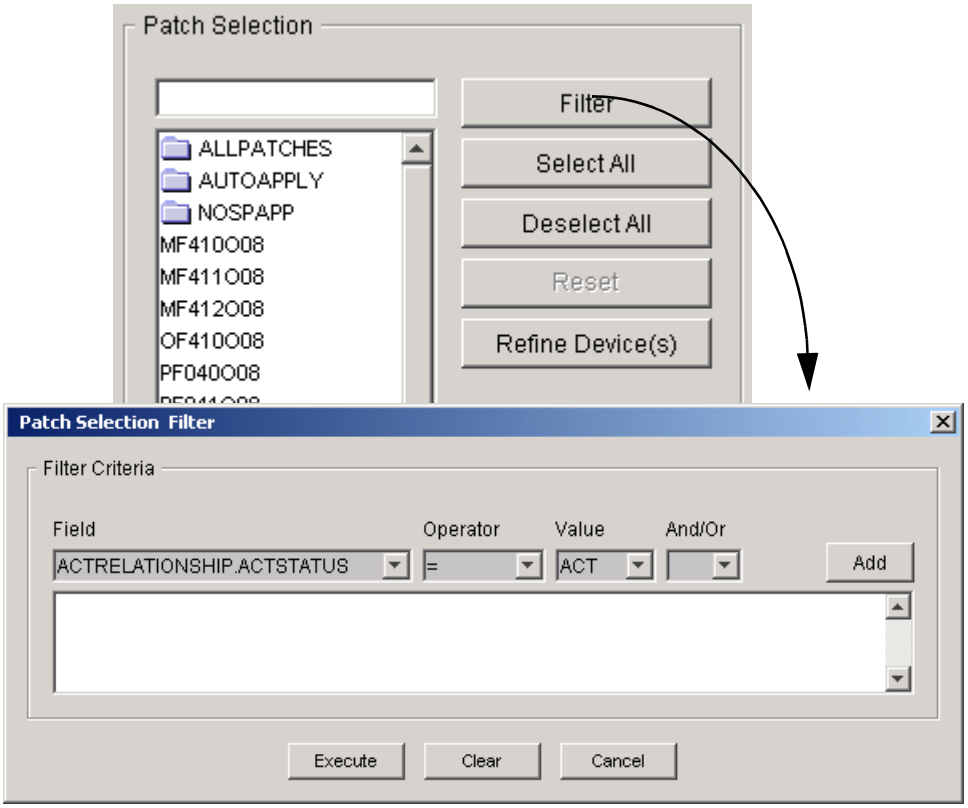
The Maintenance window is displayed.

b In the **Task** list, click **Deactivate**.



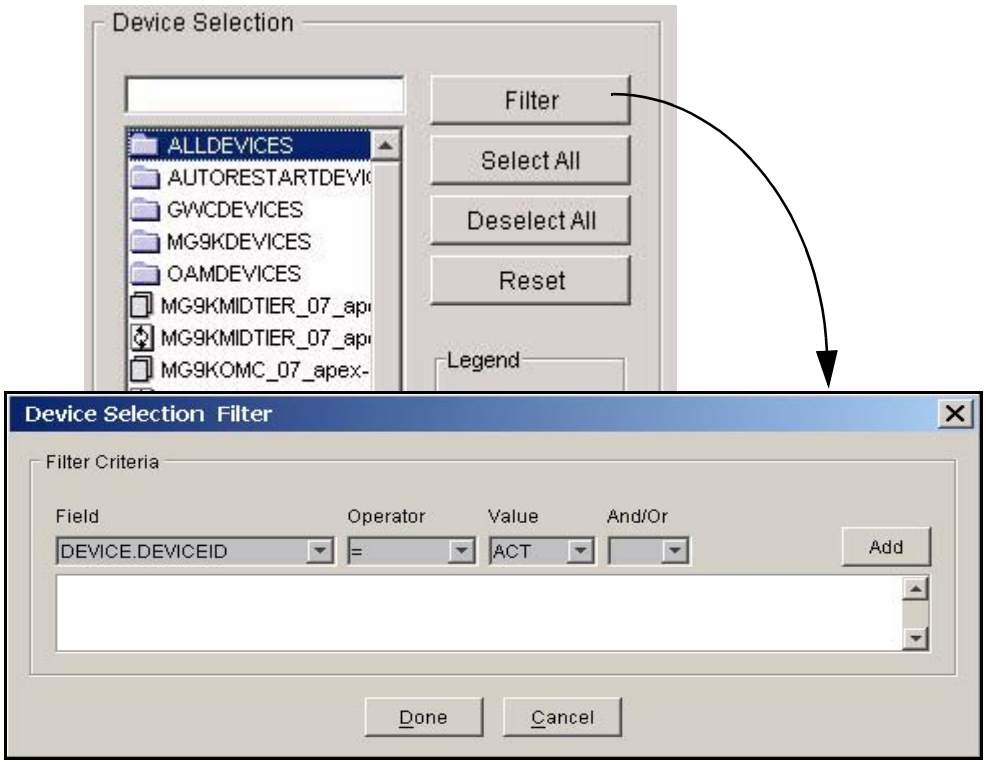
c In the **Patch Selection** list, select the patch files or patch sets you want to deactivate, then click **Refine Device(s)** to display a list of devices to which the patches apply.

To limit the patches displayed in the **Patch Selection** list, click **Filter** to configure a filtering criteria.

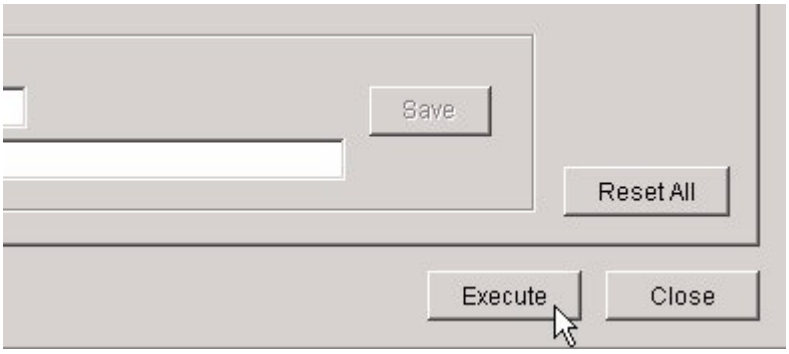


d In the **Device Selection** list, select the devices or device sets that have the applied patches you want to deactivate.

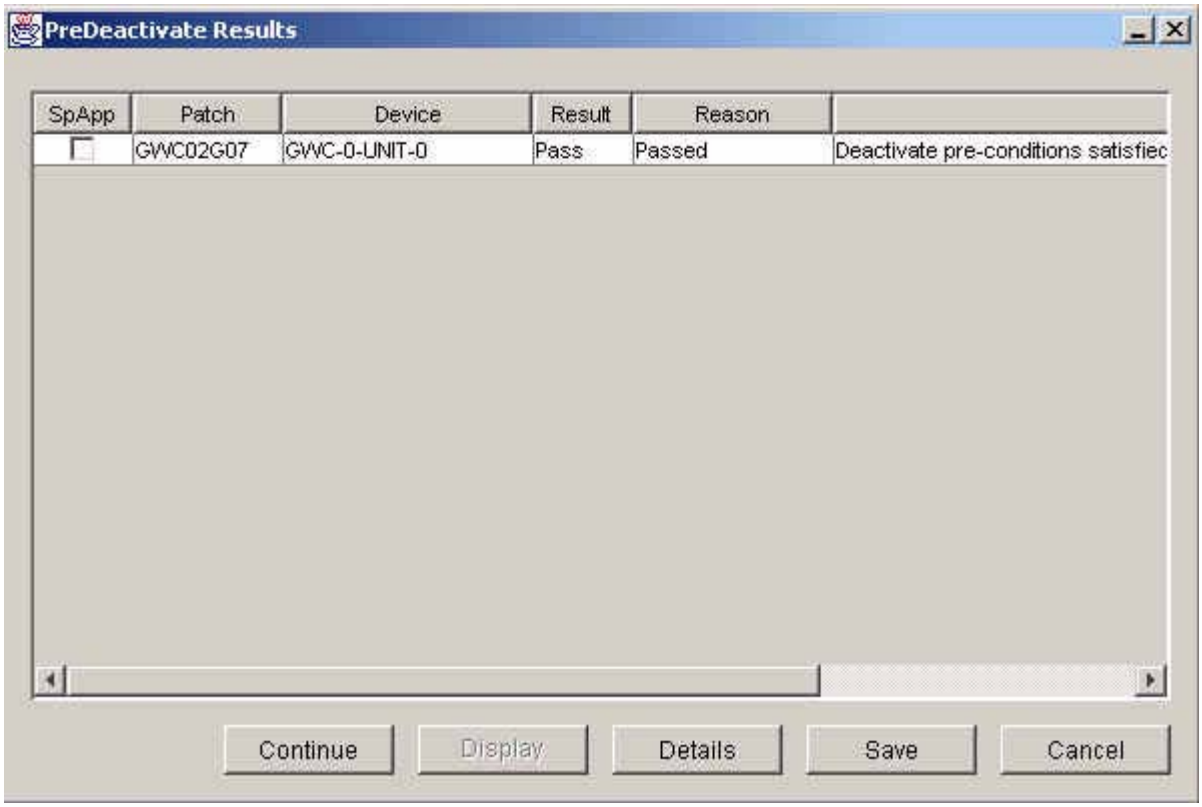
To limit the devices displayed in the **Device Selection** list, click **Filter** to configure a filtering criteria.



e Click **Execute** to begin the patch deactivation process.

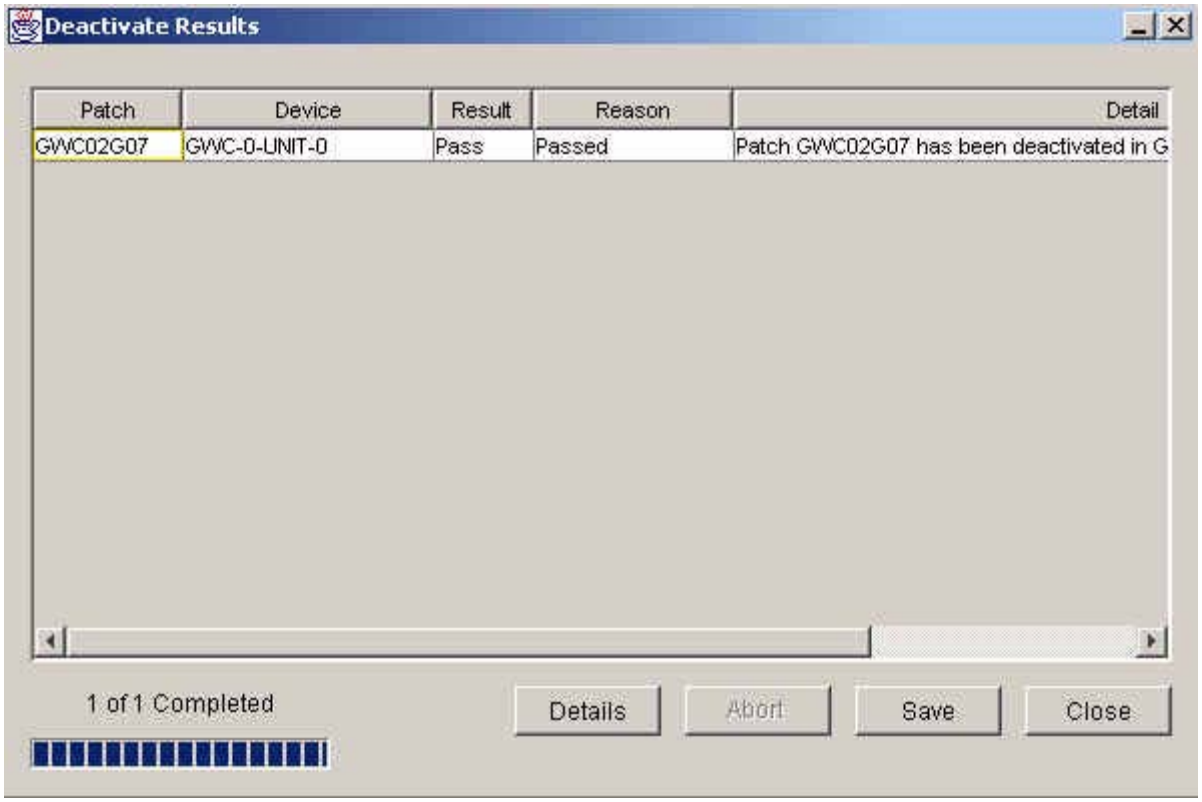


The results of the Pre-deactivate phase are displayed.



f 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.



g 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.

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 1934
- Using the NPM GUI on page 1937

Prerequisites

Before you remove ACT category patches, you must first deactivate the patches. Refer to procedure Deactivating patches using the NPM on page 1922 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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, efer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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 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:

- Patching Server Element (PSE)
- Integrated Element Management System (IEMS)
- Integrated EMS security components (IEMSCSS_DS and IEMSCSS)
- CS 2000 SAM21 Manager (SAM21EM)
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
- Core Element Manager (COREM)
- Network Patch Manager (NPM)

To restart a device, refer to procedure Restarting a device using the NPM on page 1943 if required.

You have completed this procedure.

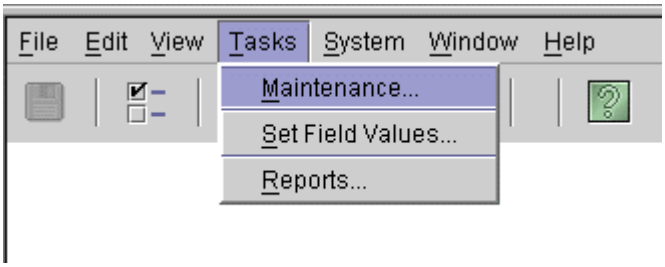
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866 if required.

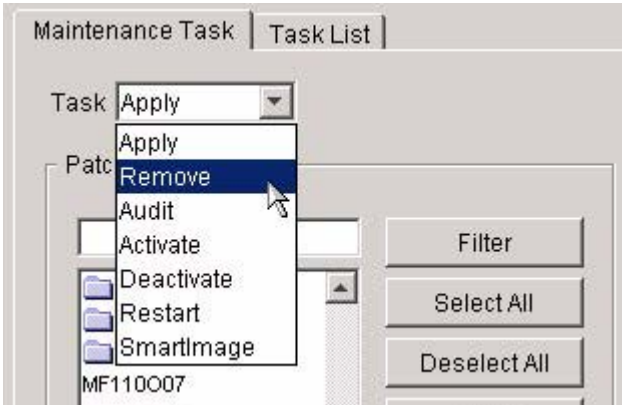
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.



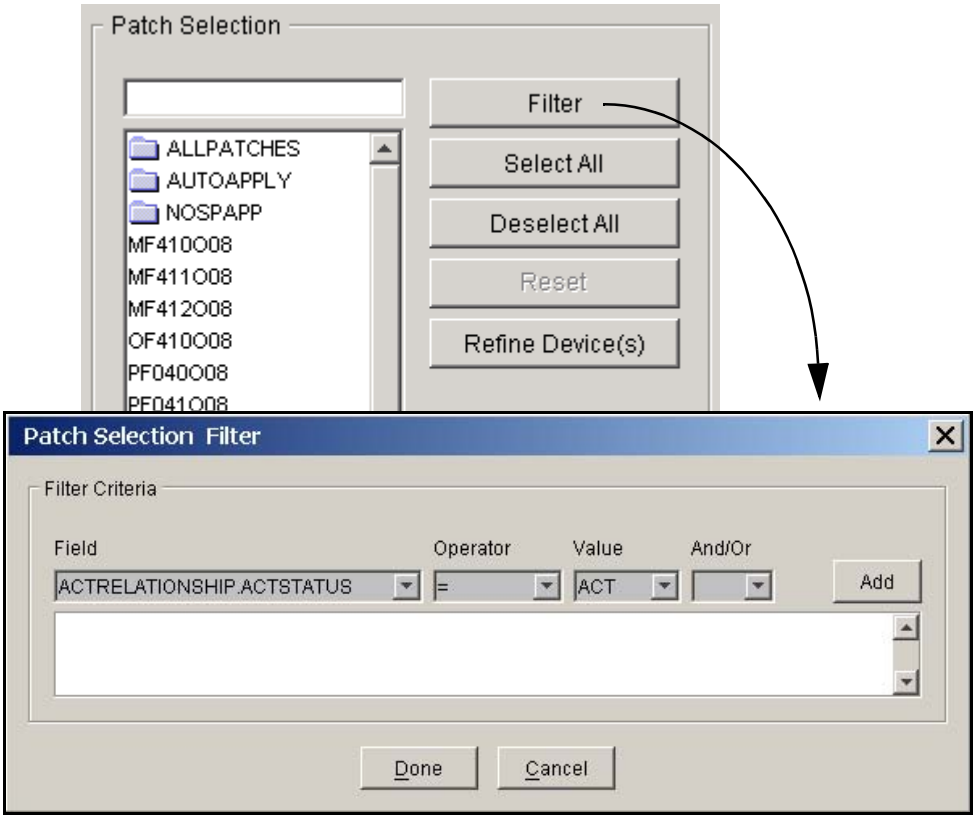
The Maintenance window is displayed.

3 In the **Task** list, click **Remove**.



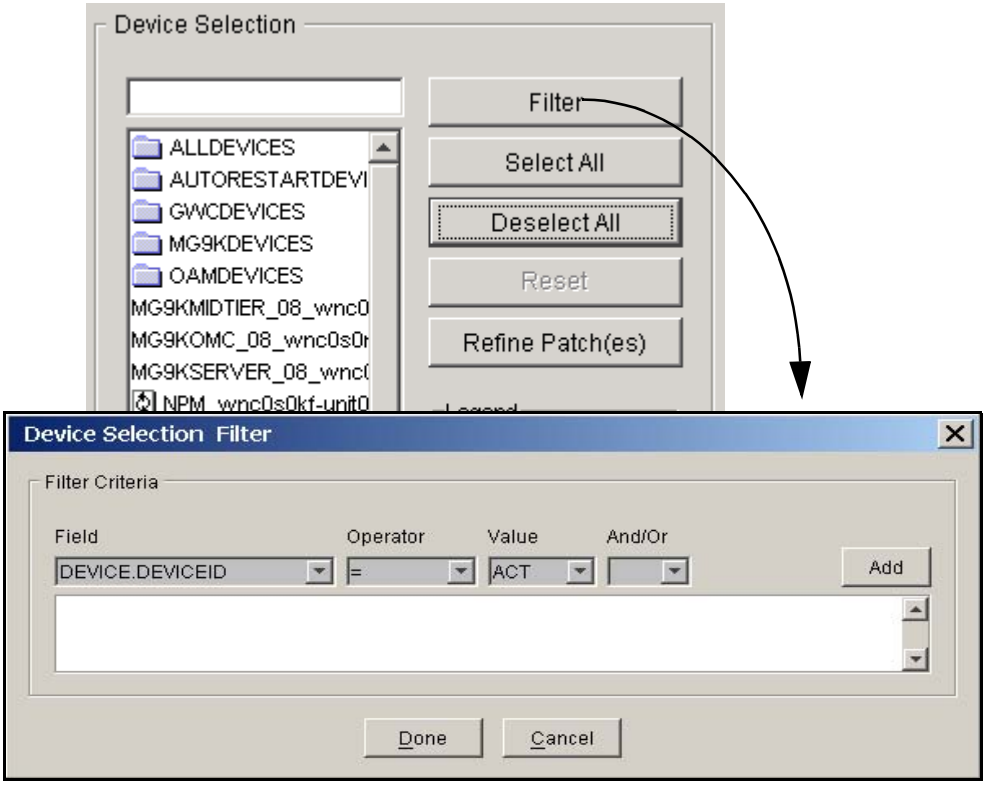
4 In the **Patch Selection** list, select the patch files or patch sets you want to remove, then click **Refine Device(s)** to display a list of devices to which the patches apply.

To limit the patches displayed in the **Patch Selection** list, click **Filter** to configure a filtering criteria.

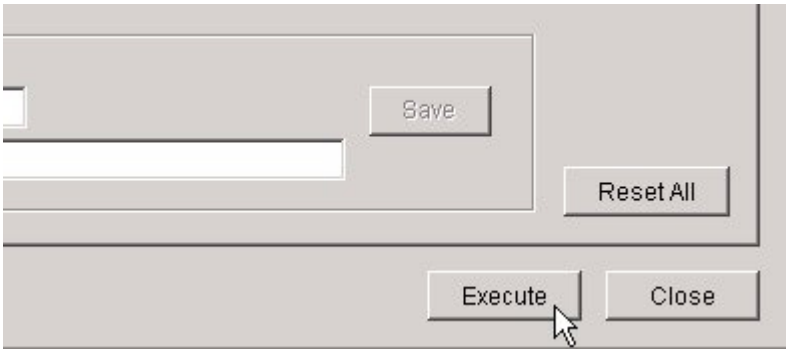


5 In the **Device Selection** list, select the devices or device sets from which you want to remove the patches.

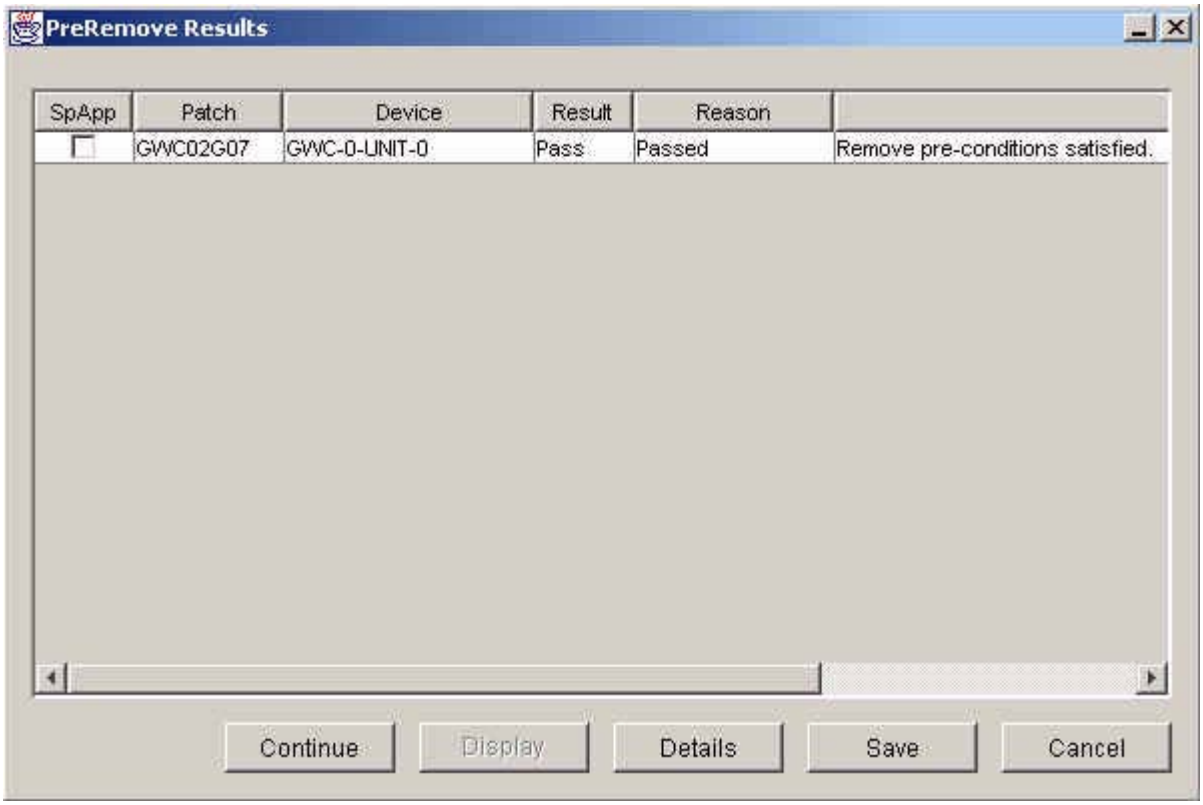
To limit the devices displayed in the **Device Selection** list, click **Filter** to configure a filtering criteria.



6 Click **Execute** to begin the patch removal process.



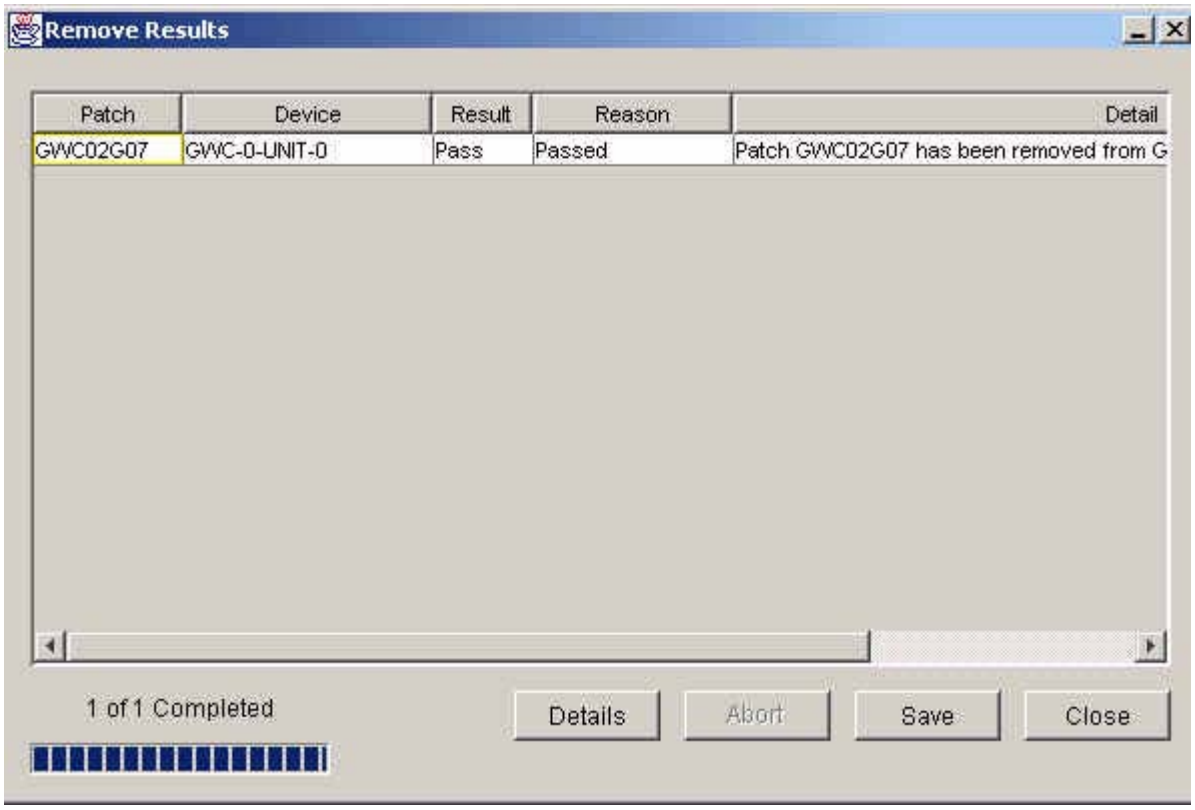
The results of the PreRemove phase are displayed.



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 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 (IEMS)
- Integrated EMS security components (IEMSCSS_DS and IEMSCSS)
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager (SAM21EM)
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
- Network Patch Manager (NPM)
- Core Element Manager (COREM)

To restart a device, refer to procedure Restarting a device using the NPM on page 1943 if required.

You have completed this procedure.

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 1944
- Using the NPM GUI on page 1947

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:

- Patching Server Element (PSE)
- Integrated Element Management System (IEMS)
- IEMS security components (IEMSCSS_DS and IEMSCSS)
- CS 2000 SAM21 Manager (SAM21EM)
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
- Core Element Manager (CEM)
- 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
- You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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` SESM_mws0c0ld

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_mws0c0ld

Result: true

Reason: Passed

Details: Device SESM_mws0c0ld 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_mws0c0ld

Reason: Passed

Detail: Restart passed on device SESM_mws0c0ld.

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 a PSE or NPM device has been successfully restarted, Nortel Networks recommends that you perform an audit on the PSE or NPM 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, refer to procedure Performing a device audit using the NPM on page 1879 if required.

You have completed this procedure.

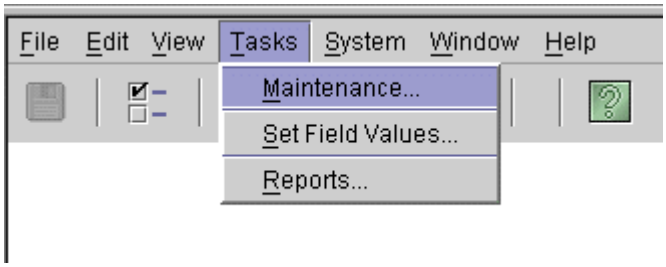
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

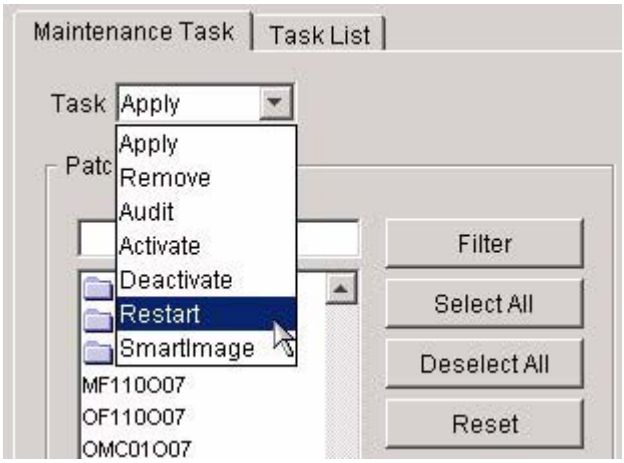
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.

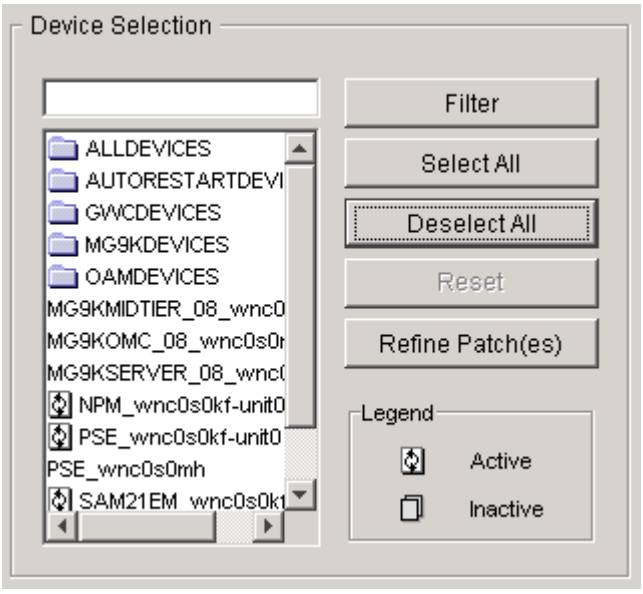


The Maintenance window is displayed.

3 In the **Task** list, click **Restart**.

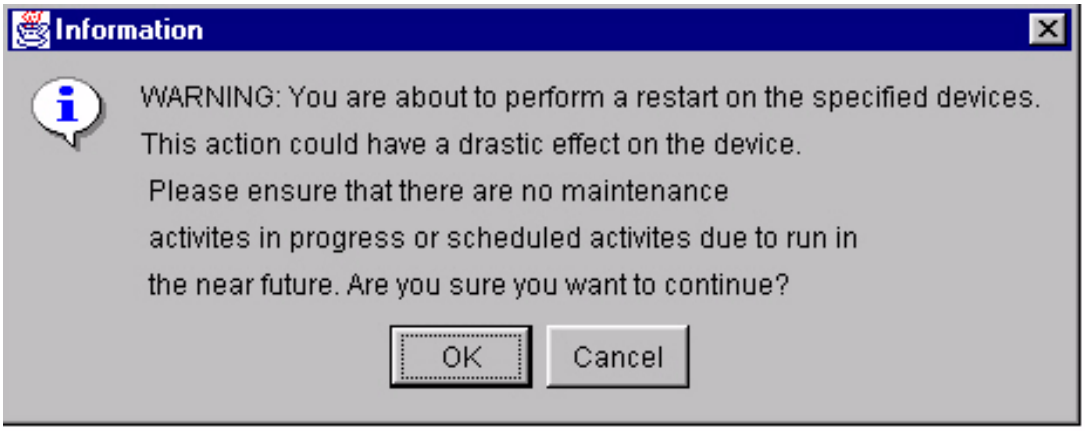


4 In the **Device Selection** list, select the device, device list, or device set that you want to restart.



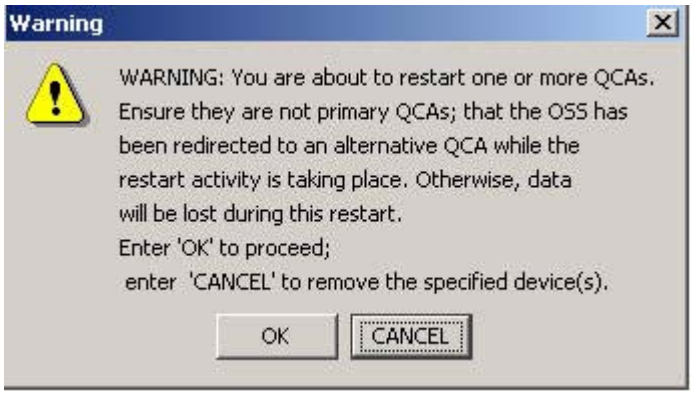
5 Click **Execute** to begin the restart.

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:

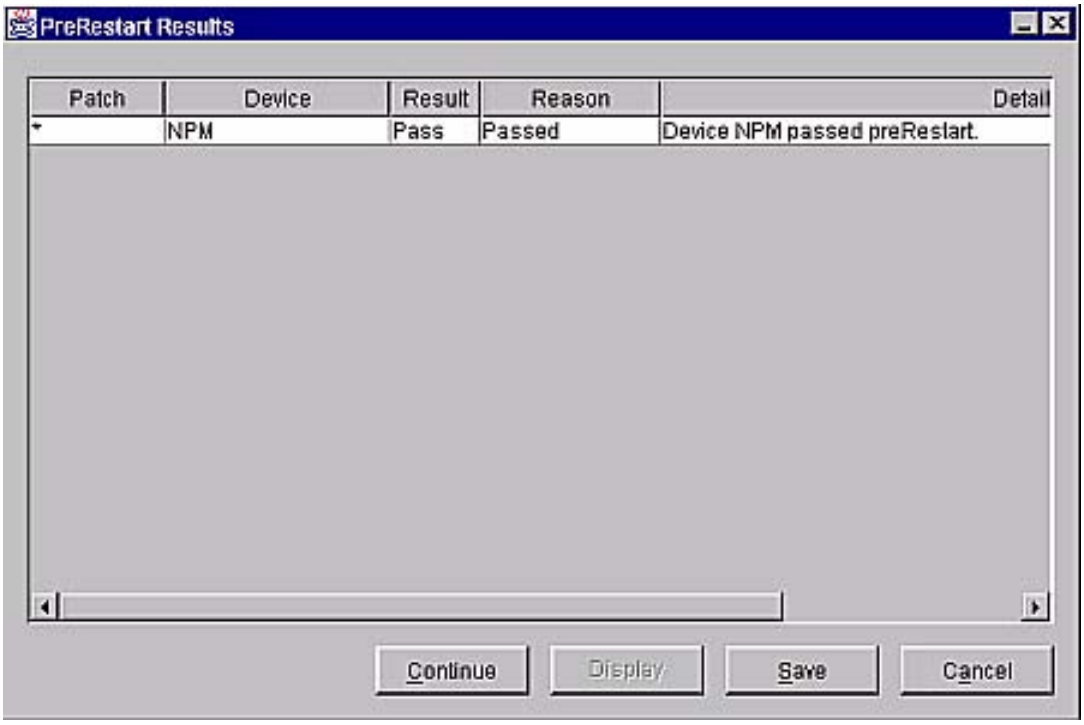


7

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 PSE or NPM device has been successfully restarted, Nortel Networks recommends that you perform an audit on the PSE or NPM 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, refer to procedure Performing a device audit using the NPM on page 1879 if required.

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 1952
- Using the NPM GUI on page 1953

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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

At the NPM CLUI

2 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.

You have completed this procedure.

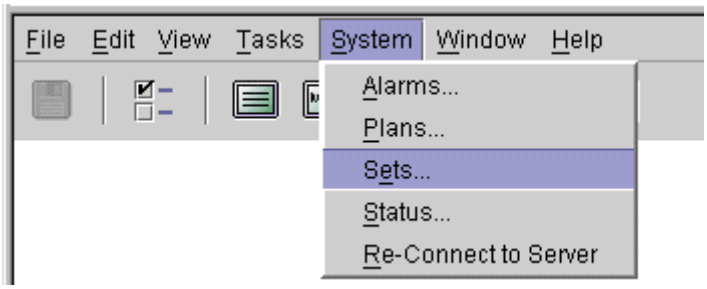
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

At the NPM GUI

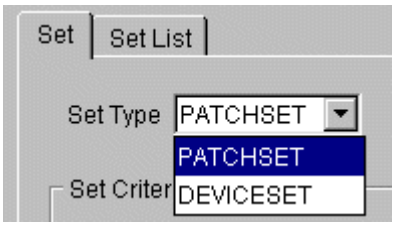
2 On the **System** menu, click **Sets...**.



The **Sets** window is displayed.

3 In the **Set Type** list, select PATCHSET to define a set of patches, or DEVICESET to define a set of devices.

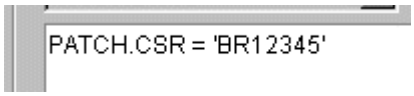
Note: You can also edit an existing set definition listed under the **Set List** tab, that contains similar criteria to the set you want to create, and save it under a new name.



4 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.

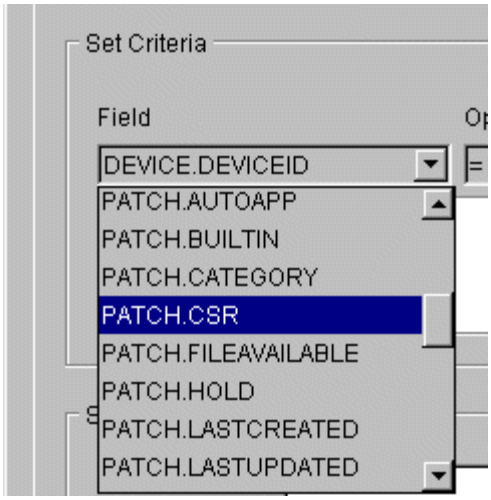
Note: Parenthesis "()" may be inserted to define precedence for multiple criteria statements.



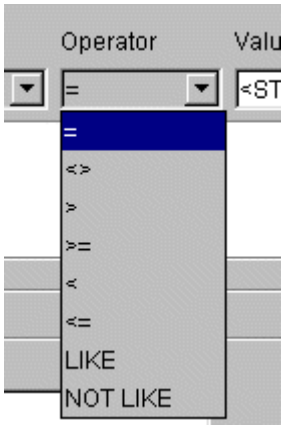
OR

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.

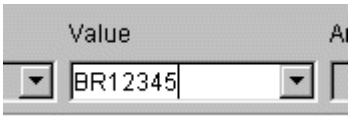


The following table lists the supported operators and their meaning.

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 (%)

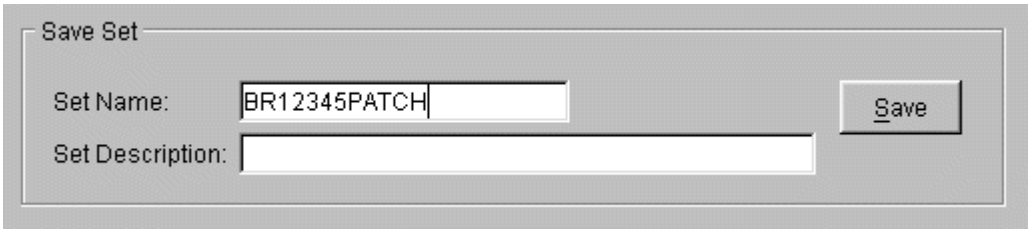
iii In the **Value** list, select the value of your choice.

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.

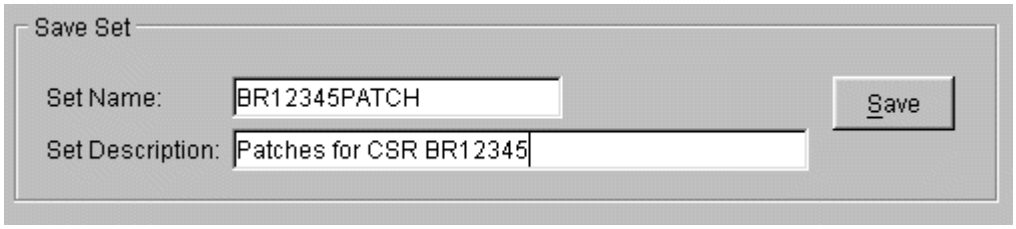


To combine multiple criteria statements, click **AND** or **OR** in the **And/Or** list.

5 Type a unique name for the set in the **Set Name** box.

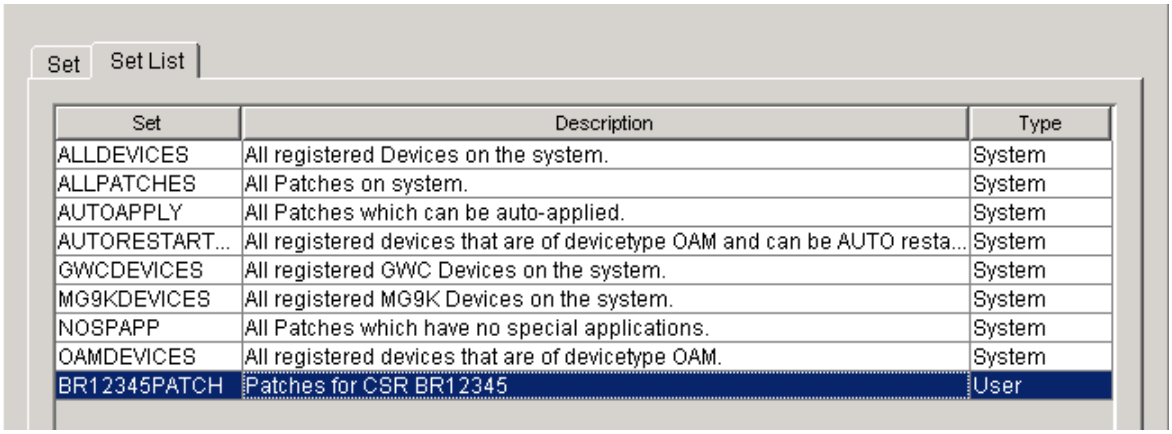


6 Type a description of the set in the **Set Description** box if desired.



7 Click **Save** to save the set.

The new set will be reflected under the **Set List** tab once the system has saved it.



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.

You have completed this procedure.

Defining a task using the NPM

Application

Use this procedure to define a task using the Network Patch Manager (NPM). You can define tasks using one of the following two NPM interfaces:

- Using the NPM CLUI on page 1957
- Using the NPM GUI on page 1959

A task is a definition of one type of maintenance activity that involves specific devices, and for some types of maintenance activities, can also involve patches. You can define a task for manual or automated execution.

The NPM is initially configured with the following system-defined tasks:

- AUTOAPPLY
- AUTORESTART
- AUDIT
- PFRSGETPATCH
- PFRSGENREPORT
- DELETEREPORTS

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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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
is the name of the task to be created

task_type
is the type of task (APPLYTASK, REMOVETASK, ACTIVATETASK, DEACTIVATETASK, AUDITTASK, RESTARTASK, or SMARTIMAGETASK)

task_desc
is a 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

Note: Tasks can only contain patchsets or devicesets, not single patches or devices. You can define 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.

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
```

You have completed this procedure.

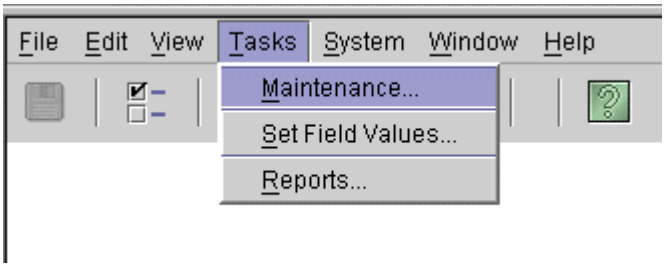
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

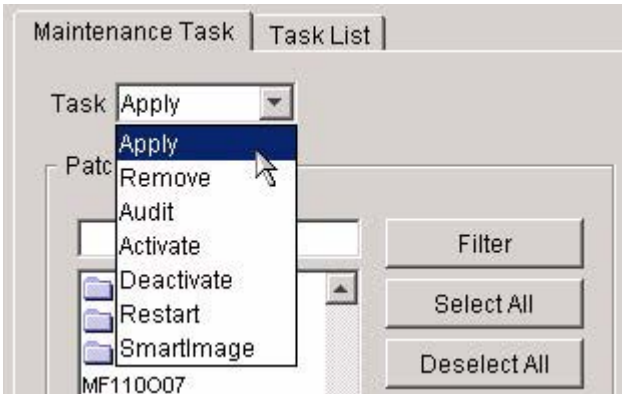
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.

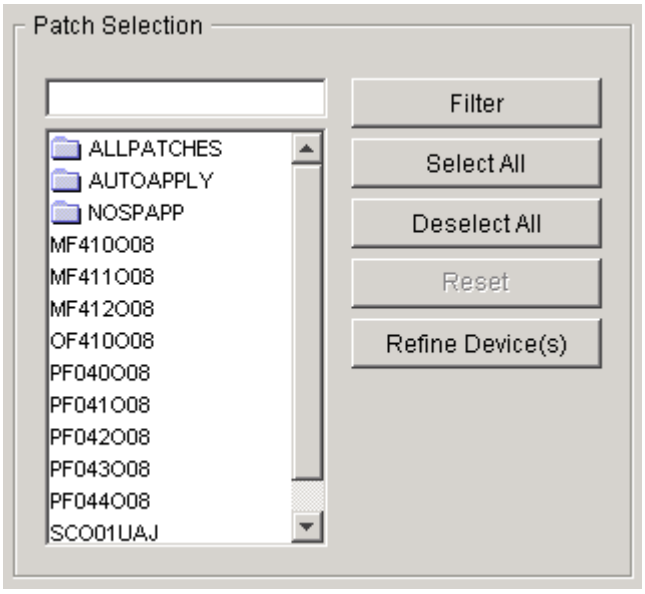


The **Maintenance** window is displayed.

3 In the **Task** list, click the task of your choice.

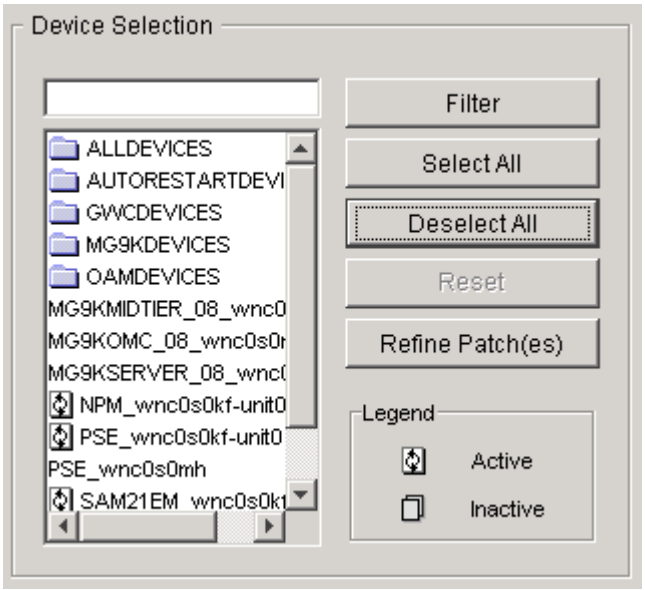


4 In the **Patch Selection** list, select the patch set (if applicable) you want to associate with the task.

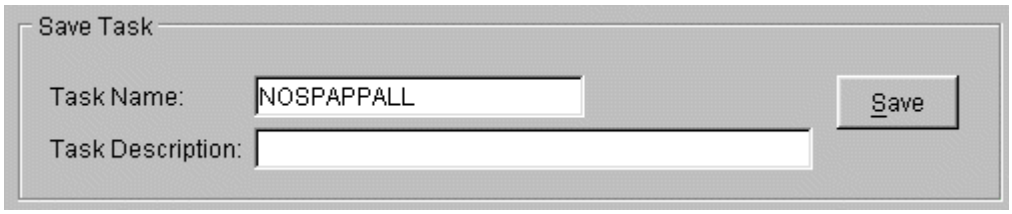


Note: Tasks can only contain patchsets or devicesets, not single patches or devices. You can define a task that applies one patch to one device by putting the patch in a single-member patchset and the device in a single-member deviceset and then applying the patchset to the deviceset.

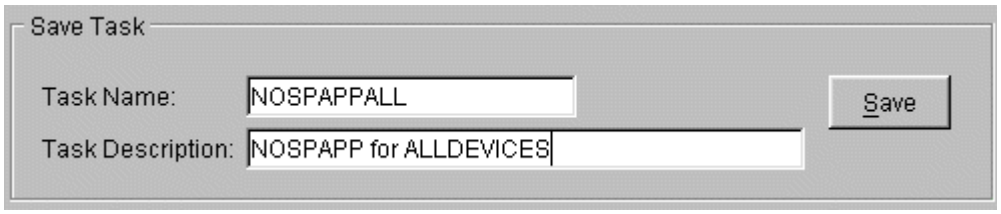
5 In the **Device Selection** list, select the device set you want to associate with the task.



6 Type a unique name for the task in the **Task Name** box.

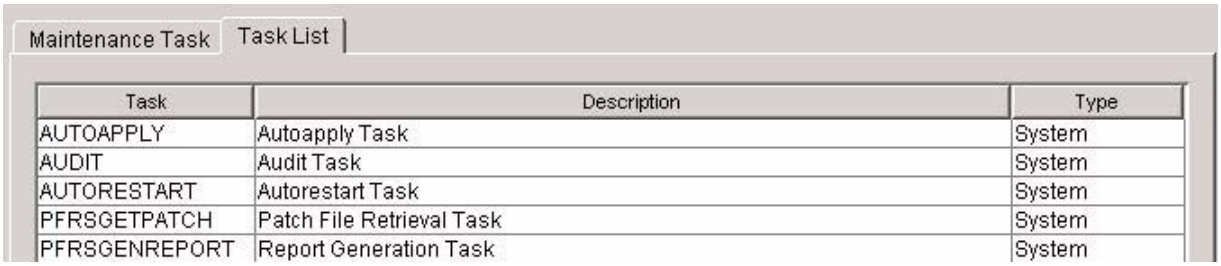


7 Optionally, type a description of the task in the **Task Description** box.



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.



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 1962
- Using the NPM GUI on page 1964

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 can be used is when a new patch is applied to a single device for a test period, without applying the patch to the remaining devices. After the test period, the patch is then 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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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 that follows, determine the Field and Value 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.

Field and Value combinations

Field	Value	Result
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. If applicable, return to the high level task or procedure that directed you to this procedure.

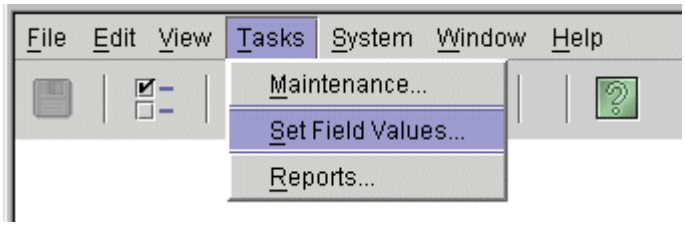
Using the NPM GUI

At your workstation

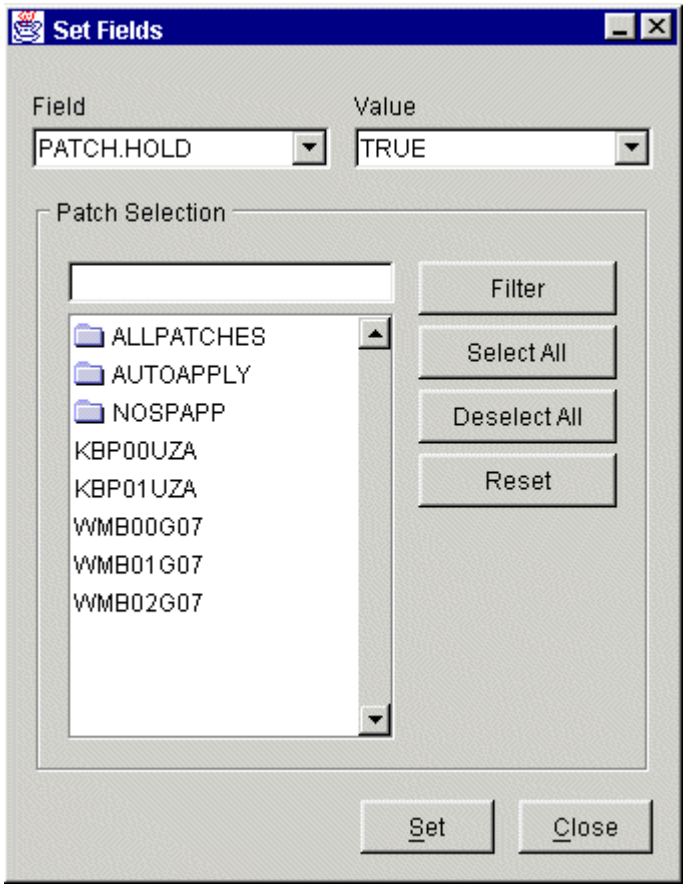
1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

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 Value to select.

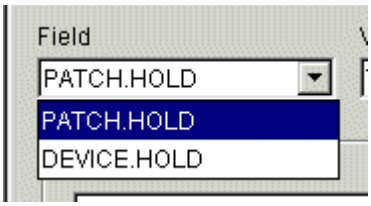
Field and Value combinations

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.

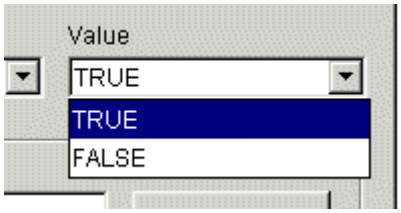
Field and Value combinations

Field	Value	Result
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.

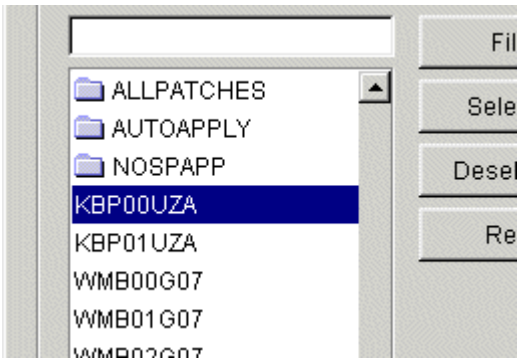
4 In the Field list, click **PATCH.HOLD** or **DEVICE.HOLD**.



5 In the Value list, click **TRUE** or **FALSE**.

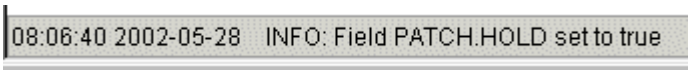


6 In the Patch Selection list (if you clicked PATCH.HOLD), select one or more patches, or in the Device Selection list (if you clicked DEVICE.HOLD), select one or more devices.



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. If applicable, return to the high level task or procedure that directed you to 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 1969
- Using the NPM GUI on page 1970

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.

The NPM is initially configured with the following system-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 1879, 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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

At the NPM CLUI

2 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

Use the command **viewtabs** to obtain a list of all the fields in the database that you can use in a 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'"
```

3 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

You have completed this procedure.

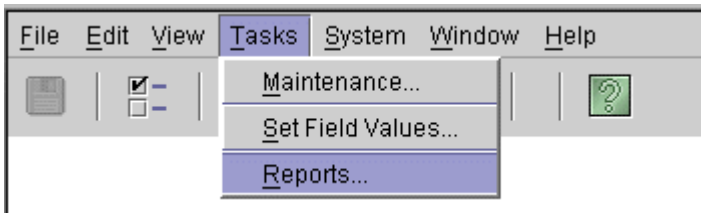
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

At the NPM GUI

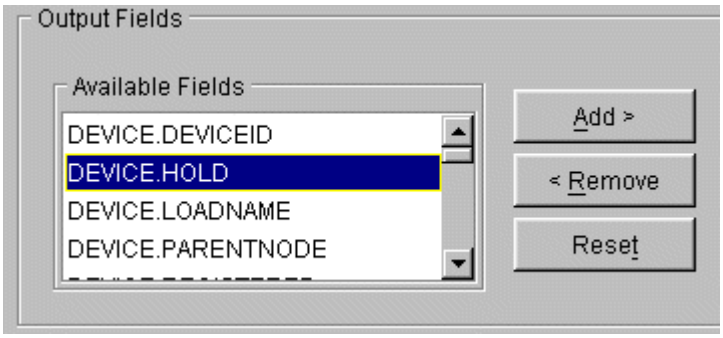
2 On the **Tasks** menu, click **Reports...**.



3 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.



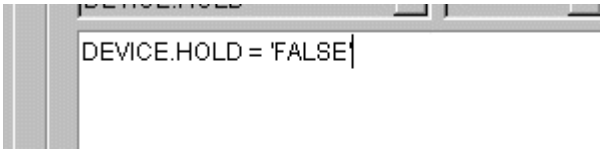
b Click **Add** to add the field to the **Selected Fields** list.

c Repeat Steps 3a and 3b for each field, then proceed to step 4.

4 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.

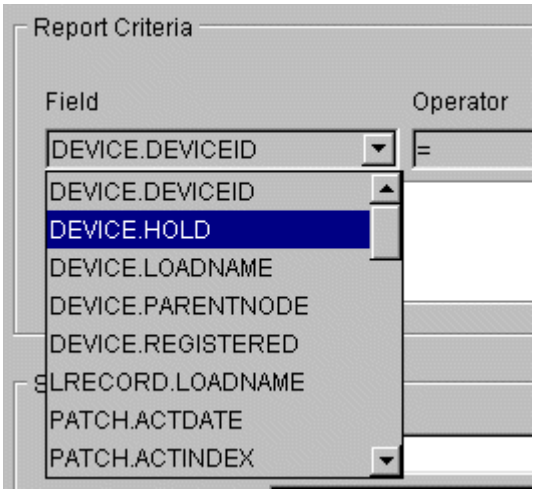
Note: Parenthesis "()" may be inserted to define precedence for multiple criteria statements.



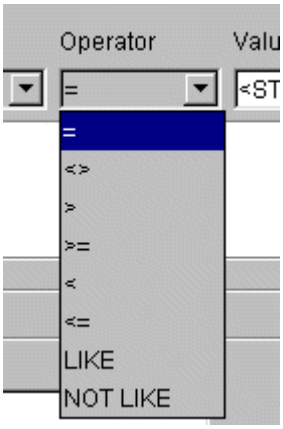
OR

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.



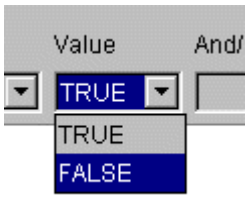
The table below lists the supported operators and their meaning.

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.



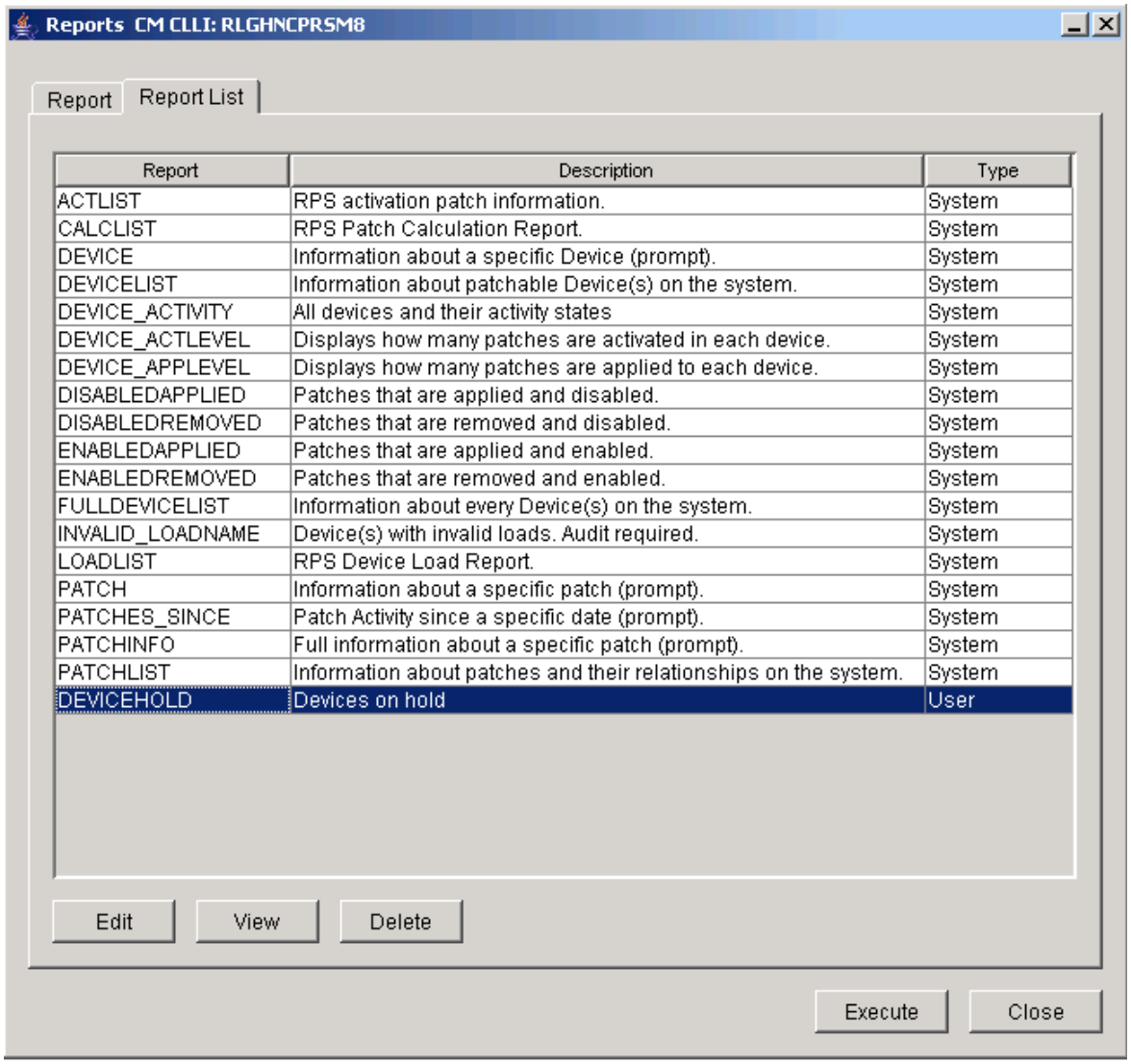
To combine multiple criteria statements, click **AND** or **OR** in the **And/Or** list.

5 Type a unique name for the report in the **Report Name** box.

6 Type a description of the report in the **Report Description** box if desired.

7 Click **Save** to save the report.

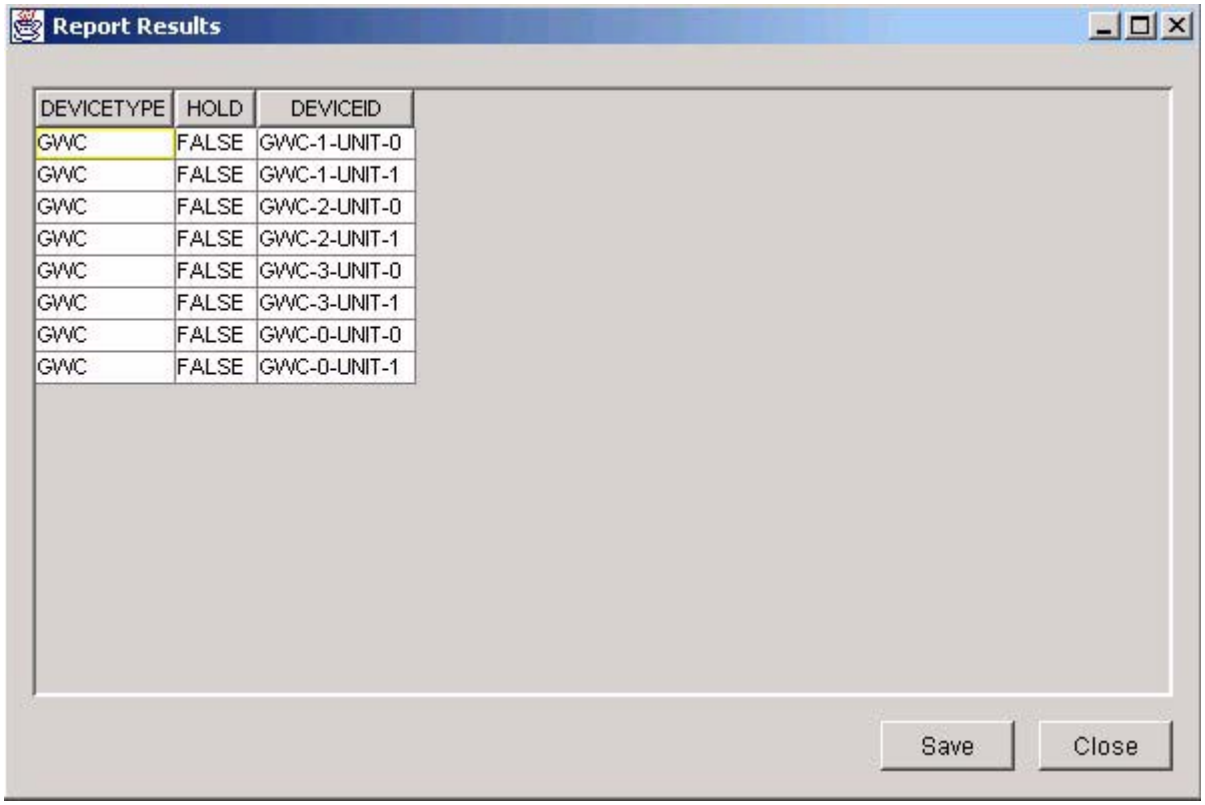
The new report will be reflected under the **Report List** tab once the system has saved it as shown below.



8 Click **Execute** to generate the report.

The system displays the Report Results window.

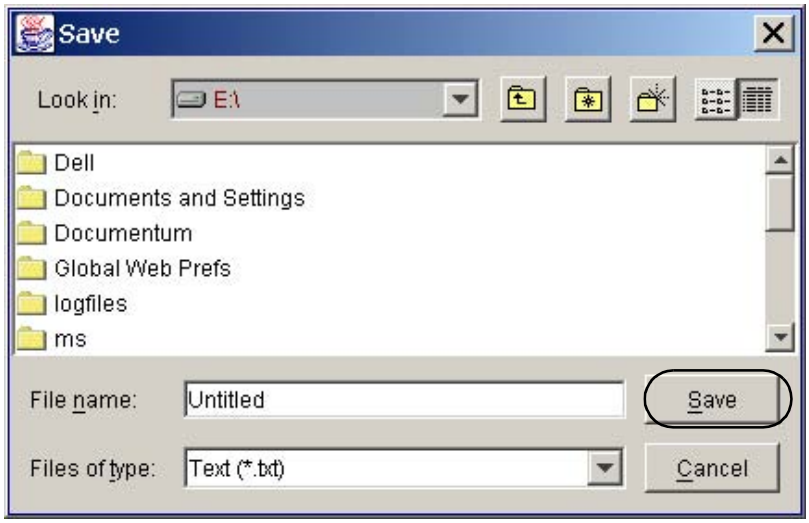
Note: The time required to generate the report depends on the number of patches and devices in the database and the complexity of the search criteria.



9 If necessary, save a copy of the report to a text file as follows:

a Click **Save** in the Report Results window.

b Type a file name in the **File name:** box, and click **Save**.



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 1978
- Using the NPM GUI on page 1980

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.

The NPM is initially configured with the following system-defined plans:

- SYSTEMPLAN (initially defined with the AUTOAPPLY and AUTORESTART tasks)
- REPORTCLEANUP (initially defined with the DELETEREPORTS task)
- GETPATCH (initially defined with the PFRSGETPATCH task)
- GENREPORT (initially defined with the PFRSGENREPORT task)

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.

The NPM supports a maximum of eight plans, therefore, four plans can be defined in addition to the four system-defined plans.

Note: You can enable or disable system-defined plans, modify their definition, or delete them, however, you cannot rename them.

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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or

procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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
```

You have completed this procedure.

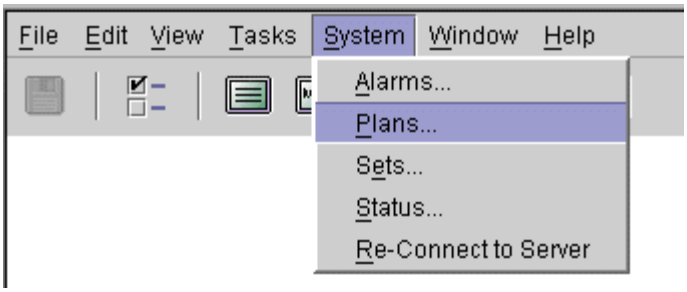
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

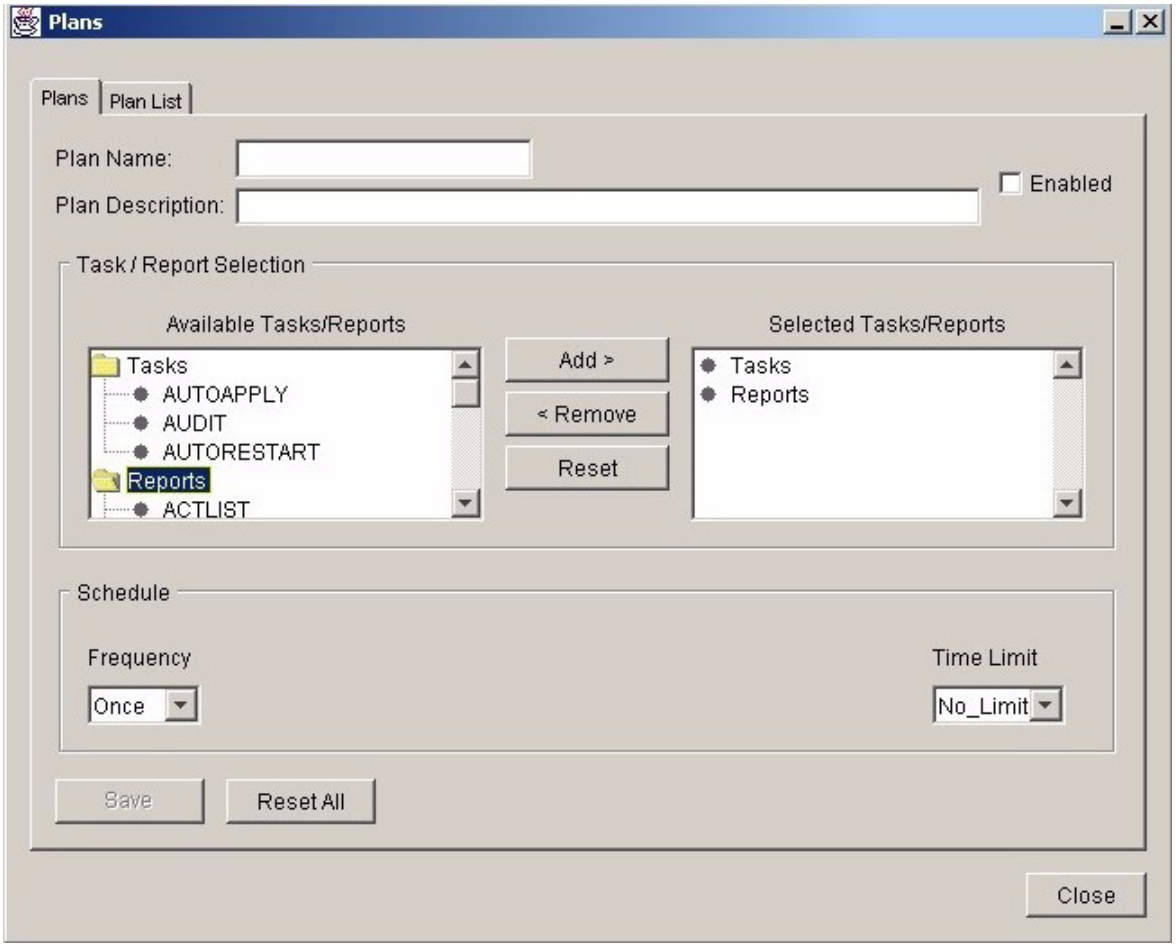
At the NPM GUI

2 On the **System** menu, click **Plans...**.



The **Plans** window opens.

3 Click the **Plans** tab if not already displayed, and click **Reset All**.

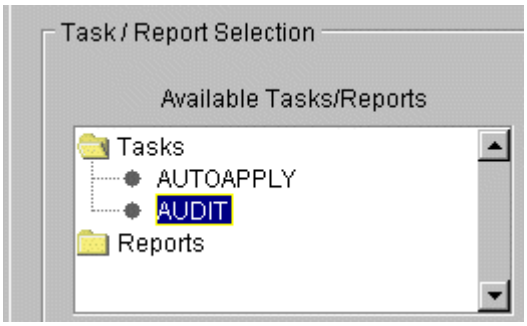


4 In the **Plan Name** box, type a unique name for the plan, and in the **Plan Description** box, type a description of the plan (optional).

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.

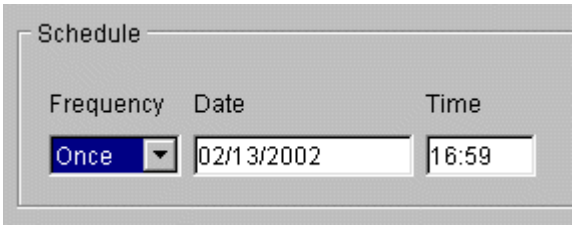
Note: You can use the **Shift** key to select multiple tasks or reports consecutively, or the **Ctrl** key to select multiple tasks or reports non-consecutively.

7 Specify the execution schedule in the **Schedule** are as follows:

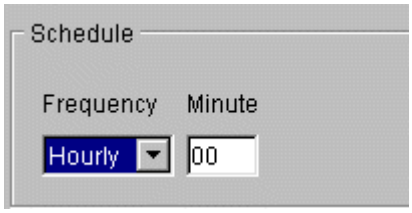
a In the **Frequency** list, click the frequency option of your choice.

When you select a frequency option, the related scheduling fields are displayed. An example of each frequency option and its related fields follows.

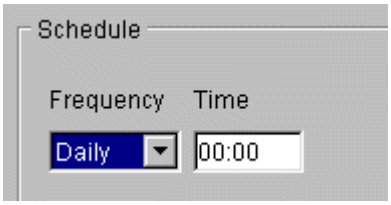
Once option



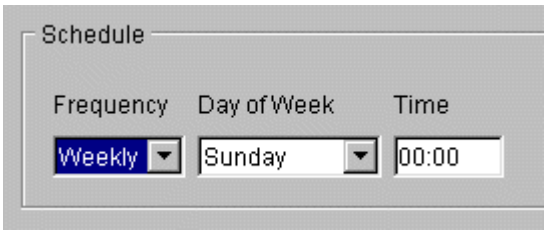
Hourly option



Daily option



Weekly option

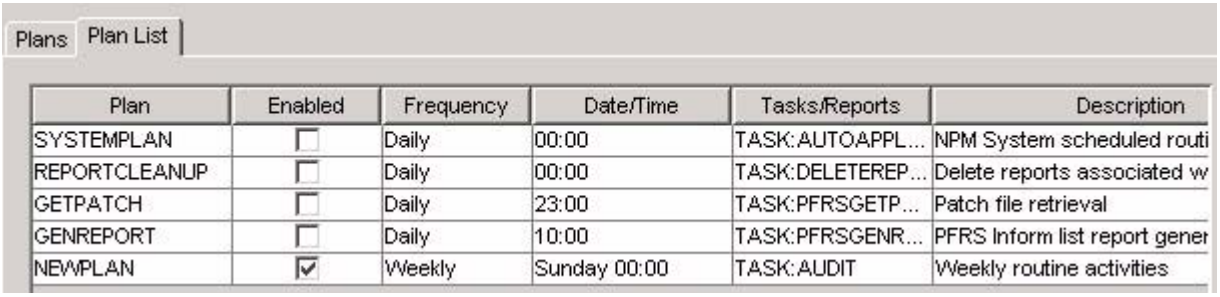


b Enter the appropriate scheduling information for the frequency option you selected.

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.



Plan	Enabled	Frequency	Date/Time	Tasks/Reports	Description
SYSTEMPLAN	☐	Daily	00:00	TASK:AUTOAPPL...	NPM System scheduled routi
REPORTCLEANUP	☐	Daily	00:00	TASK:DELETEREP...	Delete reports associated w
GETPATCH	☐	Daily	23:00	TASK:PFRSGETP...	Patch file retrieval
GENREPORT	☐	Daily	10:00	TASK:PFRSGENR...	PFRS Inform list report gener
NEWPLAN	☑	Weekly	Sunday 00:00	TASK:AUDIT	Weekly routine activities

9 Click **Close** to close the Plans window.

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 1986
- Using the NPM GUI on page 1990

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.

The NPM is initially configured with the following system-defined plans:

- SYSTEMPLAN (initially defined with the AUTOAPPLY and AUTORESTART tasks)
- REPORTCLEANUP (initially defined with the DELETEREPORTS task)
- GETPATCH (initially defined with the PFRSGETPATCH task)
- GENREPORT (initially defined with the PFRSGENREPORT task)

The system-defined plans cannot be renamed, but they can be modified or deleted.

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.

The NPM supports a maximum of eight plans, therefore, four plans can be defined in addition to the four system-defined plans.

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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864.

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

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

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

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

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.

You have completed this procedure.

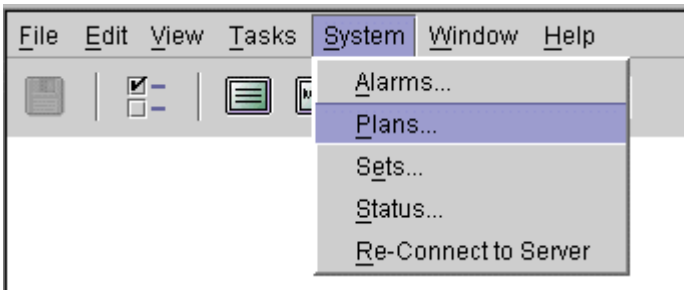
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

At the NPM GUI

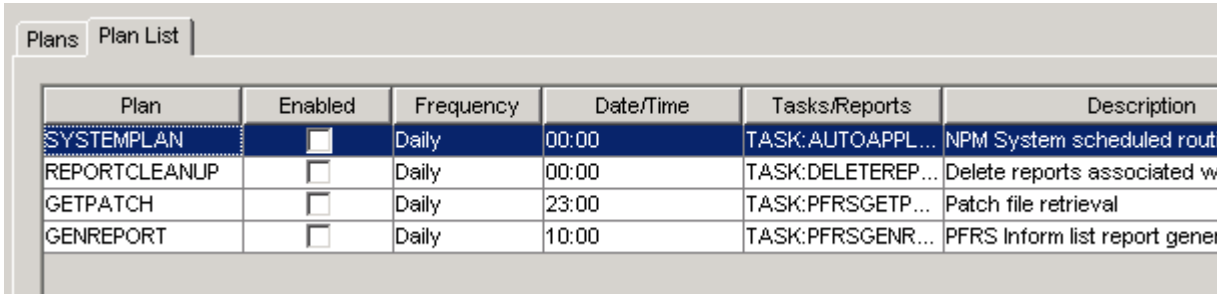
2 On the **System** menu, click **Plans...**.



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

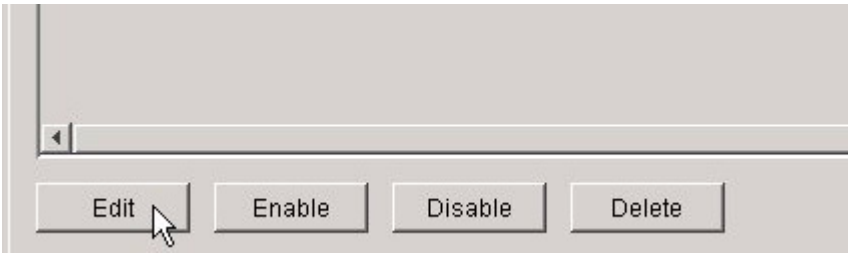
c Allow any non-completed tasks to finish.

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.

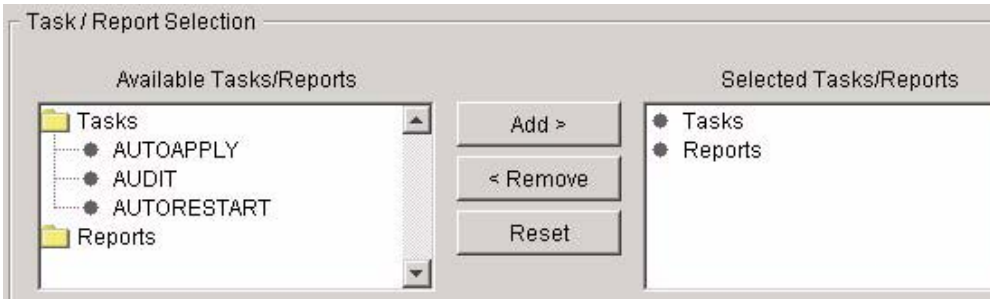
Proceed to step 13.

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.

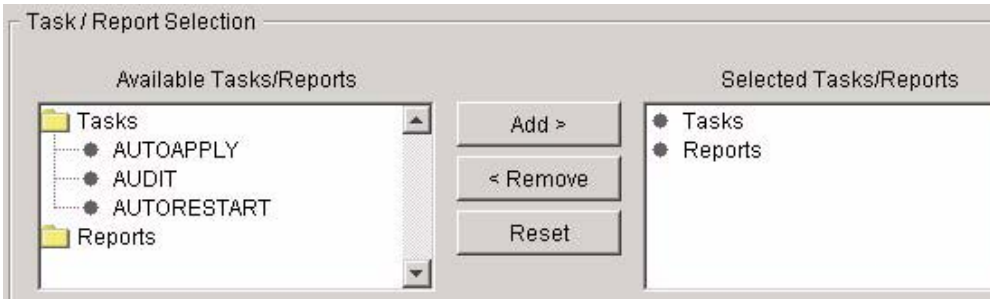
d Repeat step 10a and 10b for each task or report you want to add to the plan.

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.

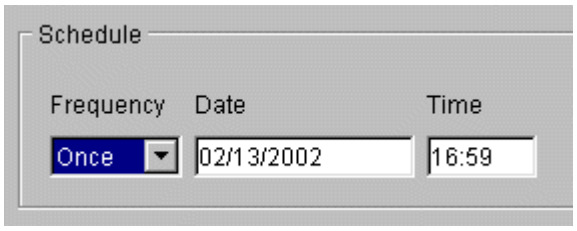
Proceed to step 13.

12 In the **Schedule** area, update the plan schedule if required, as follows:

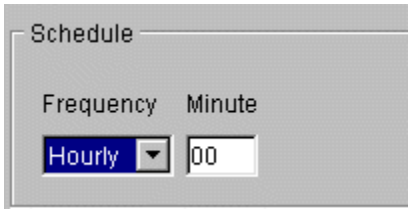
a In the **Frequency** list, click the frequency option of your choice.

When you select a frequency option, the related scheduling fields are displayed. An example of each frequency option and its related fields follows.

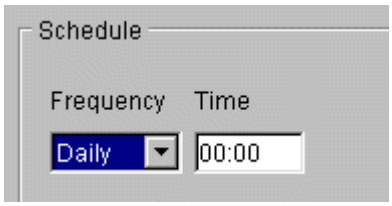
Once option



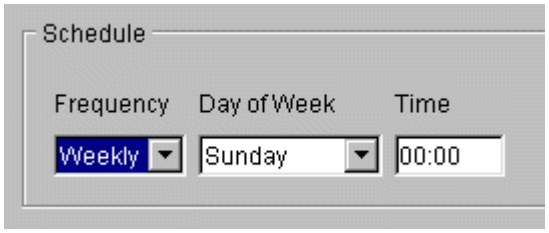
Hourly option



Daily option



Weekly option

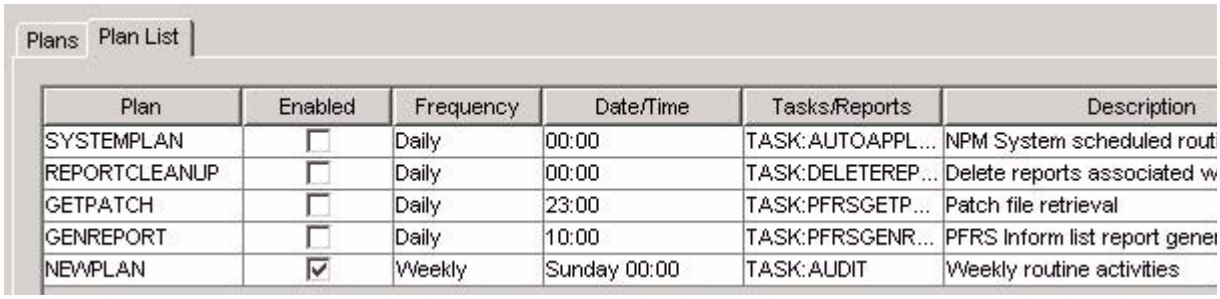


b Enter the appropriate scheduling information for the frequency option you selected.

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.

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 1998
- Using the NPM GUI on page 1999

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.

The NPM is initially configured with the following system-defined plans:

- SYSTEMPLAN (initially defined with the AUTOAPPLY and AUTORESTART tasks)
- REPORTCLEANUP (initially defined with the DELETEREPORTS task)
- GETPATCH (initially defined with the PFRSGETPATCH task)
- GENREPORT (initially defined with the PFRSGENREPORT task)

The system-defined plans cannot be renamed, but they can be modified or deleted.

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.

The NPM supports a maximum of eight plans, therefore, four plans can be defined in addition to the four system-defined plans.

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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864 .

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

You have completed this procedure.

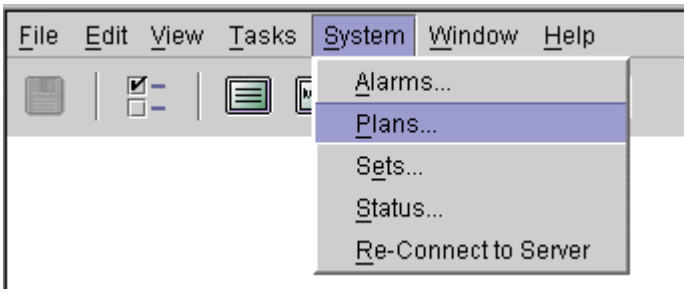
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

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.

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 2000
- Using the NPM GUI on page 2001

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” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

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. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 1864 .

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.

You have completed this procedure.

Using the NPM GUI

At your workstation

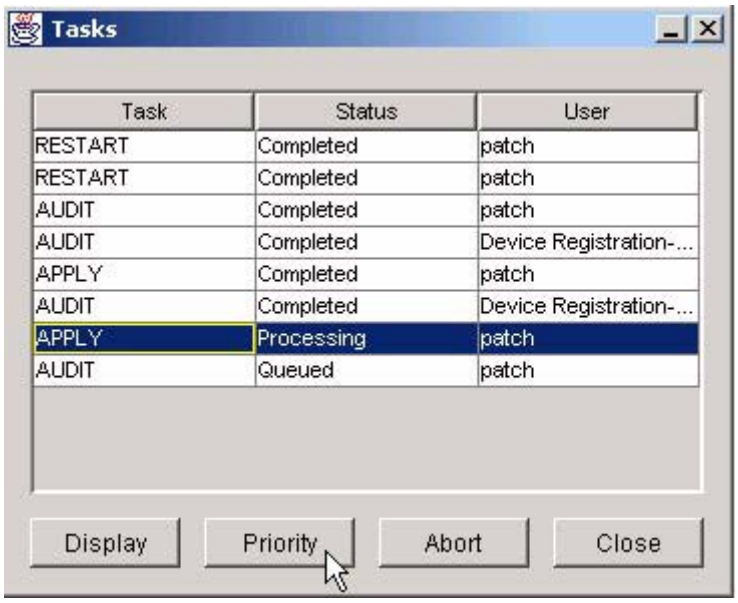
1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

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.

You have completed this procedure.

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

The web path to download Linux warranty patching has changed. Visit Nortel.com to retrieve the patches.

At the Nortel.com web site...
Select: Products *(top left under Products & Services pull-down menu)*
Select: Software *(under Popular Links*)
Select: Families *(top right under Find Products)*
Select: Succession
Select: Succession Communication Server 2000-Compact *(under Succession: General Availability)*
Select: Software

Platform patching

Patch files have the following identification scheme:

ncgl_cc_patch_r.w.c.v

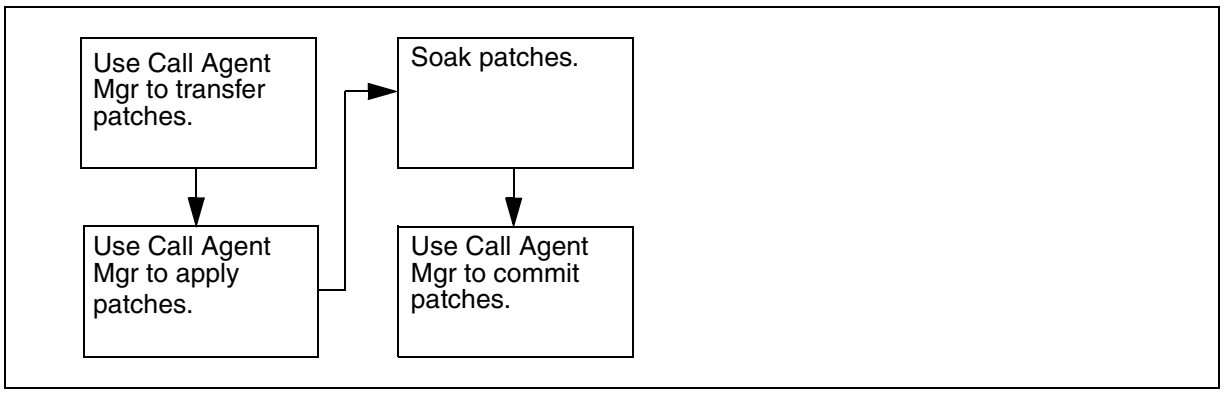
- **r** indicates the release. For example, 8.
- **w** indicates the week number of the load build. For example, 15.
- **c** indicates the compile. This value is equal to the fc value for an NCL or equal to (fc+i) for an MNCL. The patch is only applicable to a load that matches this number.
- **v** indicates 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 Nortel.com to retrieve the patches.
At the Nortel.com web site...
Select Products *(top left under Products & Services pull-down menu)*
Select: Software *(under Popular LInks)*
Select: Families *(top right under Find Products)*
Select: Succession
Select: Succession Communication Server 2000-Compact *(under Succession: General Availability)*
Select: Software

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 : 7.15.1.0
 0 Quit       Source       : /3pc/patch
 2 Select
 3 Fetch       # Patch Description                    Version
 4 Source      1 ncgl_cca_patch                       7.15.1.9
 5             2 ncgl_cca_patch                       7.15.1.8
 6             3 ncgl_cca_patch                       7.15.1.7
 7             4 ncgl_cca_patch                       7.15.1.6
 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 : 7.15.1.0
 0 Quit       Filter       : ALL
 2 Select
 3 Apply       # Patch Description              Version         Status
 4 Delete      1 ncgl_cca_patch                 7.15.1.9        NEW
 5 Commit      2 ncgl_cca_patch                 7.15.1.8        VALIDATED
 6             3 ncgl_cca_patch                 7.15.1.7        VALIDATED
 7             4 ncgl_cca_patch                 7.15.1.6        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 support personnel.
loss of mate communication while running patch commands	• link failures at router • link pulls • 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. 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 • 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 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 Call Agent*, NN10065-461.

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 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.

Cleaning up old data in the NPM database

Application

Use this procedure to clean up the old data in the Network Patch Manager (NPM) database following an upgrade.

ATTENTION

This procedure includes stopping and starting the NPM, which has the NPM re-discover the patches on the system when the NPM is brought back into service. This can take several hours depending on office configuration. Therefore, ensure patching tasks are not planned or scheduled in the timeframe you want to perform this procedure.

ATTENTION

This procedure purges any user-defined reports, tasks, sets, plans and alarms, disables any enabled plans such as AUTOAPPLY and AUTORESTART, releases any patches or devices on hold, and unconfigures the Patch File Receipt System (PFRS). Therefore, you will need to re-define any user-defined reports, tasks, sets, plans, and alarms, re-enable any plans such as AUTOAPPLY and AUTORESTART, place any desired patches or devices on hold, and re-configure PFRS following this procedure.

Prerequisites

You must have root user privileges to perform this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Generate and save a patchlist report using the NPM CLUI or GUI.

Note: The patchlist report may be useful in the event the apply time information is required at a later time.

If using the	Do
CLUI	step 2
GUI	step 3

2 Using the NPM CLUI, generate and save a patchlist as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server on which you want to generate the report

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the password for the root user.

e Change directory to /data/npm by typing

```
# cd /data/npm
```

and pressing the Enter key.

f Determine if a tmp directory exists in the npm directory by typing

```
# ls -l
```

and pressing the Enter key.

g Use the following table to determine your next step.

If	Do
a tmp directory exists	substep i
otherwise	substep h

h Create a tmp directory by typing

```
# mkdir tmp
```

and pressing the Enter key.

i Change directory to the tmp directory by typing

```
# cd tmp
```

and pressing the Enter key.

j Generate the patchlist report by typing

```
$ npm q patchlist output <filename>.list
```

and pressing the Enter key.

where

filename
is the name you want to give to the patchlist report

Example
npm q patchlist output aug032004.list

Example response

```
Enter the NPM Succession user id and
password.
Login
```

k When prompted, enter the NPM user ID.

Example response

```
password
```

l When prompted, enter the NPM user password.

Example response

```
Redirecting output to: aug032004.list
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
Redirecting output to standard I/O
```

m Display the file by typing

```
$ ls
```

and pressing the Enter key.

Example response

```
aug032004.list
local.login
local.cshrc
local.profile
```

n If required, display the contents of the file by typing

```
$ cat <filename> |more
```

and pressing the Enter key.

where

filename
is the name you gave to the patchlist report file

Example
cat aug032004.list

Example response

```
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
```

3 Using the NPM GUI, generate and save a patchlist as follows:

a Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 1866.

b On the **Tasks** menu, click **Reports....**

c Click the **Report List** tab to display the list of defined reports.

d Click on **PATCHLIST**, and then click **Execute** to generate the PATCHLIST report.

The **Reports Results** window is displayed.

e Click **Save** to save the results of the PATCHLIST report and specify the filename and location to save the report.

The **Save** window is displayed.

f Enter a name for the saved report in the **File name** field and then click **Save**.

g Click **Close** to close the Reports Results window.

h Click **Close** to close the Reports window.

i On the Edit menu, Click **Preferences**.

j Click on the **System Preferences** tab.

Copy and paste the data on display including that in the Delete Patches from the Drop Box after Retrieval checkbox.

4 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server where the NPM resides

5 When prompted, enter your user ID and password.

6 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

7 When prompted, enter the root password.

8 Stop the NPM server application by typing

```
# servstop NPM
```

and pressing the Enter key.

9 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

 X - exit

select -
```

10 Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit

Select -
```

11 Enter the number next to the “Succession Element Configuration” option in the menu.

Example response

```
Succession Element Configuration
 1 - NPM Application Configuration
 2 - SAM21EM Application Configuration
 3 - PSE Application Configuration
 4 - OMPUSH Application Configuration


 X - exit

select -
```

12 Enter the number next to the “NPM Application Configuration” option in the menu.

Example response

```
NPM Application Configuration
 1 - CreateDB (Initialize or re-initialize the
     NPM database)
 2 - ConfigureNpm (Configure the Network Patch
     Manager)


 X - exit

select -
```

13 Enter the number next to the “CreateDB” option in the menu.

Allow to complete.

14 Exit each menu level of the command line interface to eventually return to the root level, by typing

`select - x`

and pressing the Enter key.

15 Start the NPM server application by typing

`# servstart NPM`

and pressing the Enter key.

16 If any user-defined reports, tasks, sets, plans, or alarms existed prior to this procedure, re-define them using the corresponding procedure:

- for reports, use procedure Defining reports using the NPM on page 1968
- for tasks, use procedure Defining a task using the NPM on page 1957
- for sets, use procedure Defining sets using the NPM on page 1951
- for plans, use procedure Defining a plan using the NPM on page 1977
- 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 1962.

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 1985.

19 If PFRS was configured prior to this procedure, re-configure it using procedure Configuring NPM for automatic patch file delivery on page 790.

Note: If any users were logged in to the NPM GUI prior to this procedure, they must exit and re-launch the GUI. A re-connect to the NPM server from the GUI is not sufficient to clean up old data showing up in the GUI.

You have completed this procedure.