# Upgrading the Call Agent

## What's new in Call Agent upgrades for SN07

### December 2004, Standard 04.02

All SN06 sites except UA-IP sites must upgrade to SN06.2 prior to upgrading to SN07.

***Note:*** UA-IP was supported for trials only in SN06.2. However, all SN06 UA-IP sites are being upgraded to SN07.

Procedure Electronic Software Delivery (ESD) for Call Agent is added. Both the PCL and NCL software loads for the Call Agent are available for electronic transfer from Nortel Networks to a customer dropbox via ESD. ESD applies only to the following loads: CM Core, CCA LINUX, and MC.

Procedure Dump call processing application image has been modified.

The following procedures were removed from procedure LOAD_OLD_SIDE_BLADE and are now separate procedures:

- FINISH_POSTSWACT
- DUMP_OFFICE_IMAGE

### September 2004, Preliminary 04.01

SWUPGRADE is the Nortel Networks supported procedure for completing a Call Agent upgrade, also known as a One Night Process (ONP). The manual upgrade procedures such as TABXFER have been removed from this document, but the steps required to perform a platform only maintenance release (MR) upgrade remain.

Software delivery for the platform software (NCLs and MNCLs) and the call processing application (PCL) has changed to CDROM and DVD-ROM media. Software installation is performed at the host that provides the CS 2000 Management Tools with the **platform_load_install.sh** tool.

The software load name for the platform software (NCL and MNCL) changed from `3pclinuximage_6.20.1.2` for the SN06 release to `ncgl_cca_image_5.15.1.0` for the SN07 release. The software loadname for the Message Controller changed similarly, as well as the names of the patches for the Call Agent. The changes are described in Software version on page 12.

The structure of this document has changed to move the table of contents after this "What's new" section.

## What's new in Call Agent upgrades for SN06

### May 2004, Standard 03.04

The procedure for getting the call processing application software off tape has been changed. Most sites will use the GETLOAD procedure described in Restore call processing application files on page 55. Only sites with a Message Switch will use the procedure described in Upgrade Peripheral Modules and Message Switch on page 33.

### March 2004, Preliminary 03.03

The high level flowcharts that show SN04 to SN06 manual upgrade, SWUPGRADE, and platform only MR upgrade are revised to be hyperlinks.

A procedure to upgrade the Call Agent firmware manually is available in procedure Upgrading firmware on the occasion of a software upgrade on page 237.

A session trace for aborting a SWUPGRADE with the CANCEL command is added in Revert and Abort on page 155.

The procedure for performing a platform only MR has been updated to avoid a SYNC and DPSYNC, as indicated in the 3PC0M005 MR release notes, version 5.34.2.1. The new procedure replaces the SYNC and DPSYNC commands with a LDMATE command at the MAP. After the LDMATE, the procedure remains the same as in previous releases. Flowchart Platform only upgrade on page 17 shows the procedure.

### September 2003, Standard 03.02

Automatic upgrades with the SWUPGRADE tool now apply to CS 2000 - Compacts configured with Message Controller cards. All the steps in the SWUPGRADE section and the manual upgrade path now include information about the Message Controller cards.

This document is revised to include document history.

Section “Prepare for upgrade” is renamed to “Site preparation overview” to better align with the *One Night Process Procedures Guide*, 297-8991-303. The variables for step SWUPGRADE READY are listed and defined.

Section “Site responsibilites the day of the software delivery” is new.

The call processing application software can now be taken from tape on the CS 2000 Management Tools server with the SOSRF tool when upgrading from an SN06 load to an SN06 MR load. The software is then pulled to one of the Call Agent cards with the TRANSF tool. Once on the Call Agent, the IMPORT command is issued from within the call processing application to make the load available. For SN04 and SN05 upgrades to SN06, the GETLOAD command on the CS 2000 Core Manager retrieves the load from tape and then the load is FTP’d to the running call processing application image.

**June 2003, Preliminary 03.01**

SN06 and ISN06 allow upgrades from SN04 or SN05 to SN06. SN04 to SN06 upgrades require an upgrade of the Call Agent platform hardware to NTRX51FZ. No hardware change is required for SN05 to SN06 upgrades.

Software upgrade from SN04 to SN06 requires a manual upgrade. Both the automated and manual upgrade procedures are detailed in this document.

For SN04 to SN06 upgrades, a change in the messaging strategy eliminates the need for the serial link connection between the COM1 ports of the rear transition modules. After successful software upgrade of the platform and call processing application, this link can be removed. SN05 offices already have this link removed.

The Call Agent Manager application has two changes for the SN06 release. The command to start the application has changed from **tpcmtc** to **ccamtc**. The maintenance level from the application has changed name from Mtc to CoreMtc.

In some markets, the CS 2000 - Compact is deployed with Message Controller cards. Software upgrade for these cards is described in this document. Software upgrades for offices with Message Controllers are only supported with SN06 to SN06 or newer upgrades. If an upgrade of the Message Controllers only is needed, the upgrade is accomplished with the procedures in section Upgrade Message Controller software.

When the SN06 Call Agent fileset is applied or upgraded from the SWIM level on the CS 2000 Core Manager, the fileset installation checks the configuration of the PassThru users. More information is provided in procedure Apply platform software for Call Agent and Message Controller.

## What's new in Call Agent upgrades for SN05

### October 2002, Preliminary 02.01

SN05 and ISN05 require an upgrade of the Call Agent platform software and the call processing application software.

Automatic One Night Process (AutoONP) is available for SN05 to SN05 and SN05 to newer releases. AutoONP is also available for the International market. The Software Upgrade tool (SWUPGRADE) is used during the upgrade to automate many of the steps required to upgrade the call processing application software.

Software upgrade from SN04 to SN05 or from ISN04 to ISN05 requires a manual upgrade. The automated and manual upgrade procedures are detailed in this document.

A change in the messaging strategy eliminates the need for the serial link connection between the COM1 ports of the rear transition modules. After successful software upgrade of the platform and call processing application, this link can be removed.

An upgrade of the Call Agent cards from NTRX51FQ to NTRX51FZ enables increased call processing capacity. The platform and call processing application software upgrade to SN05 or ISN05 is required before this hardware upgrade. Contact your account manager for assistance with upgrading the Call Agent cards.

# Contents

# Upgrade strategy

Upgrade of the Call Agent is available as an upgrade of platform software, or platform and application software. Patches are available for both software packages. If the CS 2000 - Compact is configured with Message Controller (MC) cards, the software on these cards is upgraded during this procedure.

If a new firmware release is available for the Call Agent or Message Controller cards, the firmware is upgraded during the locking and unlocking of those cards at the CS 2000 SAM21 Manager client. Refer to the *SAM21 Platform Base Release Notes* to determine if firmware software is delivered with the release. To enable the firmware upgrade, the FW Flash Enable checkbox must be checked at provisioning tab of the CS 2000 SAM21 Manager client. For the automatic software upgrade (SWUPGRADE), this is during steps LOAD_NEW_SIDE_BLADE and LOAD_MATE, LOAD_MC0_BLADE, LOAD_MC1_BLADE, and LOAD_OLD_SIDE_BLADE. For the manual upgrade procedure, the steps are Load Message Controller 0, Load Message Controller 1, Reprovision Call Agent platform load, and Provision new software load.

Contact Nortel Networks Global Software Services or your account manager for assistance with a Call Agent upgrade and preparation for the upgrade.

## Software upgrade

Several upgrade scenarios are possible:

- upgrade Message Controller software only, Call Agent platform and call processing software remain the same
- upgrade Call Agent platform software, Message Controller and call processing software remains the same. This is the Call Agent Maintenance Release upgrade process that requires use of the Platform only software upgrade procedure.
- upgrade Message Controller, Call Agent platform, and call processing application software. This is the complete upgrade (ONP) from release to release.

## Component software upgrade order

The component upgrade order is listed in *Succession Upgrades*, NN10261-450 or NN10344-450.

## Patching software

Patching is available during software upgrade and as a maintenance activity for the Call Agent platform and call processing application software. Message Controller software is not patchable. Maintenance releases for the Message Controller are applied by following the Message Controller upgrade procedure in this document.

## Tools and utilities

Preparation activities are performed by telephone operating company personnel. The SWUPGRADE process is typically performed by a Nortel Networks Software Delivery Engineer (SDE). The SDE requires remote connectivity access to the office to perform the SWUPGRADE process and an instance of the CS 2000 SAM21 Manager client. If remote access for the display of the CS 2000 SAM21 Manager client is unavailable, telephone operating company personnel must contact and negotiate an alternative method.

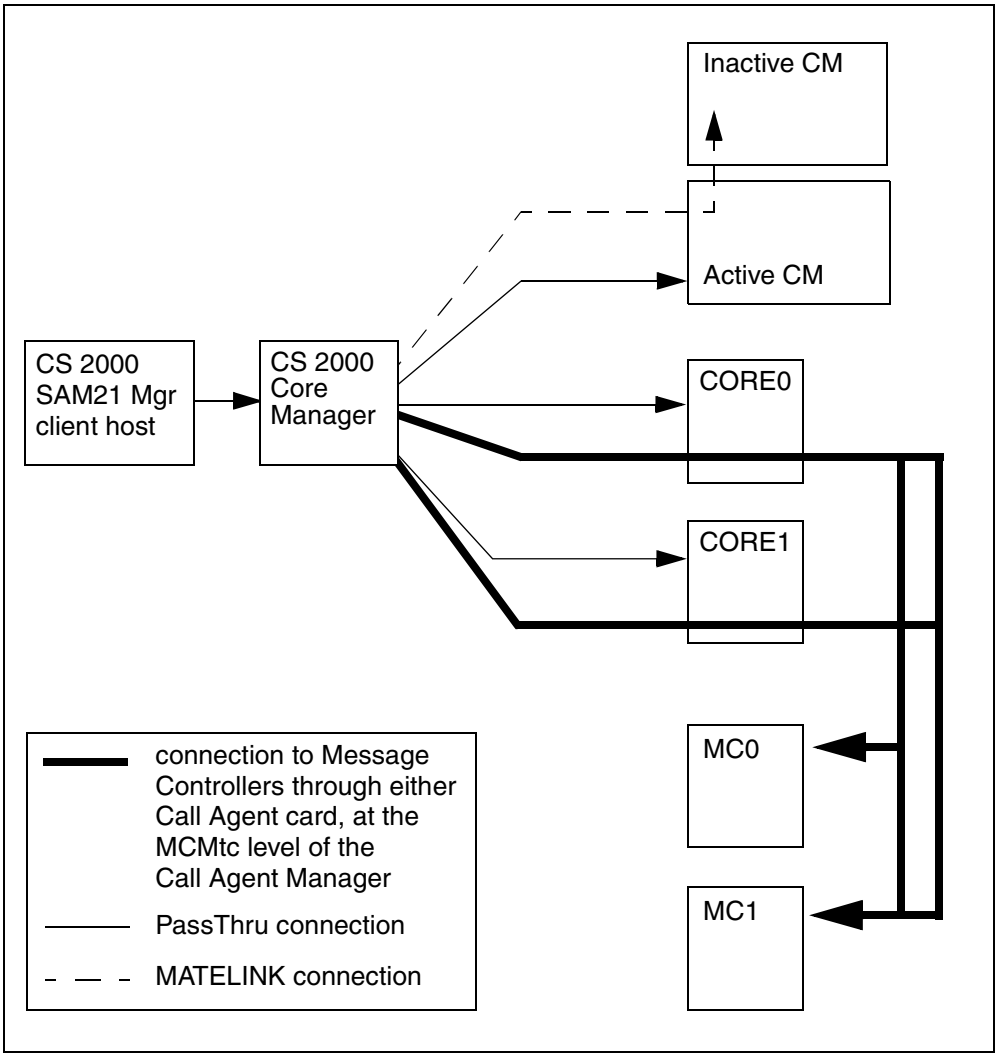
The workstation used for the CS 2000 SAM21 Manager client is the recommended platform from which to perform the software upgrade preparation procedures.

Upgrades require the CS 2000 SAM21 Manager client, the Call Agent Manager, and the MAP. The Call Agent Manager interface is used to maintain the Call Agent cards and the Message Controllers. The MAP is used to control and monitor the SWUPGRADE process and the Switch of Activity (SWACT) for the Call Agent cards.

Patching the application software requires the MAP interface. The Post-Release Software Manager (PRSM) tool is used for patching the call processing application.

For the call processing application upgrade, two MAP connections are required. One connection is to the active call processing application and the other connection is to the inactive call processing application. The connection to the inactive call processing application is made through the active call processing application by using the **MATELINK** command.

The dashed line in the following figure indicates the relationship between the connections to the active and inactive applications.




***Note:*** If the CS 2000 - Compact is equipped with Message Controllers and legacy connectivity equipment exists on the Time Division Multiplex (TDM) network, connectivity may be available from those devices to ACTIVECM. Contact your Nortel Networks account representative for assistance with determining connectivity needs.

## Software

Different software products are delivered according to the following table.

**Software product and delivery**

| Software product | Delivery method |
|---|---|
| Call processing application | This software is delivered on CDROM or DVDROM.<br><br>The CDROM or DVDROM is placed in the CDROM tray on the server that provides the CS 2000 Management Tools. Volume management software on that machine mounts the CDROM as `/cdrom/cdrom0`.<br><br>From the Call Agent, an FTP session is opened to the CS 2000 Management Tools machine, and the software is pulled from the `/cdrom/cdrom0` directory with the GET command.<br><br>The **IMPORT** command from the DISKUT level of the MAP makes the loads available to the call processing application for booting. |
| Call processing application patches | These patches are delivered through Regional Patch Selector (RPS). |
| Call Agent platform software and Message Controller software | This software is also delivered on CDROM. Use the **platform_load_install.sh** tool on the CS 2000 Management Tools machine to extract the `ncgl_cca_image.x.y.z.zz` and `ncgl_mc_image_x.y.z.zz` files from CDROM and transfers them to the CS 2000 Core Manager. If the office has a Core and Billing Manager (CBM) instead of a CS 2000 Core Manager, the files are transferred to the CBM instead. For offices without a CS 2000 Core Manager or a CBM, the loads are installed on the CS 2000 Management Tools server. |
| Call Agent platform patches | These patches are delivered through RPS. These files are placed in `/swd/3pc/patch` on the CS 2000 Core Manager or the CBM. |

### Software version

Software version information for Call Agent and Message Controller software is similar. The largest difference is that Message Controller software is not patchable.

The software loadnames changed for the SN07 and newer releases. The changes are shown in the table below.

**Software loadname changes for SN07**

| | previous to SN07 | SN07 |
|---|---|---|
| Call Agent platform | 3pclinuximage_6.20.3.1 | ncgl_cca_image_5.15.1.0 |
| Message Controller platform | mclinuximage_6.20.3.1 | ncgl_mc_image_5.15.1.0 |
| Call Agent patches | 3pclinuxpatch_6.20.3.2 | ncgl_cca_patch_5.15.1.2 |

### Call Agent

Call processing software and patch versions are described in the *Post-Release Software Manager Reference Manual*, 297-8991-540.

Call Agent platform software is managed through **platform_load_install.sh** tool available on the host that provides the CS 2000 Management Tools.

Call Agent platform software uses the following identification scheme:

- Non-Computing Load (NCL) — ncgl_cca_image_r.w.fc.0
  - — **r** indicates the release. For example, 5 for the SN07 release.
  - — **w** indicates the calendar week number of the load build. For example, 15.
  - — **fc** indicates the final compile version. For example, 1 indicates the first compile of week “w”.

    **Example**
    ncgl_cca_image_5.15.1.0
- Maintenance NCL (MNCL) — ncgl_cca_image_r.w.fc+i.1
  - — **fc+i** indicates that this is the i*th* MNCL for the NCL
  - — **r**, **w**, and **fc** values for an MNCL are the same values as for the NCL. This indicates that the MNCL applies to the NCL.

***Note:*** Only the latest version of the platform load is supported. If an MNCL exists, only the latest MNCL is supported and is

patched. Early MNCL versions and the NCL are not patched to the current release.

- Call Agent platform software patches — ncgl_cca_patch_r.w.c.v
  - — **r** indicates the release. For example, 5 for the SN07 release.
  - — **w** indicates the calendar 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. Patch versions begin at 2.

| NCL or MNCL | RPM filename on CDROM | Load to datafill at Provisioning panel of CS 2000 SAM21 Manager | Patch files for the load would be named as follows. Patch file names are applied from Call Agent Manager. |
|---|---|---|---|
| NCL | ncgl_cca_mc_image-5.32-1.0.noarch.rpm | ncgl_cca-image_5.32.1.0<br>ncgl_mc_image_5.32.1.0 | ncgl_cca_patch_5.32.1.1<br>ncgl_cca_patch_5.32.1.2 |
| MNCL MR1 | | | |
| MNCL MR2 | | | |

**Message Controller**
Message Controller software is managed through the SWIM tool available on the CS 2000 Core Manager.

Message Controller software uses the following identification scheme:

- Non-Computing Load (NCL) — ncgl_mc_image_r.w.fc.0
  - — **r** indicates the release. For example, 5.
  - — **w** indicates the calendar week number of the load build. For example, 32.
  - — **fc** indicates the final compile version. For example, 1 indicates the first compile of week “w.”

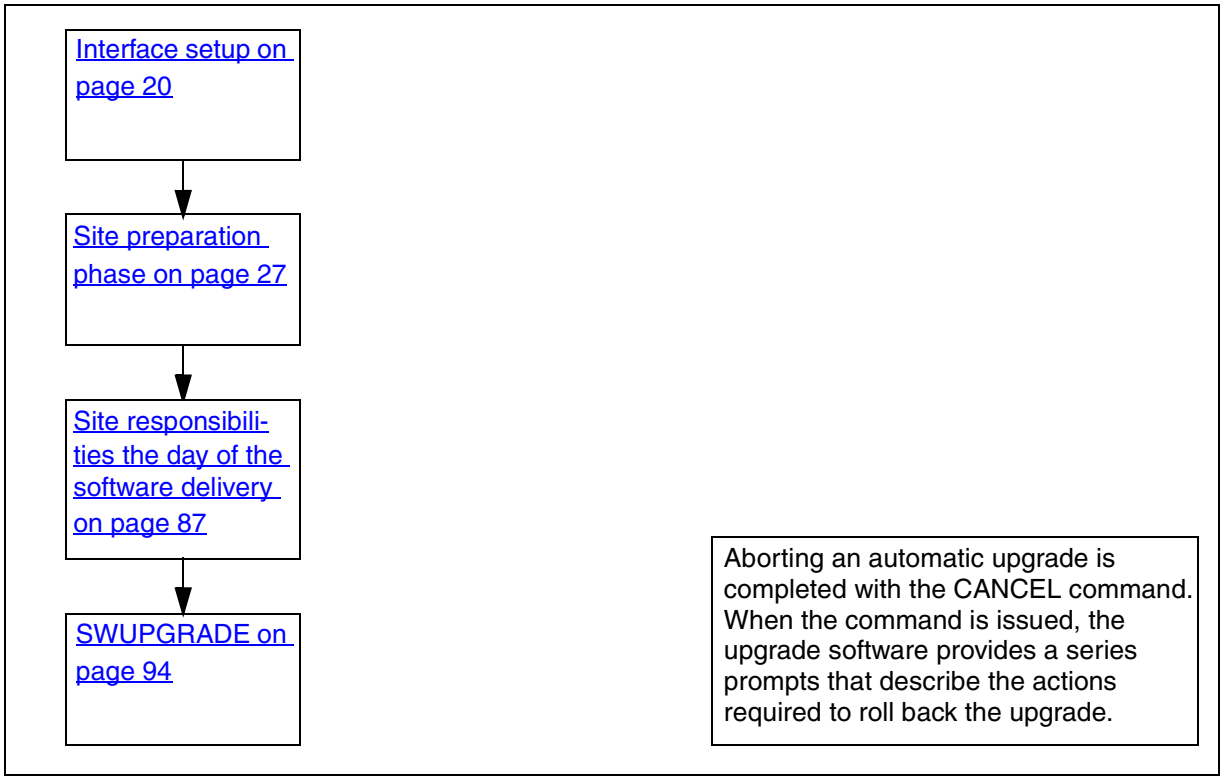
    **Example**
    ncgl_mc_image_5.32.1.0
- Maintenance NCL (MNCL) - ncgl_mc_image_r.w.fc+i.1
  - — **fc+i** indicates that this is the i*th* MNCL for the NCL
  - — **r**, **w**, and **fc** values for an MNCL are the same values as for the NCL. This indicates that the MNCL applies to the NCL.

***Note:*** Message Controller software is not patchable.

## Upgrade overview

The following flowcharts provide an overview of upgrading platform and application software.

### SN06 to SN07 or newer upgrade overview (SWUPGRADE)




## Aborting a SWUPGRADE

Aborting an automated upgrade is completed with the **CANCEL** command. The SWUPGRADE process recognizes the command and provides instruction in the form of prompts to roll back the upgrade procedures that were completed. Refer to Appendix A, Revert and Abort, on page 155.

## Platform only upgrade procedure

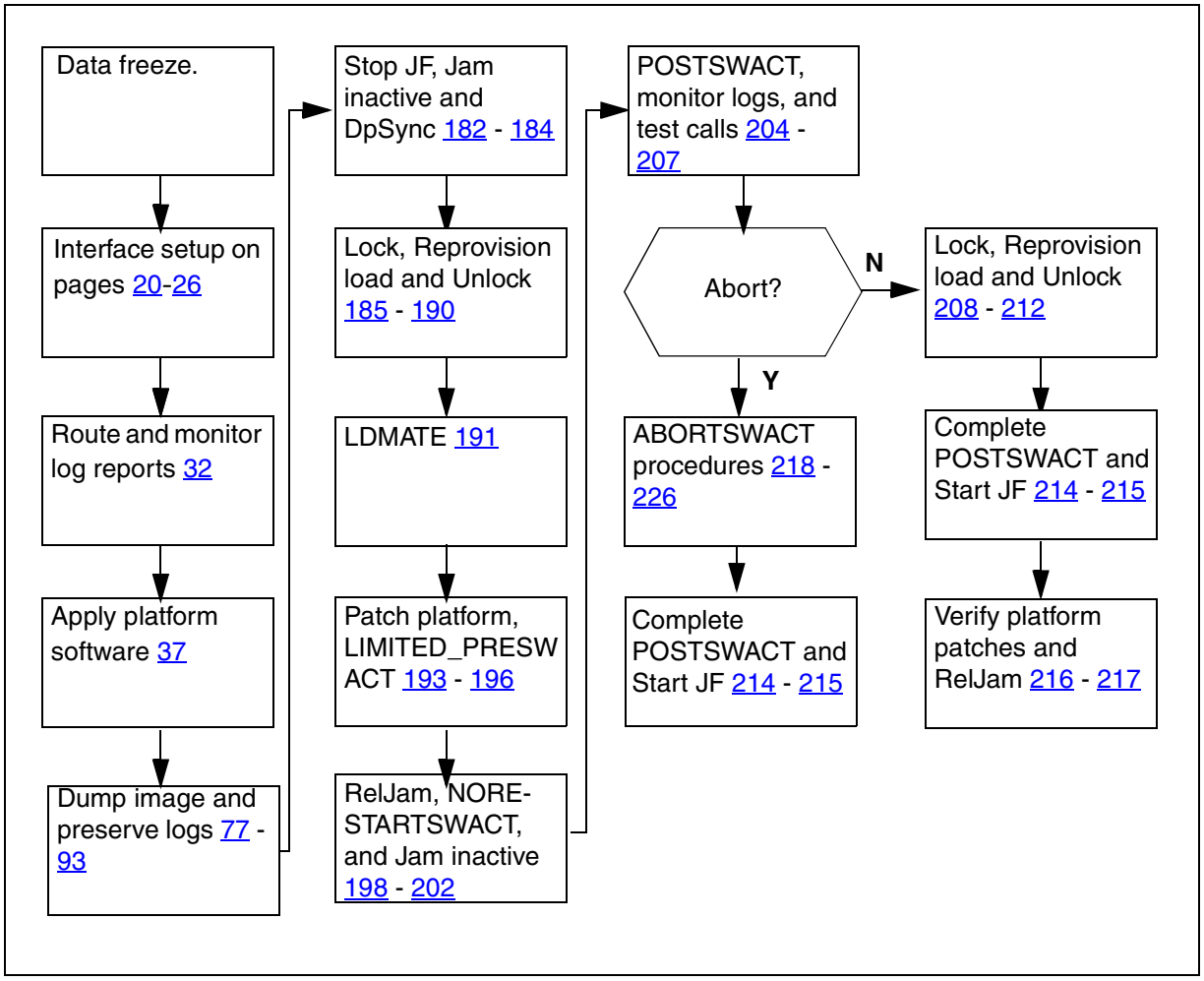
The platform only upgrade procedure is described in this document. Since many of the steps for a platform only upgrade and an ONP are the same, the platform only upgrade is provided as a path through the ONP procedure. Flowcharts and procedures indicate when a procedure applies to the platform upgrade only. The following figure shows an overview of the platform only upgrade. When performing the platform only upgrade, step Boot new platform software and all following procedures are located in Appendix B, Manual procedures, on page 164.

### Requirements

A successful platform only software upgrade requires the following:

- the telephone operating company must set aside a maintenance window during low traffic to perform the platform only upgrade
- an image is taken at the beginning of the maintenance window
- no provisioning is allowed during the maintenance window

### Platform only upgrade



## Terminology

The following information indicates personnel and interfaces.

### Personnel

Each procedure identifies which personnel perform the procedure or step.

**SITE** is the service provider personnel responsible for CS 2000 - Compact maintenance.

**SDE** is the Nortel Networks Software Delivery Engineer responsible to perform CS 2000 - Compact software upgrades.

### Interfaces

Refer to table Interfaces used to perform procedures and steps in the section Interface setup.

### Usernames and passwords

Usernames and passwords are required for the following element management interfaces:

- CS 2000 SAM21 Manager client

  A valid username and password are required to log into the client workstation. Contact your local administrator.

  A valid username and password are required to run the CS 2000 SAM21 Manager client application. Refer to *ATM and IP Administration and Security*, NN10261-600 for information about creating users and changing passwords. A user with mgcrw or mgcadm privilege is required.

- Call Agent Manager

  Configure the PassThru feature on the CS 2000 Core Manager or CBM to enable console access from a client machine to a Call Agent unit. Refer to *CS 2000 Core Manager Administration and Security*, NN10170-611or *Core and Billing Manager 850 Administration and Security*, NN10358-611for more information about enabling the PassThru feature.

  After PassThru is enabled, the maintenance username and password for the Call Agent platform are required. Contact your Nortel Networks account representative for this information.

- call processing application (MAP)

  A username and password with maintenance and administrative privilege are required to complete the upgrade. Refer to telephone operating company records for valid usernames and passwords.

**Hostnames and IP addresses**

The hostname of the CS 2000 Core Manager or CBM is required to perform this upgrade. This hostname is used to provide PassThru access to the Call Agent Manager and the call processing application.

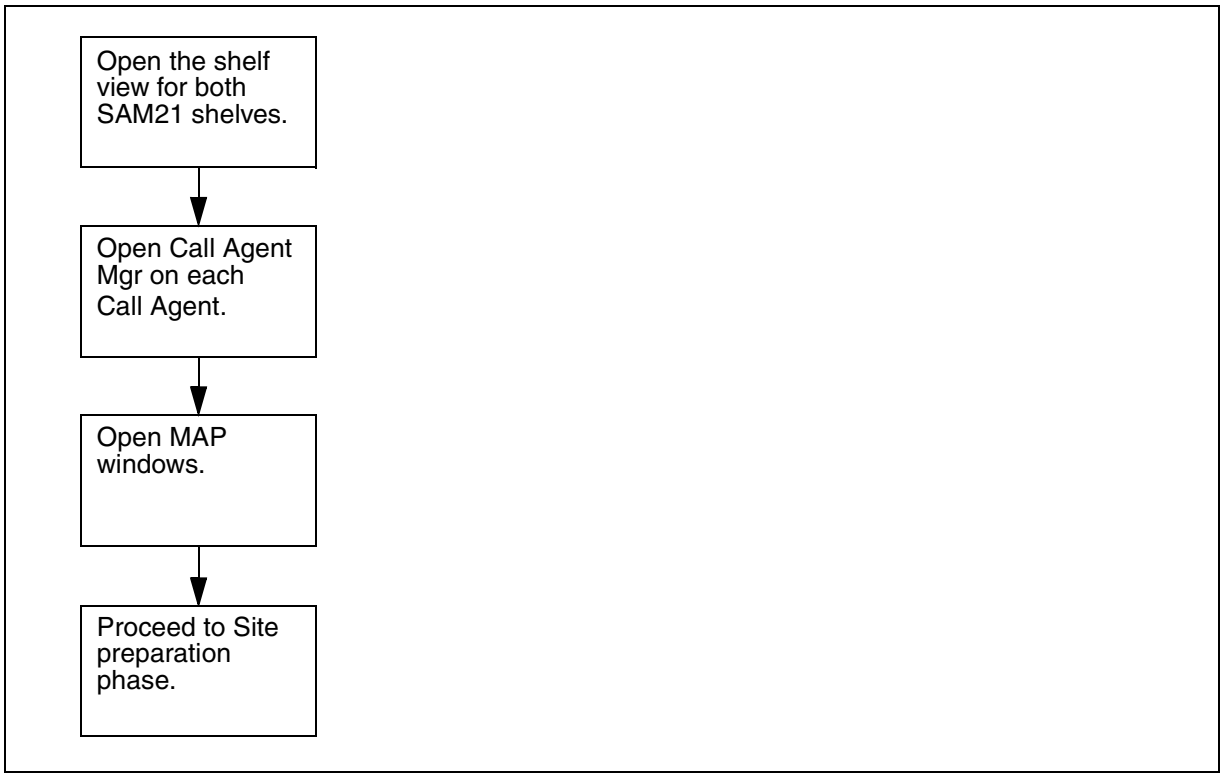
# Interface setup

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**

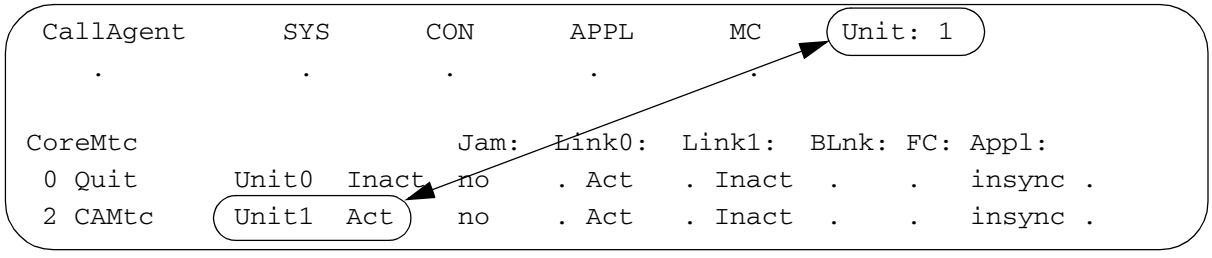


Each procedure indicates the interface used to perform the procedure or step. The following table describes the interfaces.

**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. In SN05, the command was tpcmtc |
| **CORE1** | a Call Agent Manager window connected to the Call Agent card identified as core1 and provides a maintenance interface. The maintenance interface is started from the **ccamtc** command. In SN05, the command was tpcmt |
| **Active maintenance window (CORE0 or CORE1)** | the CORE0 or CORE1 window that is connected to the active Call Agent. CORE1 is the active maintenance window for figure SN06 and newer Call Agent Manager with Message Controllers in the office on page 21. |
| **SDM** | a window connected to the CS 2000 Core Manager. The **sdmmtc** program and UNIX system activities are completed from this window |

### SN06 and newer Call Agent Manager with Message Controllers in the office



The following procedure indicates how to create a shell script that changes the title of an xterm window. This procedure only works on UNIX workstations.

***At an xterm window on the CS 2000 SAM21 Mgr client workstation***

1 Use an editor to create the following file. Available editors are vi and dtpad. Save the file with a name of “xtermtitle”.

```
#!/bin/sh
# this script changes the title of an xterm
echo "\033]2;$1\007"
echo "\033]1;$1\007"
```

2 Make the file executable.

```
UNIX> chmod +x xtermtitle
```

3 To use the script, enter the command and the new name for the window.

```
UNIX> ./xtermtitle <window_title>
```

**window_title**
is a string like core0, core1, sam21gui, activecm, or inactivecm

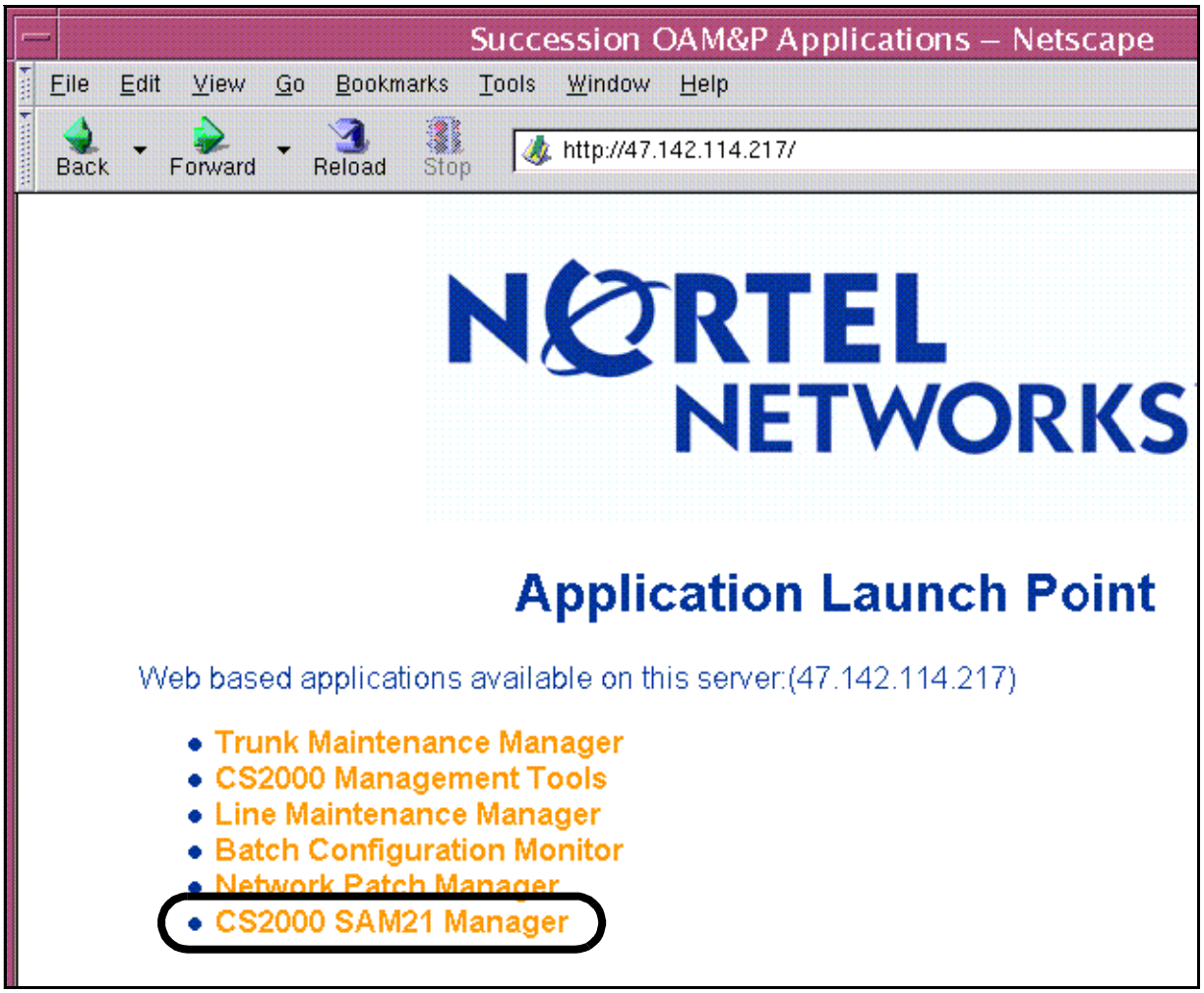
4 This procedure is complete.

For Microsoft Windows 2000 based workstations, change the title of a command prompt window with the **title <window_name>** command.

## Open SAM21 shelf views

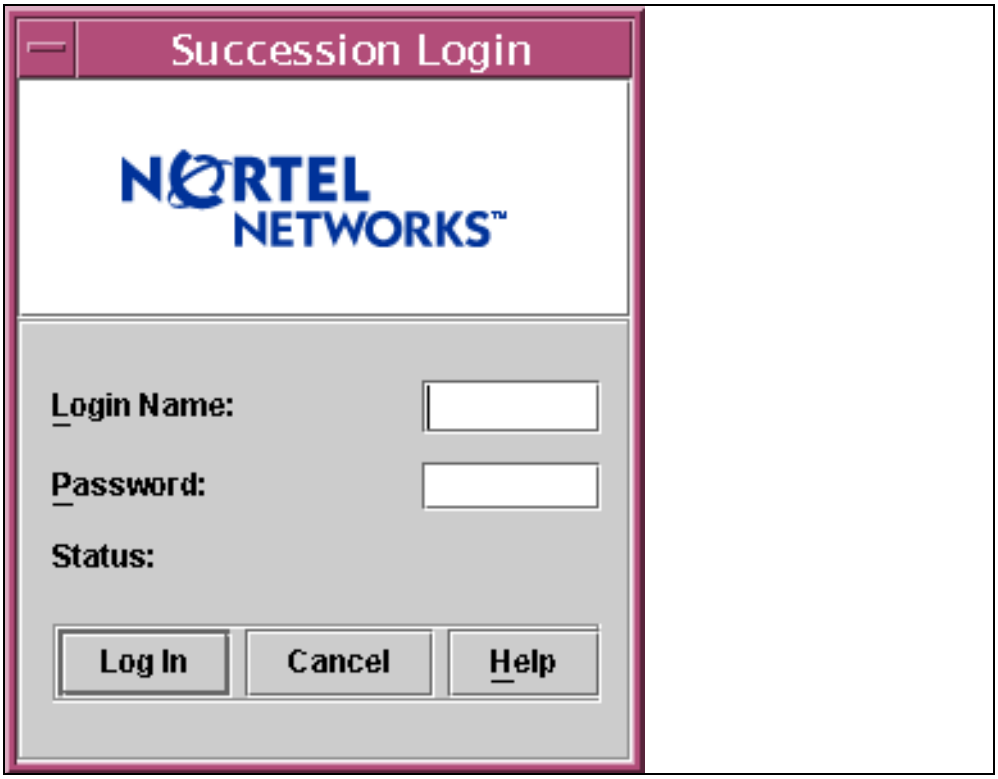
***At your workstation***

1 Open a web browser and enter the IP address or hostname of the host that provides the CS 2000 Management Tools. Click on the link for the CS 2000 SAM21 Manager.




*A login window appears.*

2 Provide the login name and password and then click Log In.




***Note:*** The login account must have mgcrw or mgcadm level permissions.

*The application starts and the Subnet View window opens.*

3 Open both Shelf View windows by double-clicking on the shelf icons from the Subnet View window.

4 Position the screens so that alarms and access to locking and unlocking cards are available.

5 This procedure is complete.

## Open 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**

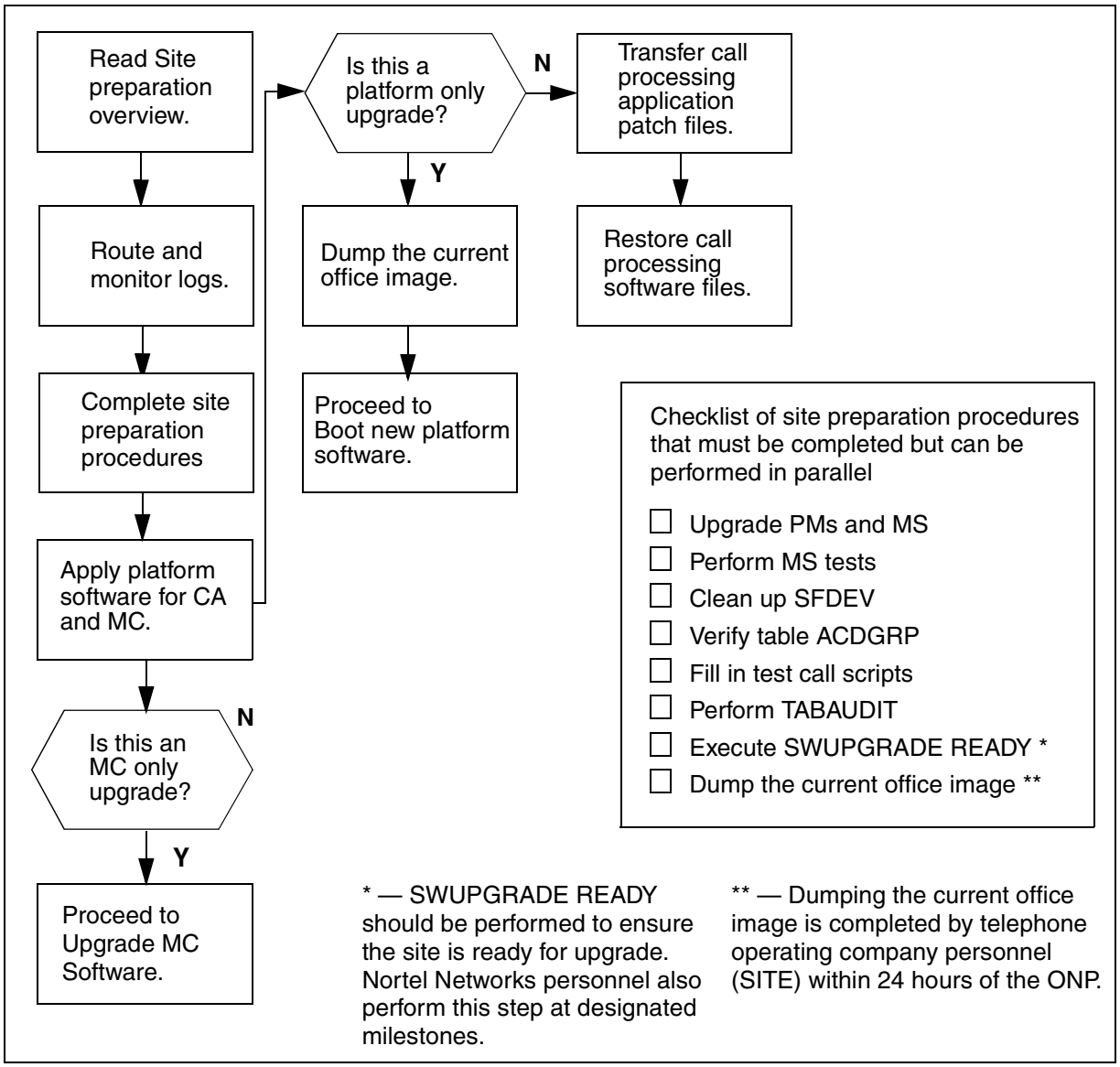


Table , Process timeline indicates the timing of events that need to be completed by telephone operating company personnel for an ONP. This timeline does not apply to platform only MR upgrades or Message Controller only upgrades.

**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<br>• site begins checking logs daily, refer to Route and monitor logs on page 32<br>• begin upgrading and verifying PMs and other network components with the latest software loads, refer to Upgrade Peripheral Modules and Message Switch on page 33 |
| 30 days | Begin data consistency checks, refer to Perform TABAUDIT on page 66 |
| 15 days | Ensure that scheduled RExTsts complete successfully |
| 7-4 days | • ensure SFDEV is clear, refer to Clean up SFDEV on page 60<br>• continue to monitor logs<br>• if office is equipped with PMs, ensure that the latest PM loads and XPM patch files are restored to the proper disk volumes<br>• site receives final shipment of software media and documentation |
| 6 days | • verify all network nodes are loaded, patched, and working<br>• verify dial in connectivity, refer to Remote site access on page 90<br>• ensure all software media are on site<br>• verify that site personnel are familiar with the upgrade process |

**Process timeline**

| Days before the upgrade | Site preparation activity |
|---|---|
| 5 days | The final site readiness check is performed by Nortel Networks personnel. Nortel Networks Software Delivery Engineer dials in an runs Execute SWUPGRADE READY on page 70. |
| 3-2 days | • verify site personnel has prepared test calls plan<br>• obtain name of site personnel representative with the authority to decide in case of an abort with the CANCEL command<br>• verify patches for the new software load are downloaded to the site<br>• ensure all site preparation checklist items are complete |
| Day of upgrade | Refer to Site responsibilities the day of the software delivery on page 87. |
| Night of upgrade | Refer to SWUPGRADE on page 94. |

# Site preparation overview

## Planning activities

**CAUTION**
**Possible service interruption**
Application of the following patch types within 30 days of the ONP must be considered a gating issue to the ONP:

Active (ACT) patch applied and activated

Limited (LTD) status patch

Verification (VO) status patch

If any of the above patches are applied to the office within 30 days of the ONP, immediately contact your Nortel Networks regional customer representative or call the Global Software Delivery Hotline for your market.

A successful software delivery application will require certain activities to be performed before the ONP. Some of these activities will depend on factors such as office type and the PCL software being delivered. This section provides a brief overview of the site preparation activities that must take place before the ONP. Other required activities not listed in this section must be approved by and coordinated through the appropriate Nortel Networks customer representatives. The following information: administrative, warnings, and software delivery data services should be reviewed by office personnel as soon as this document is received.

## Pre-application activities

Pre-application activities include upgrading all peripherals (including remotes) to PM loads compatible with the new PCL software load. In addition, Network (ENET) and Message Switch (MS) software upgrades must be completed before the ONP.

Pre-application activities can include (but are not restricted to) the following:

- First shipment of ONP CDROMs and documentation to the site
- Site polling by Nortel Networks to obtain specific switch information
- Site preparation procedures

- TABAUDIT procedure
- Final shipment of ONP CDROMs and documentation to site
- Pre-loading the message switch
- Site ready checks
- Site responsibilities the day of the software delivery application

Some of the above activities will be completed by Nortel Networks personnel and some will be completed by the operating company. Site personnel responsible for completing pre-application activities should become familiar with all sections of this document.

## Route and monitor logs

***SITE — At the ACTIVECM window***

**1** Determine if log reports are suppressed.

```
> LOGUTIL; LISTREPS SPECIAL
```

**2** If CA or MM log reports are suppressed, remove the suppression.

```
> RESUME log_type
```

**log_type**
is CA, MM, MS, SYSLOG, or ISYSLOG

**3** If CA or MM log reports have a threshold set, remove the threshold.

```
> THRESHOLD 0 log_type
```

**4** Route the logs to a printer device.

```
> LISTROUTE DEVICE printer
> ADDREP printer log_type
```

**printer**
is a terminal type device like TELNSVR00003

**5** Start the printer device.

```
> STOPDEV printer
> STARTDEV printer
> LEAVE
```

***SDE — At the ACTIVECM window***

**6** Enter the BCS update level.

```
> BCSUPDATE
```

**7** Check the logs.

```
> LOGCHECK
```

**8**

**ATTENTION**
Do not proceed until all log activity is explained.

This procedure is complete.

# Upgrade Peripheral Modules and Message Switch

**ATTENTION**
Only perform this procedure if the office is configured with an MS and legacy Peripheral Modules (PM).

**ATTENTION**
This is the first shipment of software and arrives approximately 35 days before the ONP.

Do not perform the following procedure if this is a platform only upgrade (MNCL).

The examples provided in this procedure show how to get the MS and the call processing application images, but this procedure also applies to PM loads and cutover tools necessary to upgrade a TDM to Hybrid solution.

If this procedure is not needed, go to Apply platform software for Call Agent and Message Controller on page 37.

Upgrade of the call processing application on the Call Agent requires an upgrade of all network elements in the Succession network and all element managers before an upgrade of the Call Agent. Refer to *Solutions Upgrades*, NN10261-450 or NN10344-450 for changes in this policy and the upgrade order.

Do not proceed with the Call Agent upgrade unless all other network elements and element managers have been upgraded or *Solutions Upgrades*, NN10261-450 or NN10344-450 indicates which network elements and element managers can be upgraded after the Call Agent.

If the CS 2000 - Compact is equipped with Message Controller cards, the Message Switch, Enhanced Network, and any Peripheral Modules must be upgraded before the Call Agent. Refer to the *Peripheral Module Release Document*, 297-9051-599 (EMEA) or 297-2663-599 (NA). Upgrade of the Message Controllers is completed during step SWUPGRADE in this document.

Because the CS 2000 - Compact does not have a tape drive, software loads delivered for TDM peripherals are shipped on CDROM.

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

**1** Insert the DVD or CDROM in the CDROM tray.

***SITE — At the CORE0 or CORE1 window***

**2** Exit the Call Agent Manager:

```
> 0 all
```

*The operating system prompt is returned.*

```
[mtc@hostname mtc]$
```

**3** Change directory to the destination directory for the peripheral module (PM) loads:

```
> cd /3PC/<sd0x>/<pm_loads_location>
```

**Example**
**> cd /3PC/sd00/pmloads**

**4** Open an FTP session to the CS 2000 Management Tools server and log in:

```
> ftp <cs_2000_mgmt_tools_ip>
```

***Note:*** Log in to the CS 2000 Management Tools server as a user with privilege to change directory and transfer files with FTP.

**Example**

```
[mtc@10.40.44.67 image0]$ ftp <cs_2000_mgmt_tools_ip>
Connected to <cs_2000_mgmt_tools_ip>.
220 ProFTPD 1.2.8 Server (Authorized Use Only) [hostname]
Name (hostname:mtc): maint
331 Password required for maint.
Password:
230 User maint logged in.
ftp>
```

**5** Change directory, list the file size, change the mode to binary, and get the file:

```
ftp> cd /cdrom/cdrom0
ftp> ls
ftp> bin
ftp> prompt
ftp> mget *
```

***Note:*** Do not transfer a file with a name longer than 32 characters.

**Example FTP session of getting PMLOADS**

```
ftp> cd /cdrom/cdrom0
250 CWD command successful.
ftp> ls
ERS20CE.img1020
ENX20CE.img1020
...
LRS20CE.img1020
MPF20CE.bin128
QLI20BT.img1020
ftp> bin
200 Type set to I.
ftp> prompt
Interactive mode off.
ftp> mget *
local:
200 PORT command successful.
150 Opening data connection for ERS20CE.img1020 (binary mode)(5107140 bytes)
226 Transfer complete.
150 Opening data connection for ENX20CE.img1020 (binary mode)(3913740 bytes)
226 Transfer complete.
...
```

6 End the FTP session by typing bye:

```
ftp> bye
```

***At the ACTIVECM window***

7 Enter the DISKUT level and import the upgrade PM loads:

```
> DISKUT
> IMPORT SD00PMLOADS
```

**Example IMPORT of PM loads**

```
DISKUT:
>IMPORT SD00PMLOADS

Attempting to import 24 files selected on SD00PMLOADS.

Imported ERS20CE.img1020 as ERS20CE  IMAGE 1020.
Imported ENX20CE.img1020 as ENX20CE  IMAGE 1020.
...
Imported MPF20CE.bin128 as MPF20CE  BIN 128.
Imported QLI20BT.img1020 as QLI20BT  IMAGE 1020.

Imported 24 files successfully of 24 attempts on SD00PMLOADS.
```

*The PM load files are imported from the native file system into the call processing application file system. If the disk does not have enough space, a prompt to increase the volume size is presented.*

**8** This procedure is complete.

***SITE — At a CS 2000 Management Tools terminal***

**9** Issue the eject command to open the CDROM tray:

```
# eject
```

*Software on the CS 2000 Management Tools server unmounts the DVD and opens the CDROM tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session is ended and no users have changed directory into /cdrom/... directory. Re-enter the eject command.*

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

**10** Remove the DVD from the CDROM tray.

**11** This procedure is complete.

## Apply platform software for Call Agent and Message Controller

Complete this procedure at least two days before the ONP.

This procedure installs the Call Agent platform software, `ncgl_cca_image_5.x.y.z`, and the Message Controller software, `ncgl_mc_image_5.x.y.z` onto the CS 2000 Core Manager or the Core and Billing Manager (CBM). The Message Controller software is installed even if the office is not configured with Message Controller cards. If the office is not configured with a CS 2000 Core Manager or a CBM, this procedure installs the software on `/data/swd/3pc` of the CS 2000 Management Tools server.

For offices without a CS 2000 Core Manager or a CBM, manual action is required. Refer to Offices without a CS 2000 Core Manager or CBM on page 46.

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

**1** Insert the CDROM in the CDROM tray.

***SITE — At a CS 2000 Management Tools terminal***

**2** Log in and then use the su command to gain root privilege.

```
Trying <hostname>...
Connected to <hostname>.
Escape character is '^]'.

Authorized use only, activities logged.
login: username
Password: <password>
Last login: Fri Jan 30 12:48:10 from <otherhost>
prompt:>
prompt:> su - root
Password: <root_password>
#
```

**3** Execute the platform_load_install.sh script.

```
# /opt/nortel/sspfs/Scripts/platform_load_install.sh
```

*The screen clears and a menu is displayed.*

```
      Welcome to the Platform Installation Tool Version 3.2
   ================================================================
      RPM INSTALLATION/REMOVAL
     ============================
     1) Install RPM from CDROM       2) Install RPM from Disk
     3) Uninstall RPM                4) Query all RPMs

      OTHER
     =========
    C) Change Rotation Parameters          P) View Rotation Parameters
     V) SAM21 Platform Version Installed     X) Exit

      Please choose one of the following: 1
```

**4** Enter **1** and press the Return key to install the software.

*The screen clears and the contents of the .rpm package are displayed.*

```
                Verifying CDROM is mounted
/cdrom/cdrom on /vol/dev/dsk/c0t0d0/cdrom read only/nosuid/mapl-
case/noglobal/rr/traildot/dev=16c0001 on Sat Mar 27 16:34:13 2004
                CDROM is mounted.
                Listing file names in the rpm on the cd.

/swd/3pc/ncgl_cca_5.32.1.0
/swd/3pc/ncgl_mc_5.32.1.0

                Do you want to continue (y/n)? Y
```

***Note:*** *If the message* `There is no cd in the CDROM drive, please check drive` *is displayed, ensure that the CDROM is inserted in the tray for this unit.*

**5** Enter **Y** to proceed with the software installation.

*The software is extracted from the .rpm package. The .rpm package is transferred to the CS 2000 Core Manager or CBM.*

```
              Extracting files from the rpm archive on the cd.

Installing RPM package ncgl_cca_mc_image-5.32-1.0.noarch.rpm
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
ncgl_cca_mc_image-5.32-1.0.noarch.rpm       100%   11MB 750.4KB/s   00:14
root@47.135.214.127's password: <enter root password>
```

**6** Enter the root password for the CS 2000 Core Manager or CBM.

*The software is installed on the CS 2000 Core Manager or CBM. If a CBM is used, the .rpm package is then copied to the inactive CBM unit and another prompt for the root password appears. If this happens, enter the root password and press Return. After the load file is installed on the CS 2000 Core Manager or CBM, the transferred .rpm package is deleted from the CS 2000 Core Manager or CBM.*

```
              Extracting files from the rpm archive on the cd.

Installing RPM package ncgl_cca_mc_image-5.32-1.0
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
ncgl_cca_mc_image-5.32-1.0.noarch.rpm      100%   11MB 750.4KB/s   00:14
root@47.135.214.127's password: <enter root password>
Mate IP is 47.135.214.129
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
root@47.135.214.129's password: <enter root password>

      ******* Please hit ENTER key to continue ***********
```

**7** A script is run to verify connectivity to the ACTIVEIRM IP address (the call processing application) and to verify hostname aliases. The output depends on whether the office is configured with a CS 2000 Core Manager or a CBM. Refer to Additional information on page 40 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 77 |
| otherwise | Transfer call processing application patch files on page 53 |

## Additional information

After applying the platform software, the installation process invokes the `/swd/3pc/bin/user_config.sh` script to verify or set:

- the configuration of the PassThru feature on the CS 2000 Core Manager or CBM
- hostname aliases core, core0, and core1
- NFS sharing of the Call Agent platform software load

The installation process asks if the ncgl_cca_image software is for CA (Call Agent) or HMEM (Home Location Registry Memory).

The CS 2000 Core Manager or CBM software provides a prompt to determine if the fileset is for a CA or HMEM application.

Enter **CA** and press the Enter key.

```
Is this a CA or HMEM application? [CA/HMEM] CA: CA
```

A check is made to determine if aliases core, core0, and core1, as well as PassThru accounts cmusr, core0usr, and core1usr exist. The response is determined by the current configuration.

## New installation on Core Business Manager

The software prompts for the ACTIVEIRM IP address, adds the host aliases to the `/etc/hosts` file, and creates the PassThru users on both CBM units.

### New installation on CBM

```
Is this a CA or HMEM application ? [CA/HMEM] CA : CA
Checking for existing core alias...
---------------------------------
hostmtc: Hostname or IP address is not in the hosts database: 'core'.


No existing alias from core found

Cleaning up any alias for core0 core1 and any related passthru accounts,
 if found.

Enter the ACTIVEIRM IP ADDRESS (e.g. 172.16.16.72 ) or q : 10.40.64.72

Adding aliases...
-----------------
10.40.64.72~core~~
10.40.64.67~core0~~
10.40.64.70~core1~~

Configuring Passthru Users ...
------------------------------

Creating Passthru accounts...
Creating passthru user cmusr
Creating passthru user core0usr
Creating passthru user core1usr


Sharing NFS mount For CCA Access of /swd/3pc ...
----------------------------------------
NFS mount /swd/3pc successfully shared.
```

### Upgrade on CBM

In an upgrade on the CBM, the software always prompts to confirm the ACTIVEIRM IP address, always removes the core, core0, and core1 aliases, and always adds them back to the `/etc/hosts` file.

**Upgrade on CBM**

```
Is this a CA or HMEM application ? [CA/HMEM] CA : CA
Checking for existing core alias...
-----------------------------------
10.40.64.72~core~~
Please confirm ACTIVE IRM IP address is [10.40.64.72] (yes/no):YES

Temporarily removing alias from /etc/hosts for core core0 core1
and related passthru accounts, while performing network engineering
validation.

Adding aliases...
-----------------
10.40.64.72~core~~
10.40.64.67~core0~~
10.40.64.70~core1~~

Configuring Passthru Users ...
------------------------------

Creating Passthru accounts...
Creating passthru user cmusr
Creating passthru user core0usr
Creating passthru user core1usr

Sharing NFS mount For CCA Access of /swd/3pc ...
-----------------------------------------
NFS mount /swd/3pc successfully shared.
```

### New installation on CS 2000 Core Manager

For a new installation, the software prompts for the ACTIVEIRM IP address. This information is available from the Nortel Networks

Installation Services engineer, or documentation provided by Nortel Networks Installation Services

### New installation on CS 2000 Core Manager

```
Checking for existing aliases...
--------------------------------
hostmtc:Hostname or IP address is not in the hosts database:‘core’.
hostmtc:Hostname or IP address is not in the hosts database:’core0’.
hostmtc:Hostname or IP address is not in the hosts database:’core1’.

Checking for existing passthru accounts...
------------------------------------------
passthru:Undefined passthru user cmuser.
passthru:Undefined passthru user core0usr.
passthru:Undefined passthru user core1usr.

Enter the ACTIVEIRM IP ADDRESS (e.g. 172.16.16.72) or q: 10.40.24.80
Do you wish to proceed? [y/n] y: Y

Checking for existing IP in hosts database.
-------------------------------------------
hostmtc:Hostname or IP address is not in the hosts database:’10.40.24.80’
hostmtc:Hostname or IP address is not in the hosts database:’10.40.24.75’
hostmtc:Hostname or IP address is not in the hosts database:’10.40.24.78’

Adding aliases...
-----------------
10.40.24.80:core::
10.40.24.75:core0::
10.40.24.78:core1::

Adding passthru accounts...
---------------------------
cmuser::221:202,passthru:CA SOS Image:/sdmtools/bin/cm_screener:
  /home/cmuser::telnet:core
core0usr::222:202,passthru:CA Unit 0:/sdmtools/bin/cm_screener:
  /home/core0usr::telnet:core0
core1usr::223:202,passthru:CA Unit 1:/sdmtools/bin/cm_screener:
  /home/core1usr::telnet:core1

exporting NFS mount /swd/3pc...
-------------------------------
Mount already exported to core*.
```

The aliases and PassThru accounts are created. The status information about installation in the figure above does not remain on the screen very long since the installation software clears the screen once the configuration is complete. Please read Important password information.

### Upgrade with correct configuration on CS 2000 Core Manager

In SN05, the cmusr, core0usr, and core1usr accounts were not true PassThru accounts on the CS 2000 Core Manager. These accounts were maint accounts with a profile that launched a telnet session to the destination host. If the configuration information (hostname aliases and user accounts) is available on the CS 2000 Core Manager, then that information is deleted from the CS 2000 Core Manager and reconfigured as true PassThru accounts. Please read Important password information.

**Upgrade with correct configuration on CS 2000 Core Manager**

```
Checking for existing aliases...
--------------------------------
10.40.24.80:core:cm CLLI:Core's IPNETWRK IP Address
10.40.24.75:core0::
10.40.24.78:core1::

Checking for existing passthru accounts...
------------------------------------------
passthru:Undefined passthru user cmuser.
passthru:Undefined passthru user core0usr.
passthru:Undefined passthru user core1usr.

Adding passthru accounts...
---------------------------
cmuser::221:202,passthru:CA SOS Image:/sdmtools/bin/cm_screener:
  /home/cmuser::telnet:core
core0usr::222:202,passthru:CA Unit 0:/sdmtools/bin/cm_screener:
  /home/core0usr::telnet:core0
core1usr::223:202,passthru:CA Unit 1:/sdmtools/bin/cm_screener:
  /home/core1usr::telnet:core1

exporting NFS mount /swd/3pc...
-------------------------------
Mount already exported to core*.
```

***Note:*** Long lines in the display were wrapped.

### Upgrade with incorrect configuration on CS 2000 Core Manager

The SN05 accounts were not true PassThru accounts. If all the necessary information (hostname aliases and user accounts) is not complete on the CS 2000 Core Manager, the fileset application software does not perform any configuration or deletion of data.

Instruction for deleting the existing configuration and reconfiguring the fileset is provided. Once the information is deleted and the reconfiguration is started, the display is similar to New installation on

CS 2000 Core Manager. Please also read Important password information.

**Upgrade when old configuration was incorrect on CS 2000 Core Manager**

```
Checking for existing aliases...
--------------------------------
10.40.24.80:core:cm CLLI:Core's IPNETWRK IP Address
10.40.24.75:core0::
hostmtc:Hostname or IP address is not in the hosts database:'core1'.

Checking for existing passthru accounts...
------------------------------------------
cmusr::221:202,passthru:CA SOS Image:/sdmtools/bin/cm_screener:
  /home/cmuser::telnet:core
core0usr::222:202,passthru:CA Unit 0:/sdmtools/bin/cm_screener:
  /home/core0usr::telnet:core0
core1usr::223:202,passthru:CA Unit 1:/sdmtools/bin/cm_screener:
  /home/core1usr::telnet:core1

There is a partial list of aliases and/or passthru accounts.
THE 3PC APPLICATION WILL NOT BE CONFIGURED.
To configure the 3PC application, please carry out the following steps.

1. From the sdmmtc;nodes level, delete the entries core, core0, core1.
2. Delete the entries cmusr, core0usr, core1usr from either the
   sdmmtc;passthru level or the sdmmtc;user level. These entries could
   exist in either of these levels.
3. From the sdmmtc;config level run config <fileset name>.
```

***Note:*** Long lines in the display were wrapped.

### Important password information

For new installations, PassThru accounts are created. For upgrades from SN05 with correct configuration the old style cmuser, core0user, and core1usr accounts are deleted and then reconfigured as true PassThru accounts. For upgrades without correct configuration data, no changes are made to the existing setup; manual deletion of accounts and reconfiguration of the fileset is required to create the PassThru accounts.

These new PassThru accounts are created without passwords. In this configuration, users log in to the CS 2000 Core Manager or CBM with a username of cmusr, core0usr, or core1usr, and are immediately forwarded to a destination host. The destination host provides a login with password authentication. If password authentication is preferred on the CS 2000 Core Manager or CBM, in addition to the destination host, then reconfigure the accounts at the passthru level of sdmmtc or cbmmtc.

### Offices without a CS 2000 Core Manager or CBM

Offices without a CS 2000 Core Manager or a CBM require manual action to ensure that load delivery is complete. Failure to perform these actions may result in a “no boot” situation. Two tests are available to determine this situation:

- The CS 2000 Management Tools server boots the cards in the SAM21 shelf. This is indicated at the CS 2000 SAM21 Manager client if the SAM21 EM Server IP value at the Reprovisioning window is also the value for Server IP on the same window.
- If the command **echo $SDM_IP** returns a blank line from a command prompt at the CS 2000 Management Tools server.

#### Required actions for offices without a CS 2000 Core Manager or CBM

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

**1** Become the superuser with the **su - root** command and enter the root password when prompted.

**2** View the /etc/hosts file:

```
# cat /etc/hosts
```

**3** If values for `core`, `core0`, and `core1` are not listed, enter them in the file.

- `core` is the same IP address as the ACTIVEIRM IP address. For example, 172.16.16.72.
- `core0` is the same as the `core` value, but the last octet is 5 less than the last octet of the `core` value. For example, 172.16.16.67.
- `core1` is the same as the `core` value, but the last octet is 2 less than the last octet of the `core` value. For example, 172.16.16.70.

Make a backup copy of the /etc/hosts file:

```
# cp /etc/hosts /etc/hosts.bak
```

Enter the values with the vi editor, the dtpad graphical editor, or appending the lines to the end of the file:

```
# echo “172.16.16.72 core” >> /etc/hosts
# echo “172.16.16.67 core0” >> /etc/hosts
# echo “172.16.16.70 core1” >> /etc/hosts
```

4 Edit the /etc/dfs/dfstab file to allow the /data/swd/3pc directory to be shared on the network:

```
# echo "#Begin CCA NFS Configuration" >>
/etc/dfs/dfstab

#  echo "share -F nfs -o rw=core0:core1
/data/swd/3pc" >> /etc/dfs/dfstab

# echo "#End CCA NFS Configuration" >>
/etc/dfs/dfstab
```

5 View the file to ensure the changes are correct:

```
# cat /etc/dfs/dfstab
```

*Ensure that the end of the file resembles the following output.*

```
...
#Begin CCA NFS Configuration
share -F nfs -o rw=core0:core1 /data/swd/3pc
#End CCA NFS Configuration
```

6 Enable the sharing:

```
# /usr/sbin/shareall
```

7 This procedure is complete.

# Electronic Software Delivery (ESD) for Call Agent

Both the PCL and NCL software loads for the Call Agent are available for electronic transfer from Nortel Networks to a customer dropbox. An example of the PCL is CSNN07BG, and an example of the NCL is ncgl_cca_image_5.33.1.0.

**ATTENTION**
This procedure applies only to the following loads: CM Core, CCA LINUX, and MC.

## Audience

This procedure is intended for telephone operating company personnel who have an ESD agreement with Nortel Networks. When the agreement was established, the operating company furnished Nortel Networks with the location of an electronic dropbox and a username and password pair for delivering software loads. When Nortel Networks delivers a software load to the dropbox, an electronic mail notification is sent to the E-mail address specified by the telephone operating company when the ESD agreement was established.

## When to use this procedure

Use this procedure after receiving electronic notification for the following software loads:

- PCL
  - SNC0000n.n.R.PCL.PPC3.vault.nn.D.tar.gz for North America
  - SWC0000n.n.R.PCL.PPC.vault.nn.D.tar.gz for International
  - SEC0000n.n.R.PCL.PPC3.vault.nn.D.tar.gz for SL-100
  - SDC0000n.n.R.PCL.PPC3.vault.nn.D.tar.gz also for SL-100
- NCL
  - 3PC000n0.n.R.NCL.NAP.vault.nn.D.tar.gz for Standard release
  - 3PC0M0n0.n.R.NCL.NAP.vault.nn.D.tar.gz for Maintenance releases

**n**
is an integer value such as 7 and is part of the product order code

**vault**
is a string that identifies the Nortel Networks software vault that holds the software

**nn**
is an integer value that indicates the repository version of the software

## Action

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

**1** Make a temporary directory to store the ESD software:

```
$ mkdir /data/iso_esd
```

**2** Change directory to the newly created location:

```
$ cd /data/iso_esd
```

**3** Ensure that enough disk space is available for the ESD software. For one PCL and one NCL, 500 MB is recommended.

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

*The free space on the device that /data is mounted is printed. The value for "avail" is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes.*

```
$ df -k /data
Filesystem             kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d20       3082223  144123 2876454     5%    /data
```

2876454 / 1000 = 2876 MB free

**4** Transfer the ESD software files from the dropbox on the repository server. The repository server is the machine owned by the telephone operating company that was selected to be the destination for the ESD software files:

```
$ ftp <repository_server>
```

Log in and change directory to the dropbox location on the repository server.

**5** Change the transfer mode to binary.

```
ftp> bin
```

**6** Retrieve the ESD software load:

```
ftp> get <esd_filename>.tar.gz
```

**Example**
**ftp> get 3PC0M070.7.R.NCL.NAP.SDC.1.D.tar.gz**

***Note:*** Determine the actual ESD filename from the Nortel Networks notification, or listing the contents of the dropbox with the **ls** command.

**7** Repeat step 6 for all ESD software loads recorded in the notification from Nortel Networks and then end the FTP session:

```
ftp> bye
```

**8** Extract the ESD software load from the tape archive format:

```
$ gtar xvzf <esd_filename>.tar.gz
```

**Example**
**$ gtar xvzf 3PC0M070.7.R.NCL.NAP.SDC.1.D.tar.gz**

*The ESD software load is uncompressed, and a new directory named after the ESD software filename is created. The directory name is the name of the ESD filename without the .tar.gz suffix. The contents of the ESD software load are placed in this new directory.*

**9** Change directory to the newly created directory:

```
$ cd <esd_filename>
```

**Example**
**$ cd 3PC0M070.7.R.NCL.NAP.SDC.1.D**

**10** The remainder of this procedure depends on the ESD file:

| If the ESD file is a | Do |
|---|---|
| PCL | step 11 |
| NCL | step 12 |

**11** This step applies to PCL ESD software loads only.

**a** Rename the PCL file from a .bin1020 suffix to a .img1020 suffix:

```
$ mv SNC0007_CM.bin1020 SNC0007_CM.img1020
```

**b** Record the location of the call processing application files, /data/iso_esd/<esd_filename>, such as /data/iso_esd/SNC00007.7.R.PCL.PPC3.SDC.2.D.

c Go to procedure Restore call processing application files on page 55 and specify this location for the call processing application files instead of /cdrom/cdrom0 in step 5. This procedure is complete.

**12** This step and the remainder of the procedure applies to NCL ESD software loads only.

Become the root user:

```
$ su - root
```

*A prompt for the root password is presented. Enter the root password.*

**13** The ESD software is formatted as an ISO 9660 image. Use the mount_iso.ksh script to mount the ISO 9660 image:

```
# /opt/nortel/sspfs/Scripts/mount_iso.ksh mount
/data/iso_esd/<esd_directory>/<iso_image>.img.
tape
```

**Example**
**# mount_iso.ksh mount /data/iso_esd/3PC0M070.7.R.NCL.NAP.SDC.1.D/iso_ncgl_cca-5.33-1.0.img.tape**

***Note:*** A space is required after the word mount and before the word /data.

*A response is printed to the terminal. Use the response to determine if the command was successful:*

**mount_iso.ksh command responses**

| Response | Meaning |
|---|---|
| Is is very important for the user of this command to know that if you mount an iso image. It is a MUST that you unmount an image before removing the image file. If the file is deleted while the OS has it mounted, it can be harmful to the runtime applications on this unit | This response indicates success. |
| Provided full path to ISO image does not exist | Verify the location and name of the ISO 9660 image, such /data/iso_esd/3PC0M070.../...img.tape, and retry. |

**mount_iso.ksh command responses**

| Response | Meaning |
|---|---|
| ISO Image Already Mounted | Enter **mount_iso.ksh umount** to unmount whatever ISO 9660 image is currently mounted, and retry. |
| Error creating the image device location | This response indicates an operating system error with the loopback file driver. Retry the command, and if it fails a second time, contact Nortel Networks support personnel. |
| ERROR MOUNTING <ESD_filename> | This response indicates that either the ISO 9660 file is corrupt, or the `/tmpmnt` directory has been deleted. |

*The contents of the ESD software file are available in directory `/tmpmnt/noarch`.*

**14** To install the software now, list the contents of the `/tmpmnt/noarch` directory (**ls /tmpmnt/noarch**) and record the name of the .rpm file.

Enter the **platform_load_install.sh** command.

Select **2**, Install RPM from Disk.

Enter the .rpm filename when prompted.

Enter /tmpmnt/noarch when prompted for the location of the .rpm file.

**15** To install the software later, copy the contents to a location on the CS 2000 Management Tools server. When installing the software at the later date, proceed as in step 14 except specify the location of the software instead of /tmpmnt.

**16** Unmount the ESD file:

```
# mount_iso.ksh umount
```

**17** This procedure is complete.

# Transfer call processing application patch files

Complete this procedure at least two days before the ONP.

**ATTENTION**
Do not perform this procedure for a platform only upgrade.

Call processing application patch files are delivered electronically through Regional Patch Selector (RPS). Contact Nortel Networks support personnel for information about RPS and call processing application patch files.

***SITE — At a terminal window***

**1** Log in to the CS 2000 Core Manager or CBM as the root user if not already logged in:

```
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

**2** Change directory to the location of the call processing application patch files:

```
# cd <path_to_files>
```

**3** Open an FTP session to the call processing application:

```
# ftp cm
```

**4** Login with a valid username and password.

***Note:*** The user must have FTP privilege and permission to write to SFDEV.

**5** Change directory to the store file device (SFDEV):

```
ftp> cd /SFDEV
```

**6** Set the transfer options:

```
ftp> bin; site lrecl 128
```

**7** Use the put command to transfer the call processing application patch files:

```
ftp> put <patch_file_name>
```

***Note:*** Optionally use the MPUT and PROMPT commands to transfer multiple files. The MPUT command transfers multiple files. The MPUT command accepts wildcard pattern matching characters. The PROMPT command prevents prompting for each file.

**8** This procedure is complete.

## Restore call processing application files

Complete this procedure when the final shipment of software arrives.

**ATTENTION**
Do not perform this procedure for a platform only upgrade.

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

**1** Insert the DVD in the CDROM tray.

***SITE — At the CORE0 or CORE1 window***

**2** Exit the Call Agent Manager:

```
> 0 all
```

*The operating system prompt is returned.*

```
[mtc@hostname mtc]$
```

**3** Change directory to the destination directory for the upgrade call processing application image:

```
> cd /3PC/<sd0x>/<image_file_location>
```

**Example**
**> cd /3PC/sd00/image**

**4** Open an FTP session to the CS 2000 Management Tools server and log in:

```
> ftp <cs_2000_mgmt_tools_ip>
```

***Note:*** Log in to the CS 2000 Management Tools server as a user with privilege to change directory and transfer files with FTP.

**Example**

```
[mtc@10.40.44.67 image0]$ ftp <cs_2000_mgmt_tools_ip>
Connected to <cs_2000_mgmt_tools_ip>.
220 ProFTPD 1.2.8 Server (Authorized Use Only) [hostname]
Name (hostname:mtc): maint
331 Password required for maint.
Password:
230 User maint logged in.
ftp>
```

5 Change directory, list the file size, change the mode to binary, and get the file:

```
ftp> cd /cdrom/cdrom0
ftp> ls
ftp> bin
ftp> prompt
ftp> mget *
```

***Note:*** Do not transfer a file with a name longer than 32 characters.

**Example**

```
ftp> cd /cdrom/cdrom0
250 CWD command successful.
ftp> ls
MUC00020810335_MS.img1020
SNC00007810335_CM.img1020
ftp> bin
200 Type set to I.
ftp> prompt
Interactive mode off.
ftp> mget *
local: SNC00007810335_CM.img1020 remote: SNC00007810335_CM.img1020
200 PORT command successful.
150 Opening data connection for SNC00007810335_CM.img1020 (binary mode)
226 Transfer complete.
150 Opening data connection for MUC00020810335_MS.bin1020 (binary mode)
226 Transfer complete.
```

6 End the FTP session by typing bye:

```
ftp> bye
```

***At the ACTIVECM window***

7 Enter the DISKUT level and import the upgrade call processing application and Message Switch images:

```
> DISKUT
> IMPORT <volume_name>
```

**Example of IMPORTing image files**

```
DISKUT:
>IMPORT SD00IMAGE1

Attempting to import 2 files selected on SD00IMAGE1.

Imported MUC00020810335_MS.img1020 as MUC00020810335_MS  IMAGE 1020.
Imported SNC00007810335_CM.img1020 as SNC00007810335_CM  IMAGE 1020.

Imported 2 files successfully of 2 attempts on SD00IMAGE1.
```

*The call processing application and Message Switch images are imported from the native file system into the call processing application file system. If the disk does not have enough space, a prompt to increase the volume size is presented.*

**8** Use the set boot file command to enter the image in to the ITOC and make it bootable:

```
> ITOCCI
> SBF CM <filename_cm> 15
```

**Example**
**> SBF CM SNC00007547159_CM 15**

*The complete ITOC is printed to the terminal. If an MS image was loaded too, use the SBF MS <image_name> <position> command for the MS image too. If there is no free space in the ITOC use the clear boot file command to remove the oldest entry: CBF CM <image_name>.*

***SITE — At a CS 2000 Management Tools terminal***

**9** Issue the eject command to open the CDROM tray:

```
# eject
```

*Software on the CS 2000 Management Tools server unmounts the DVD and opens the CDROM tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session is ended and no users have changed directory into /cdrom/... directory. Reenter the eject command.*

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

**10** Remove the DVD from the CDROM tray.

**11** This procedure is complete.

# Perform MS tests

**ATTENTION**
Only perform this procedure for offices with Message Controllers and a Message Switch.

If the CS 2000 - Compact is configured with Message Controller cards, test the Message Switch at this point.

***SITE — At the ACTIVECM window***

**1** Enter the MS level of the MAP:

```
> MAPCI;MTC;MS
```

*The MS level of the MAP is displayed and the master and slave Message Switches are identified.*

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

MS                Message Switch    Clock    Shelf  0      Inter-MS Link 0 1
 0 Quit        MS 0      .          Master          .                    . .
 2             MS 1      .          Slave           .                    . .
 3
 4
 5
 6 Tst_       MS:
 7 Bsy_
 8 RTS_
 9
10 LoadMS_
11
12 SwMast
13 Shelf
14 QueryMS
15
16
17 InterMS_
18 Clock
  ADMIN
Time  09:52  >
```

2 Busy the slave Message Switch:

```
> BSY <x>
```

*MS101 and MS305 log reports and a major ManB alarm are raised.*

3 Test the slave Message Switch:

```
> TST <x>
```

*The results of the test are displayed. If the test failed, resolve any problems and repeat the test.*

4 Return the busied Message Switch to service:

```
> RTS <x>
```

*MS304, MS100, and MS104 log reports are generated. The major ManB alarm clears, and a report about the RTS is displayed.*

*Wait 5 minutes to ensure the clocks are stable and to allow the hardware audit to run. Both Message Switches should be in service.*

5 Switch clock mastership:

```
> SWMAST
```

*Two MS104 log reports are generated and the Master and Slave Message Switches exchange mastership.*

*Wait 10 minutes to allow the Message Switch clocks to stabilize.*

6 Test the other Message Switch by completing steps 2 through 4.

7 After completing the tests, quit to the CI level:

```
> QUIT ALL
```

8 Monitor front end stability logs until the scheduled start of the ONP.

# Clean up SFDEV

Use this procedure to remove files from the Store File Device (SFDEV).

If call processing application patch files were downloaded in SFDEV, do not delete these files.

***ACT — At the ACTIVECM window***

1 Determine the files in SFDEV:

```
> LISTSF ALL
```

2 Copy files from SFDEV to storage:

```
> SCANF SFDEV COPY <disk_vol> NAME <file_name>
```

**disk_vol**
is the destination storage volume like SD00TEMP

**file_name**
is the name of the file to copy

3 Erase files that are not essential from SFDEV:

```
> ERASESF <file_name>
```

4 This procedure is complete.

# Verify table ACDGRP

Perform this procedure to prevent the software from incorrectly renumbering tuples in table ACDGRP during the call processing software upgrade.

### *ACT — At the ACTIVECM window*

**1** Determine if there are non-consecutive keys in table ACDGRP:

```
> OMSHOW ACDGRP ACTIVE
```

**2** Review the output and note if any keys are missing:

```
ACDGRP
CLASS:   ACTIVE
START:2002/06/20 09:30:00 THU; STOP: 2002/06/20 09:54:27 THU
SLOWSAMPLES:        15 ; FASTSAMPLES:        147 ;
       KEY (AUTOMATIC_CALL_DISTRIB_GROUP)
          ACDOFFR    ACDANSR   ACDDFLCT   ACDABNDN
            ACDNS   ACDPRMPT   ACDBLOCK   ACDTMOFL
         ACDTMINF   ACDTMANS     ACDCIF    ACDXFER
           ACDCPK   ACDUSAGE   ACDUSAG2    ACDICQD
          ACDREQD    ACDDMCT   ACDRQABN   ACDRQRTE

   0 NACDP
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0

   2 NACD2P
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
```

Index key 1 is missing.

**3** If any index keys are missing, have translation personnel provision dummy tuples in the key indexes. Also provide datafill in table DNROUTE for each tuple added to table ACDGRP.

**4** This procedure is complete.

## Fill in test call scripts

Test calls should be made and verified to work as expected prior to the software upgrade, preferably on the day of the ONP. Identify calling irregularities ahead of time. This will avoid unnecessary investigation of a pre-existing condition after SWACT.

**ATTENTION**
Nortel Networks recommends that SITE personnel complete their Test Call Scripts before continuing with the software release upgrade process. Identifying calling irregularities now avoids unnecessary troubleshooting after SWACT.

This section presents generic guidelines for creating a test call plan to be used both before and after the switch of activity (SWACT) to a new load.

The purpose of test calls is to verify the performance of newly installed software for telephone switching systems. Test calls can ensure the smooth operation of thousands of calling situations with different combinations of telephone sets, service features, and traffic conditions on the network. Such testing helps ensure the availability and reliability of features and services for telephone users.

“Test call scripts” refers to the verification calls as predefined by the Telephone/Carrier Operating Company. These are test calls to be performed after activating the new software load in order to confirm acceptability of the new load. In the ONP procedure the test call scripts are put to use as follows:

- As a part of site preparation, this procedure instructs the operating company to fill in and test the test call scripts before beginning the upgrade. This is to provide a thorough test plan exercise for validating the new software load.
- Then, after activating the new software load, the operating company performs the test call scripts again to verify the software load.

The test call scripts provided below are only examples of call types that could be included in the Test Call Scripts. These samples include only basic call processing tests and provide some, but not all, critical test calls. These are provided only as a guideline. Each telephone/carrier

office should determine the best mix of test calls to use based on the office's unique configuration.

**ATTENTION**

The test calls listed in the following procedures will not apply to every office.

The telephone office will have to customize the list according to its own particular configuration.

Nortel Networks recommends including the following items in your POSTSWACT testing routine.

Add any other items that are determined to be important.

POSTSWACT call checklist

__ Verify date, time and DIALTONE

__ Perform Critical Call Tests (for example, 0- and 0+7/10). See the following procedure.

__ Perform IDDD (International Direct Distance Dialing) calls

__ Check Equal Access origination and termination

__ Perform CCIS (Common Channel Inter-office Signaling) calls

__ Verify ACTS (Automatic Coin Toll Service)

__ Verify DRAMS (announcements and SIT tones)

__ Check WATS (Wide Area Telephone Service), INWATS, OUTWATS, 2-way

__ Verify Pay Station Coin Control (Coin Collect and Coin Return)

__ Verify miscellaneous services such as 311, 411, 611, and repair services

__ Check EAS (Extended Area Service) calls

__ Perform TOPS (Traffic Operator Position System) calls

__ Perform MCCS (Mechanized Calling Card Service) calls

__ Perform DISA (Direct Inward System Access) calls

__ Verify Custom Calling Features

***SITE — At the office***

**1** Perform the critical test calls and record the results.

| Test description | From: line type or CLLI | To: call type and digits dialed | Test result |
|---|---|---|---|
| Check for DIALTONE on all line modules | | | |
| Verify ‘0’ minus route | | | |
| Verify ‘0’ plus route | | | |
| Verify ONI 1-7, 1-10 digits | | | |
| Verify EAS incoming and outgoing routes | | | |
| Verify CAMA routes | | | |
| Verify local Tandem routes | | | |
| Verify DDO routes | | | |
| Verify Directory Assistance | | | |
| Verify critical service routes (911, police, file, hospitals, and radio stations) | | | |
| Verify TOLL COMP (DTS) route | | | |
| Verify 1FR intra-office call | | | |
| Verify Remotes:<br>• EAS outgoing (one route)<br>• ‘0’ plus ‘0’ minus<br>• CAMA ANI<br>• 1FR intra-Remote | | | |
| Verify Operator Intercept route | | | |
| Verify all (idle) customer/network trunks | | | |

**2** Perform additional test calls sample.

**a** Verify regular POTS calls:

line (1FR) -> line (1FR)

(969-xxxx -> 969-xxxx)

line (PPHONE) -> trunk -> line (1FR)

(969-xxxx -> 9-1-514-970-xxxx)

**b** Verify use of different PM types:

line (LM) -> line (RLM)

(969-xxxx -> 969-xxxx)

line (LCM) -> line (RLCM)

(969-xxxx -> 969-xxxx)

**c** Verify use of different trunk types:

line (1FR) -> PTS trunk -> line (1FR)

(968-xxxx -> 969-xxxx)

line (1FR) -> ISUP trunk (all variants supported by office) -> line (KSET-Disp M5209T)

(968-xxxx -> 6-456-xxxx)

**d** Verify ISDN calls:

line (KSET-Disp M5317T) -> trunk -> line (KSET-Disp M5209T)

(968-xxxx -> 6-456-xxxx)

line (PPHONE-Disp M5317T) -> trunk -> line (1FR-Disp Maestro)

(968-xxxx -> 9-969-xxxx)

line (KSET-Disp M5317T) -> trunk -> line (PPHONE-Meridan Bus.)

(968-xxxx -> 9-1-819-456-xxxx)

line (KSET-Disp M5317T) -> line (KSET-PSET)

(968-xxxx -> 968-xxxx)

line (BRAMFT set) -> line (BRAFS set)

(968-xxxx -> 968-xxxx)

line (1FR) -> line (BRAKS set)

(968-xxxx -> 968-xxxx)

**3** Proceed after test call scripts are verified.

# Perform TABAUDIT

Begin this procedure 30 calendar days before the software delivery application date and complete the TABAUDIT with no errors at least 10 days before the ONP. Nortel Networks Global Software Delivery recommends scheduling automatic TABAUDITs (AUTOTABAUDIT), rather than manual TABAUDITs. TABAUDIT must complete successfully before the ONP.

Restrictions on AUTOTABAUDIT:

- Only one user at a time is allowed to enter the AUTOTABAUDIT level.
- Before executing AUTOTABAUDIT, a list of session parameters must be defined from within the AUTOTABAUDIT level.
- Only one AUTOTABAUDIT session can execute at a time. However, multiple AUTOTABAUDIT sessions can be scheduled.
- The parameters for the active AUTOTABAUDIT session cannot be changed without terminating the session first.
- AUTOTABAUDIT cannot be executed at the same time as TABXFR or an image dump.
- For wireless applications on HLR offices, AUTOTABAUDIT should be scheduled to execute during off hours to avoid delays with subscriber provisioning.

***SITE — At the ACTIVECM window***

**1**

**CAUTION**
**Possible service interruption**
Review software delivery bulletins and current warning bulletins about TABAUDIT.

Enter the automated table audit level:

```
> TABAUDIT; AUTO
```

**2** Clear the list of tables to be included in the check:

```
> CLEAR INCLUDED
```

3 Clear the scheduled list of time frames:

```
> CLEAR SCHEDULE ALL
```

***Note:*** This command clears all scheduled TABAUDIT sessions identified in table AUTOTAB.

4 Set all tables for verification:

```
> INCLUDE ALL
```

5 Define the scheduled AUTOTABAUDIT session:

```
> TIMEFRAME SINGLE <start_time> [<start_date>]
<stop_time> [<stop_date>]
```

**start_time**
is the hour and minute to begin the TABAUDIT and is specified as HH:MM, such as 23:30

**start_date**
is an optional parameter and is specified as YYYY:MM:DD, such as 2002:06:21

**stop_time**
identifies the latest time by which that the TABAUDIT must complete

***Note:*** The timeframe must be 30 minutes or more.

6 Verify the parameters:

```
> STATUS
```

```
AUTOTABAUDIT is scheduled to execute during the start
and stop period between the start and stop dates.
-------------------------------------------------------------------------
|                                                                       |
|                        AUTOTABAUDIT STATUS                            |
|                                                                       |
-------------------------------------------------------------------------
| Active Timeframe    | Executing Timeframe  |                          |
-------------------------------------------------------------------------
| Start        Stop   |   Start      Stop    | Scheduling  |  REGULAR   |
| Date         Date   |   Time       Time    | Option      | or SUBSET  |
-------------------------------------------------------------------------
|                                                                       |
|2002/06/24 2002/06/24    18:30      20:00   | SINGLE      |  REGULAR   |
|                                                                       |
-------------------------------------------------------------------------
Current time      : 2002/06/24 07:16:07
AUTOTABAUDIT      : Inactive
The following events were logged while verifying tables:
 1 TABAUDIT aborted. All included tables not verified. Out of time.
The following tables are included for the REGULAR AUTOTABAUDIT:
  From table VERSIONS (0)                  to table INWATNPA (1408).
No tables have been excluded for the REGULAR AUTOTABAUDIT.
No tables have been included for the SUBSET AUTOTABAUDIT.
The following tables are excluded for the SUBSET AUTOTABAUDIT:
  From table VERSIONS (0)                  to table INWATNPA (1408).
```

**7** Begin the table audit;

**> EXECUTE**

**8** Confirm the table audit:

**> Y**

**9** The audit can require 30 minutes to complete.

**10** Verify the table audit results:

**> REPORT ERRORS**

| If | Do |
|---|---|
| no errors are reported | step 12 |
| errors are reported | Correct the errors using the table editor and repeat from step 4. Refer to the Additional information. |

**11** If any tables failed, perform the following steps for each table.

**a** Quit to the TABAUDIT level:

```
> QUIT
```

**b** Include the failed table:

```
> INCLUDE <table_name>
```

**c** Execute the TABAUDIT:

```
> EXECUTE
```

**d** View the results:

```
> REPORT <table_name>
```

**e** Repeat from step b for each failed table.

**12** Quit to the CI level:

```
> QUIT ALL
```

**13** This procedure is complete.

## Additional information

Use the following procedure to assist in repairing tables.

***SITE — At the ACTIVECM window***

**1** Enter the table that has an error:

```
> TABLE <table_name>
```

**tab_name**
is a table name like TRKMEM

**2** Position on the failed tuple:

```
> POS <tuple>
```

**tuple**
is the failed tuple such as “AL7ITICS7 2”

**3** Check the tuple:

```
> CHECK
```

**4** Note the error message and make corrections.

**5** Repeat this procedure for all failed tables.

## Execute SWUPGRADE READY

Nortel Networks Global Software Delivery personnel complete this procedure at scheduled milestones before the ONP.

At any time during this procedure, to determine the status, use the **DISP STEPS** command. Help for steps is available with the **HELP** command. A step can be re-run with the **RUNSTEP <step_name>** command. Ensure that all steps complete successfully, but a step can be overridden with the **OVERRIDE** command. To cancel the procedure, use the **CANCEL** command.

The steps are determined by the CS 2000 - Compact configuration. If the CS 2000 - Compact is configured with Message Controller cards, more steps are provided.

**SWUPGRADE READY steps**

| without Message Controllers | with Message Controllers |
|---|---|
| SETUP_ENV_VARS | SETUP_ENV_VARS |
| | VERIFY_SN_PECS_INFO |
| VERIFY_LOGS_INFO | VERIFY_LOGS_INFO |
| DEVICE_CHECK | DEVICE_CHECK |
| TABAUDIT_VERIFY_TABLES | TABAUDIT_VERIFY_TABLES |
| | DISPLAY_PERIPHERAL_LOAD_NAMES |
| | DISPLAY_SPM_LOADNAMES |
| | DISPLAY_PRL_LOADS |
| | CHECK_ISN_PMS |
| | DISPLAY_MS_FW_LOADS |
| | VERIFY_PM_LOAD_NAMES |
| | LIUINV_CHECK |
| | C7LINK_CHECK |
| | CHECK_LTCINV |

**SWUPGRADE READY steps**

| without Message Controllers | with Message Controllers |
|---|---|
| DISPLAY_NOP_USERS | DISPLAY_NOP_USERS |
| DISPLAY_DPP_VERSION | DISPLAY_DPP_VERSION |
| | CHECK_LCMINV |
| SBA_CHECK | SBA_CHECK |
| SBA_VOLSIZE_CHECK | SBA_VOLSIZE_CHECK |
| READY_STATUS | READY_STATUS |
| READY_COMPLETE | READY_COMPLETE |

***SDE — At the ACTIVECM window***

**1** Enter the SWUPGRADE level:

```
> SWUPGRADE READY
```

**2** Begin the process:

```
> START
```

*Step SETUP_ENV_VARS begins. This step sets the environment variables that will be used during the READY session. Default values appear in square brackets and variables without brackets have no default. To accept the default value press the Return key without entering a value.*

*Values consisting of more than one word must not be enclosed in quotes. If they are, the quotes will be considered as part of the word and the variable will be either set to an incorrect value or not set at all.*

**a** Set the TRACE_USER variable.

**TRACE_USER (no default)**
Holds the USER name on whose console output messages are printed. Changing the value of this variable, also changes the value of the TRACE_DEVICE variable, and causes the output to be redirected to the new USER device.

Value: <user name> or ME - a user name, such as ADMIN, or ME which indicates the current user

***Note:*** For clarity purposes, it is recommended to set this variable to a user other than the current user.

The USER must be LOGGED IN when this variable is set. The current setting is: <none>

```
> ME
```

**b** Do not change the TRACE_DEVICE variable, press the Enter key.

**TRACE_DEVICE**
Holds the device name on which output messages are printed. Changing the value of this variable causes the output to be redirected to the new device.

Value: <trace device name> - a string, such as MAP

***Note:*** For clarity purposes, it is recommended to set this variable to a device other than the terminal currently logged onto.

The current setting is: <none>

```
>
```

**c** Set LOGS variable.

**LOGS**
Holds the names of the logs that are checked by the LOGS step. More than one log can be specified by entering log names separated by a blank.

**Example**
CM — Check CM logs and display a message if CM logs are recorded.

**Example**
'SWERR TRAP' — Check traps and swerrs. Display a message if traps or swerrs are recorded.

The current setting is: TRAP SWERR

```
> TRAP SWERR
```

**d** Set TO_CSP_CM_LOAD variable. Enter the value of the CSP load number.

**TO_CSP_LOAD**
The TO_CSP_LOAD variable allows the user to set the CSP load to which the site plans to upgrade. This variable is then used to check the PMs for a software load which equals this value.

The current setting is: 0

```
> 19
```

***Note:*** CSP 19 is equivalent to the SN06 release.

**e** Do not set the PM_VERIFY_FILE variable, press the Enter key.

**PM_VERIFY_FILE**
The PM_VERIFY_FILE variable allows the user to set which verification file will be used to validate if the queried peripheral module loads are valid.

The current setting is: NONE

>

**f** Do not change the PRINTER variable, press the Enter key.

**PRINTER**
The PRINTER variable holds the name of the printer on which output messages are recorded. The printer echoes all output sent to the trace device. Changing the value of this variable causes the recording to be directed to the new device.

Value: <printer name> or SINK

where <printer name> is a device datafilled in table TERMDEV. SINK indicates not to record to a printer device.

The current setting is: SINK

>

**g** Do not change the PAUSE_ENABLED variable, press the Enter key.

**PAUSE_ENABLED**
PAUSE_ENABLED is used to determine if the READY steps will run continuously or be paused out after executing. A NO setting allows the READY platform to run until completion of all the steps. A YES setting prompts the process to pause after each step is run. This pause allows time for the user to review the results and set a step COMPLETED/NEEDED before proceeding.

***Note:*** Type HELP STEP_STATUS for more information on setting the step status.

The current setting is: YES

>

```
SWUPGRADE variables for target READY:

Variable Name                                        Value
-------------------------------------------------------------
TRACE_USER                          =    ME
TRACE_DEVICE                        =    TELNSVR00033
LOGS                                =    TRAP SWERR
TO_CSP_LOAD                         =    19
PM_VERIFY_FILE                      =    NONE
PRINTER                             =    SINK
PAUSE_ENABLED                       =    YES

Setup completed.
Enter GO to begin execution of steps.
```

**h** Commit the variable changes:

**> GO**

*Step SETUP_ENV_VARS completes.*

*If the CS 2000 - Compact is configured with Message Controller cards, step VERIFY_SN_PECS_INFO runs. This step checks and prints the Message Switch software load and all the hardware in the Message Switch.*

*Step VERIFY_LOGS_INFO runs and completes. This step displays any log reports provided in environment variable LOGS. These logs should be checked periodically for front-end stability. Include or exclude any log(s) the user would like displayed.*

*Step DEVICE_CHECK runs. This step verifies that all devices on the active CPU are in an OK, OFFLINE, or UNEQUIPPED status. These are acceptable states for SWACT. Any devices found in any other state are displayed.*

*Step TABAUDIT_VERIFY_TABLES runs. This step verifies that TABAUDIT has been executed and tables to be dumped and restored have been audited in the last thirty days.*

*If the CS 2000 - Compact is configured with Message Controller cards, steps DISPLAY_PERIPHERAL_LOAD_NAMES, DISPLAY_SPM_LOADNAMES, DISPLAY_PRL_LOADNAMES, CHECK_ISN_PMS, and DISPLAY_MS_FW_LOADS run. These steps print all the PM names, locations, and software load names for the PMs in the office, as well as the firmware loads in the Message Switch.*

**3** If the CS 2000 - Compact is configured with Message Controller cards, step VERIFY_PM_LOAD_NAMES runs. This step queries all the PMs with downloadable software and verifies that each PM is loaded with the load specified in PM_VERIFY_FILE. PM_VERIFY_FILE was set during step SETUP_ENV_VARS. This file is a PM to PM load cross reference. If the file is not available, or a PM is running a different load, the process stops. Correct the problem, type GO and press the Enter key.

*Step VERIFY_PM_LOAD_NAMES completes.*

*If the CS 2000 - Compact is configured with Message Controller cards, steps LIUINV_CHECK, C7LINK_CHECK, CHECK_LTCINV, and CHECK_LCMINV run. These steps ensure that no LIU name has a LIUNO greater than 512, that all MSB7 and LIU7 PMs have field LINKNAME datafilled, that all DTCs datafilled in table LTCINV for CCS7 are datafilled correctly, and that LCMs have the amount of memory datafilled in table LCMINV and that the LCMs are in service.*

**4** Step DISPLAY_NOP_USERS runs and completes.

*This step displays all NOP/MPC users and their status.*

**5** Step DISPLAY_DPP_VERSION runs and completes.

*This steps displays DPP hardware and software information and DPP status.*

**6** Steps SBA_CHECK runs and completes.

*This step verifies that on an XA-Core machine if an upgrade is being performed to CSP16 and beyond, then all the backup volumes are configured only on IOP disks. No older disk types are supported as backup for the SBA streams on an XA-Core platform from CSP16 onwards.*

**7** Step SBA_VOLSIZE_CHECK runs and completes.

*This step verifies that the size of the volumes that are configured as backup for SBA satisfy the minimal size requirements. This check will print out those stream-volume pairs whose backup volume sizes are below the minimal criterion that have been set.*

**8** Step READY_STATUS runs and completes.

*This step displays step state and status.*

**9** Step READY_COMPLETE runs and completes. Ensure that step READY_STATUS indicates all steps are complete.

```
> QUIT
```

*This step reminds the user to quit the SWUPGRADE increment and QUIT from the switch after the READY program is completed.*

**10** This procedure is complete.

## Dump call processing application image

Complete this procedure the day of the ONP.

***SITE — At the ACTIVECM window***

**1** Enter the disk utilities level:

```
> DISKUT
```

**2** Verify that there are at least 500 000 free blocks for an office image:

```
> LV SD00IMAGE; LV SD01IMAGE
```

```
> LV SD00IMAGE; LV SD01IMAGE
Volumes found matching the prefix SD00IMAGE:
-----------------------------------------------
NAME        TYPE      TOTAL       FREE TOTAL  OPEN  ITOC  LARGEST
                     BLOCKS     BLOCKS FILES FILES FILES  FREE SEGMENT
-------------------------------------------------------------------------
SD00IMAGE   STD    1638400     822665     0     0     0     822665
Total number of volumes matching prefix SD00IMAGE : 1.
Volumes found matching the prefix SD01IMAGE:
-----------------------------------------------
NAME        TYPE      TOTAL       FREE TOTAL  OPEN  ITOC    LARGEST
                     BLOCKS     BLOCKS FILES FILES FILES  FREE SEGMENT
-------------------------------------------------------------------------
SD01IMAGE   STD    1638400     814430     3     0     1     814430
Total number of volumes matching prefix SD01IMAGE : 1.
>
```

***Note:*** If there is not enough space, determine if old images can be deleted. Use the **DDF** command to delete files. Refer to DDF Example for more information.

**3** Dump the image to a disk volume:

```
> AUTODUMP MANUAL
```

if AUTODUMP is active for the office.

*or*

```
 > DUMP <image_name> <disk_vol> ACTIVE UPDATE
VERBOSE NODE CM
```

**image_name**
is the name of the file to create

**disk_vol**
is sd00image or sd01image

if AUTODUMP is not active for the office

*The dump can require two hours to complete.*

4 Record the name of the image on a sheet of paper. If this upgrade is an ONP, it is important to have a current image as a backup in the event that the ONP fails. If this is a platform only MR upgrade, it is necessary to know the name of the image so it can be loaded during procedure LDMATE (Load inactive) on page 191.

5 Nortel Networks recommends backing up the image. The backup procedure is documented in *Call Agent Fault Management*, NN10087-911 and is reproduced here for convenience under heading Backup image.

6 This procedure is complete.

If this is a platform only upgrade, proceed to Boot new platform software on page 181. 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 87.

## DDF Example

The following figure shows an example of using the DDF command.

```
>diskut
Disk utility now active.
DISKUT:
>lf sd00image0

File information for volume SD00IMAGE0:
{NOTE:  1 BLOCK = 512 BYTES }


-------------------------------------------------------------------------
FILE NAME                       O R I O O V FILE   MAX    NUM OF    FILE
                                R E T P L L CODE   REC   RECORDS    SIZE
                                G C O E D D        LEN        IN      IN
                                    C N                     FILE  BLOCKS
-------------------------------------------------------------------------
CSNW06BA                        I F            0  1020    208457  415286
.ITOC                           O F            0  1024         1       2
SCS06BA_WC_0131_CM              I F Y          0  1020    213073  424482
SCS05BK_WC_0131_CM              I F            0  1020    196563  391591
SCS05BK_WC_0128_CM              I F            0  1020    196563  391591

>ddf CSNW06BA
Delete CSNW06BA from volume SD00IMAGE0?
Please confirm ("YES","Y","NO","N"):
>y
File CSNW06BA has been deleted from volume SD00IMAGE0.
```

## Backup image

Use the following procedure to back up a call processing application image.

***At the active Call Agent Manager window (CORE0 or CORE1)***

**1** Quit the Call Agent Manager interface:

```
> QUIT ALL
```

**2** Change directory to the location of the image. If the image was dumped to disk SD01, substitute sd01 for sd00 in the following figure.

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

**3** Use the mount command to determine the IP addresses of the STORM units.

```
[mtc@ip_address mtc]$ mount
```

*Determine which STORM unit provides sd00 and which provides sd01. This information is needed in* step 7*.*

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

***At the CS 2000 Management Tools frame***

**4** Insert a DVD-RW (write once DVD) in the CDROM tray. A rewritable DVD (DVD+RW) will not work. If the CS 2000 Management Tools server uses two Sun Microsystems Netra 240 machines, insert the DVD-RW into the active unit. The active unit is identified by a lit USER LED.

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

**5** Log in as a maintenance level user such as the maint user. Root permissions are needed later in this procedure to write the DVD.

**6** Change directory to `/data` and create a temporary directory to store the files:

```
$ cd /data
$ mkdir tmp
```

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

**7** Secure copy the files from the STORM unit to the `/data/tmp` directory created in step 6. Enter the root password for the STORM unit when prompted.

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

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

**stormip**
is the IP Address of the STORM unit such as 10.40.44.238. Use the value determined in step 3.

**/path_to_file**
is the absolute path to the files on the STORM unit to copy such as
`/nfsserv/3pc/cs/sd00/image0/IMG_TO_BACKUP`

**Example**
Copy an office image named S040210135002_CM from SD00ADUMP0:

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

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

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

**8** Rename the image file to end in ".img1020:"

```
$ cd /data/tmp
$ mv <IMG_TO_BACKUP> <IMG_TO_BACKUP>.img1020
```

9 Change directory to `/data` and make an ISO9660 image named dvdimage.iso with Rock Ridge extensions from the image:

```
$ cd /data
$ mkisofs -R -o /data/dvdimage.iso
/data/tmp/<IMG_TO_BACKUP>.img1020
```

***Note:*** There is a space after /data/dvdimage.iso and before /data/tmp/<IMG_TO_BACKUP>.img1020

*Status is printed to the terminal:*

**Create dvdimage.iso with mkisofs command**

```
$ mkisofs -R -o /data/dvdimage.iso /data/tmp/<IMG_TO_BACKUP>.img1020
4.56% done, estimate finish Tue Feb 10 14:52:00 2004
9.11% done, estimate finish Tue Feb 10 14:52:00 2004
13.67% done, estimate finish Tue Feb 10 14:52:00 2004
...
95.67% done, estimate finish Tue Feb 10 14:52:05 2004
Total extents actually written = 109764
Total translation table size: 0
Total rockridge attributes bytes: 421
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 8000
109764 extents written (214 Mb)
$
```

10 Become the root user:

```
$ su - root
```

Provide the root password at the prompt.

11 Optionally verify the ISO9660 image:

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

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

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

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

**List contents of the ISO 9660 image**

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

**12** Determine the name of the DVD-RW device:

**`# cdrw -l`**

*All optical disk devices are printed.*

**Determine the DVD-RW device name**

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

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

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

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

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

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

**14** Record the image. This step requires approximately 10 minutes:

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

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

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

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

**CDRW command progress**

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

*Approximately nine minutes pass before the command completes.*

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

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

**15** Check that ISO 9660 image recorded correctly:

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

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

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

```
# eject cdrom
```

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

```
# umount /mnt
# lofiadm -d /dev/lofi/1
```

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

Exit from root privilege:

```
# exit
$
```

*The dollar sign command prompt returns.*

**17** Use the **rm** command to erase the image so the volume does not fill up:

```
$ rm /data/tmp/<IMG_TO_BACKUP>.img1020
$ rm /data/dvdimage.iso
```

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

**18** Remove the DVD-RW from the tray and close the tray. Label the DVD-RW.

**19** Store the DVD-RW per office procedure.

**20** This procedure is complete.

## 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 30, Perform TABAUDIT on page 66, and Restore call processing application files on page 55.

2 Verify the ONP start time. Either Nortel Networks and/or the operating company established this start time during the site preparation phase. To verify this time, refer to the software delivery site-ready reports or contact your next level of support. If requesting a change to the start time contact your Nortel Networks regional customer representative.

3 Verify front-end stability by ensuring the last REx test passed.

4 Take an office IMAGE and back it up. Refer to Dump call processing application image on page 77. 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.

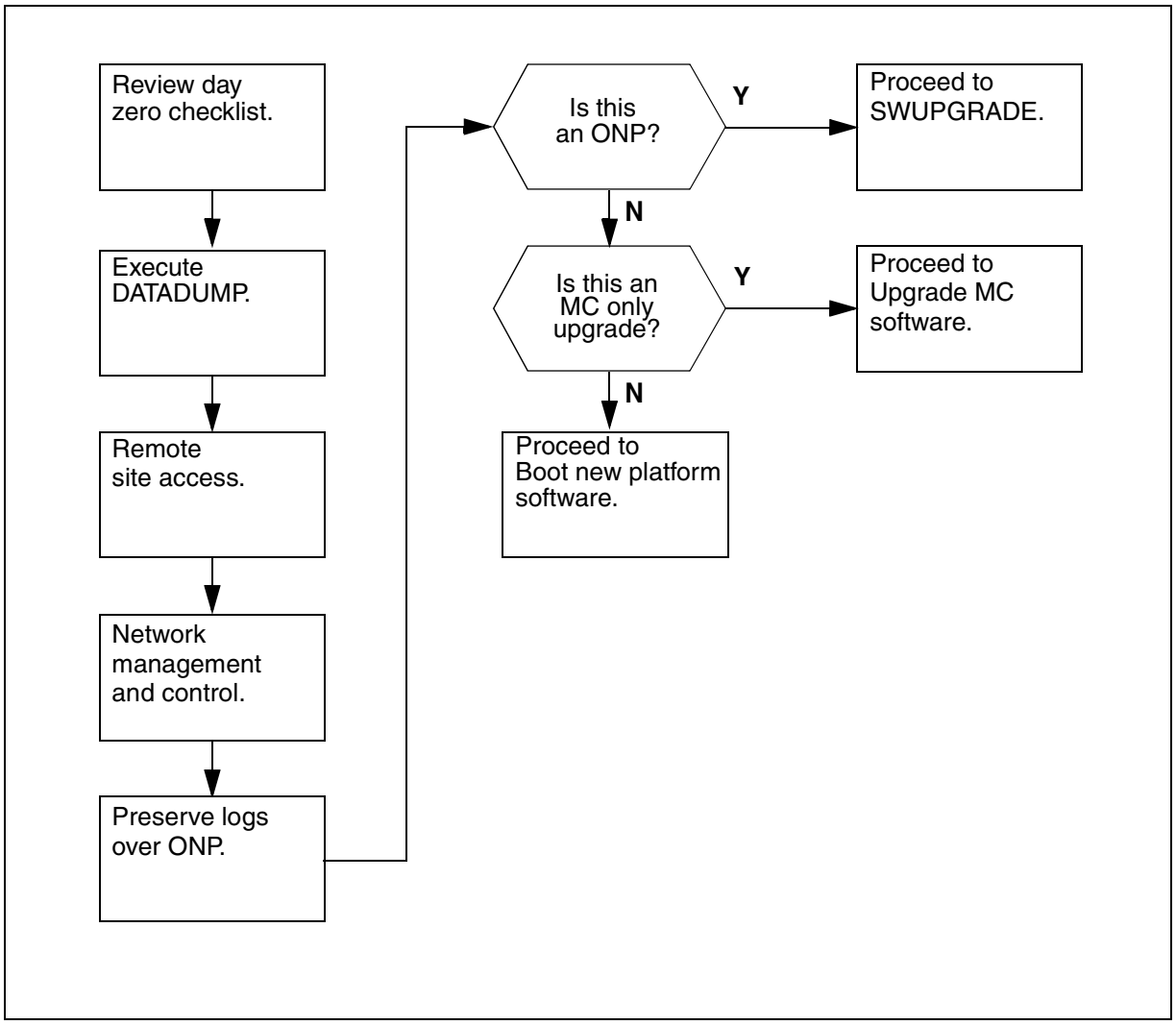
**11** Set up user interfaces and ensure they are available.

**12** This procedure is complete.

# 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**



# Execute DATADUMP

**ATTENTION**
Allow sufficient time to run the DATADUMP. Depending on the office, DATADUMP can require eight hours or more. Failure to allow sufficient time may impact the application start time.

***SITE — At the MAP***

**1** Record the datadump on disk or in the storefile device (SFDEV):

```
> RECORD START ONTO <device>
```

**device**
is a disk device such as SD00TEMP or is the storefile device, SFDEV

***Note:*** The name of the created file is RECORDFILE.

**2** Execute the DATADUMP:

```
> BCSUPDATE;DATADUMP
```

*Several confirmation prompts are presented. Confirm each prompt with "yes."*

```
Data Dump for CO: OFC_CLLI              Date: MAY 11, 2004  13:36:34
================================================================================
Do you want to display INB, MB and RES trunks?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display 1MR registers?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display INB lines?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display tables?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display hardware?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
```

*The datadump runs and completes.*

3 When the DATADUMP completes, quit to the CI level:

```
> QUIT ALL
```

4 Stop the recording:

```
>RECORD STOP ONTO <device>
```

5 This procedure is complete.

## Remote site access

At the established ONP start time, the telephone operating company is responsible for providing remote site access to the Nortel Networks Applicator. If not provided to Nortel Networks in advance, be prepared to furnish all the necessary information for this task.

***SITE***

**1** Ensure there will be uninterrupted communication with the Applicator during the ONP. Nortel Networks recommends using Foreign Exchange (FX) voice and data lines for this purpose.

- Two site connections — One connection is used for the active terminal (controlling the ONP procedure) and the second is used for tracing. If IOC or IOM equipment is available, Nortel Networks recommends that one site connection reside on one unit of the device, and the other connection on the second unit.
- One reliable voice number is required.

***Note 1:*** If these services are unavailable, contact Nortel Networks support personnel to determine if the available services are sufficient.

***Note 2:*** Foreign Exchange (FX) numbers are recommended for both voice and data lines for Applicator remote site access.

**2** Ensure two usernames and passwords with at least the following settings are provided for the ONP:

- COMCLASS — ALL
- PRIVCLASS — ALL
- STACKSIZE — 10000
- PRIORITY — 4

**3**

**DANGER**

**Prolonged software upgrade time**

Failure to provide working and reliable dialup access may cause problems during the software upgrade.

Failure to provide two dialups will jeopardize the software upgrade.

If the software delivery engineer loses contact with the office during SWACT, any datakits or defender modems will require more time accessing the switch, prolong office recovery times, and extend any potential service degradation. The operating company is responsible for providing all of the required information (pin #, passcodes, destinations, etc.) to the Applicator at the start of the ONP. The operating company is also responsible for ensuring that access is completely operational before starting the ONP.

## Network management control

**ATTENTION**
If necessary, contact your Network Maintenance support for assistance with these steps.

If Network Management code blocking is active before the ONP, the code blocking must be restored after the ONP is complete.

***SITE — At the MAP***

1 Make a list of all active code controls before the ONP to aid in restoration of code blocking.

```
> MASSCALL LIST CGAP ACODE ALL
```

2 Code blocking must be restored after the ONP. Make arrangements with Network Maintenance personnel for assistance.

3 This procedure is complete.

## Preserve logs over ONP

Logs that are suppressed or have a threshold set are configured for each site. Unless these logs are datafilled in table LOGCLASS, the settings will not be restored in the new call processing software load. Follow this procedure to determine which log reports are specially configured and how to provision table LOGCLASS.

***SITE — At the MAP***

**1** Determine which log reports are specially configured:

```
> LOGUTIL
> LISTREPS SPECIAL
> QUIT
```

**2** Determine if these log reports are already datafilled in table LOGCLASS:

```
> TABLE LOGCLASS
> LIS ALL (THRESHLD NE '0')
> LIS ALL (SUPPRESS NE 'N')
```

***Note:*** The field for threshold is spelled THRESHLD. The second command lists all tuples with a threshold that does not equal zero.

**3** If the output from step 2 does not equal the output from step 1, change as necessary to match the output from the LISTREPS output:

```
> RWOK ON
> POS <log_name>
> CHA <THRESHLD or SUPPRESS> <value or Y>
> YES
```

**log_name**
is the log report name such as TRKMEM listed in the LISTREPS output

**value**
is an integer value listed in the LISTREPS output

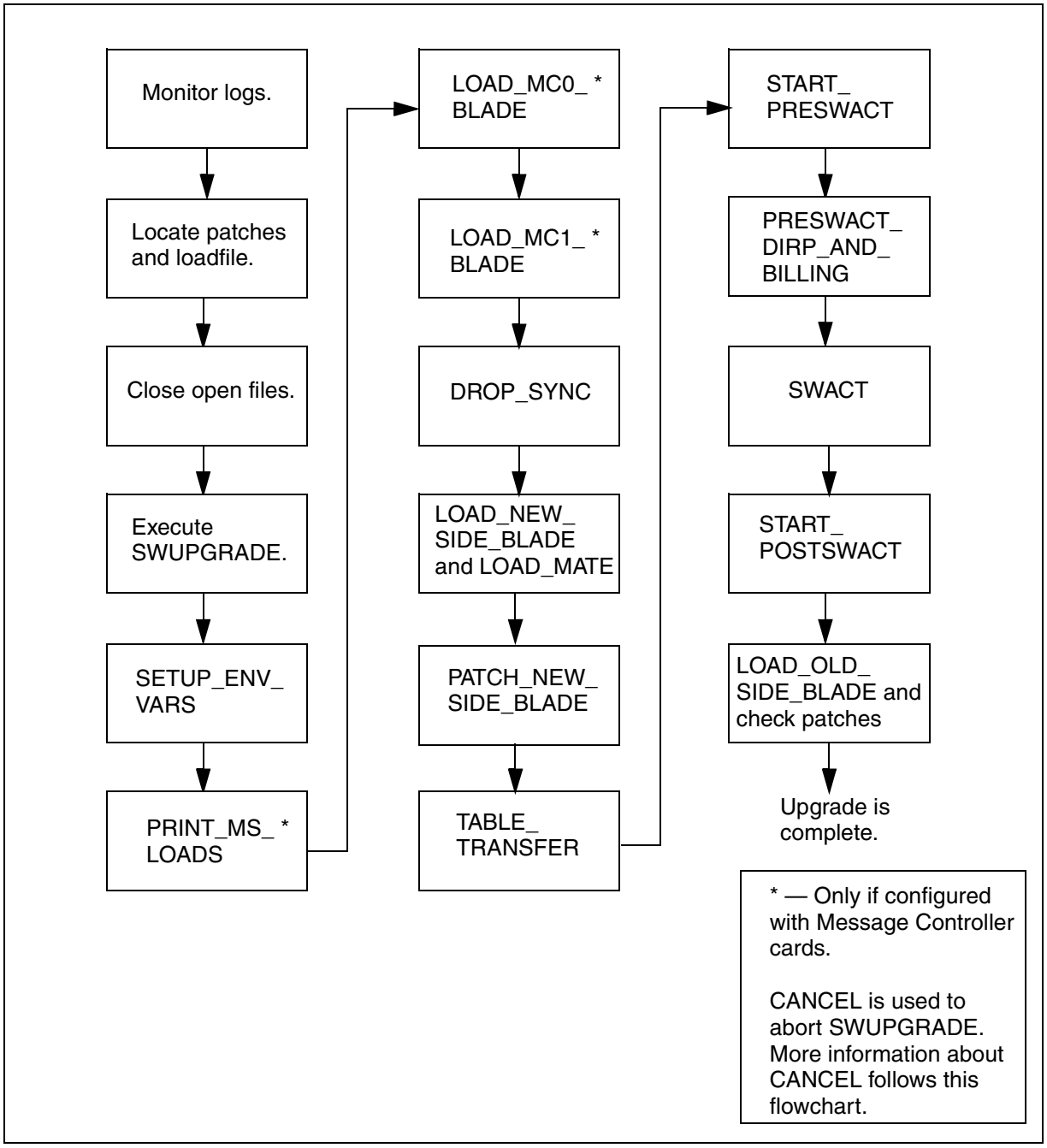
**4** Repeat step 3 for each required change and then exit the LOGUTIL level:

```
> QUIT
```

**5** This procedure is complete.

# SWUPGRADE

This section contains procedures that automate many of the upgrade tasks. Please read the important information following this flowchart.



Before proceeding with the procedures in this SWUPGRADE section of this document, complete the procedures in sections Interface setup on page 20, Site preparation phase on page 27, and Site responsibilities the day of the software delivery on page 87.

## 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 37.

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 55.

If the office is configured with Message Controller cards, then a Message Switch software image is required for the Message Switch. This software image is taken from DVD on the CS 2000 Management Tools server at the same time as the upgrade call processing application image. Once the Message Switch software is transferred, it is imported to one of the disk volumes. If the Message Switch software load is not available on one of the disk volumes, refer to Upgrade Peripheral Modules and Message Switch on page 33.

## 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.

## Monitor logs

***SDE — At the ACTIVECM window***

1 Check log reports to verify stability:

```
> BCSUPDATE; LOGCHECK
```

2 Investigate any log reports that indicate an office stability problem. If necessary, contact Nortel Networks support personnel for assistance.

3

**ATTENTION**

Do not continue if any log report indicates an office stability problem.

Quit the BCSUPDATE level:

```
> QUIT
```

4 This procedure is complete.

## Locate patches and loadfile

Call processing application patch files were loaded into the first device listed in table PADNDEV during the preparation phase. Use this procedure to verify the location of the patch files. The location is a required parameter during the SETUP_ENV_VARIABLES step of the software upgrade.

The call processing application image was retrieved from DVD, transferred, and stored during the preparation phase. Verify the location of the image.

### *SDE — At the ACTIVECM window*

1 Determine the default call processing application patch file location provisioned in table PADNDEV:

```
> TABLE PADNDEV; LIS ALL; QUIT
```

2 Make a note of the location. This value is a required parameter for the software upgrade.

3 Enter the disk utilities level and list the disk volumes:

```
> DISKUT; LV
```

4 List the contents of the volume with the upgrade call processing software image:

```
> LF <volume_name>
```

**volume_name**
is a string like SD00IMAGE

5 Make a note of the image file name. This value is a required parameter for environment variable LDMATE_IMAGE.

6 This procedure is complete.

If the CS 2000 - Compact is configured with Message Controller cards, check the Message Switch software loads and ensure that both Message Switches are running the same load and the load is specified in the *Peripheral Module Software Release Document*.

### *SDE — At the ACTIVECM window*

1 Remote login to Message Switch 0:

```
> REMLOGIN MS 0
```

*The terminal is now active on Message Switch 0.*

2 Issue the IMAGENAME command:

```
MS0> IMAGENAME
```

*The software load running in the Message Switch is displayed.*

```
MS-U BCS 55 CE built on 2004-APR-12 at 19:26:00
using mux20ce
LOAD: NIL.000
LAYER: BAS.21.0.CE
LAYER: TL.20.0.CE
```

3 Logout of the Message Switch:

```
MS0> REMLOGOUT
```

4 Ensure that the software load displayed (mux20ce in the example) is the correct Message Switch load for this release.

Use the REMLOGIN command to log into Message Switch 1, issue the IMAGENAME command, and REMLOGOUT. Ensure that the two Message Switches are running the same software load.

5

**CAUTION**

**Possible service interruption**

If the Message Switch is not loaded correctly, escalate immediately. Incorrect MS loads will cause subsequent AutoONP processes to fail and will jeopardize the software delivery application.

This procedure is complete.

## Close open files

Open files may have data in cache rather than written to storage. Follow this procedure to ensure that data is written to storage.

### *SDE — At the ACTIVECM window*

**1** Determine if there are any open files:

```
> DISKUT; LV
```

```
DISKUT:
Volumes found:
--------------
NAME                  TYPE      TOTAL       FREE TOTAL  OPEN
                              BLOCKS     BLOCKS FILES  FILES F
-------------------------------------------------------------
SD00IMAGE              STD    1638400     269821     4     0
SD00IMAGE1             STD    1638400     718476     3     0
SD00TEMP               STD     409600     409498     4     0
```

**2** For billing and Device Independent Recording Package (DIRP) files, rotate the volumes:

```
> MAPCI;MTC;IOD;DIRP
> ROTATE <subsystem>
> QUIT ALL
```

**subsystem**
is a billing or DIRP subsystem such as AMA

**3** For regular files, determine the name of the open file and close the file:

```
> LF <volume_name>
> FILECLOSE <file_name> <volume_name>
```

**volume_name**
is the name of the volume with open files from step 1

**file_name**
is the name of the file to close returned by the LF command

**4** For assistance with closing open files, contact Nortel Networks support personnel.

**5** This procedure is complete.

# Execute SWUPGRADE

The Automated One Night Process (AutoONP) maintains a list of steps to execute. When a step fails or requires user input, the process stops, the user responds to the problem and types **GO** to continue until all steps are executed.

Help for the SWUPGRADE level commands is available by typing **HELP** while in the SWUPGRADE level.

Step DOWNLOAD_FILES reminds the Software Delivery Engineer to retrieve the bulletins file. If the bulletins file is not available in SFDEV, the software upgrade will fail.

The number of steps in the AutoONP process is determined by the CS 2000 - Compact configuration. If the CS 2000 - Compact is configured with Message Controller cards, there are more steps.

**SWUPGRADE CA steps**

| without Message Controllers | with Message Controllers |
|---|---|
| SETUP_ENV_VARS | SETUP_ENV_VARS |
| NOTIFY_USERS | NOTIFY_USERS |
| SET_LOGIN_BANNER | SET_LOGIN_BANNER |
| DOWNLOAD_FILES | DOWNLOAD_FILES |
| READ_BULLETINS | READ_BULLETINS |
| VERIFY_DEVICES | VERIFY_DEVICES |
| PRINT_PARMS_AND_SAVE | PRINT_PARMS_AND_SAVE |
| CHECK_LOGS_1 | CHECK_LOGS_1 |
| STOP_JOURNAL_FILE | STOP_JOURNAL_FILE |
| | PRINT_MS_LOADS |
| DISABLE_PRSM_AUDIT_ACT | DISABLE_PRSM_AUDIT_ACT |
| | LOAD_MC0_BLADE |
| | LOAD_MC1_BLADE |

**SWUPGRADE CA steps**

| without Message Controllers | with Message Controllers |
|---|---|
| DROP_SYNC | DROP_SYNC |
| LOAD_NEW_SIDE_BLADE | LOAD_NEW_SIDE_BLADE |
| LOAD_MATE | LOAD_MATE |
| PATCH_NEW_SIDE_BLADE | PATCH_NEW_SIDE_BLADE |
| MATELINK_RTS | MATELINK_RTS |
| UPDATE_STEPS_AND_VARS | UPDATE_STEPS_AND_VARS |
| CHECK_NEW_LOAD | CHECK_NEW_LOAD |
| SET_DATE_AND_LOGMSG | SET_DATE_AND_LOGMSG |
| CHECK_LOGS_2 | CHECK_LOGS_2 |
| CLEAR_TRAPINFO | CLEAR_TRAPINFO |
| TRANSFER_DEVICES_INFO | TRANSFER_DEVICES_INFO |
| TRANSFER_PARM_VALUES | TRANSFER_PARM_VALUES |
| | MS_CHECK |
| DISABLE_AUTOIMAGE | DISABLE_AUTOIMAGE |
| SET_OFFICE_TUPLES | SET_OFFICE_TUPLES |
| SET_PADNDEV | SET_PADNDEV |
| SEND_PATCHES | SEND_PATCHES |
| APPLY_PATCHES | APPLY_PATCHES |
| CHECK_LOGS_3 | CHECK_LOGS_3 |
| RESTORE_PADNDEV | RESTORE_PADNDEV |
| TABLE_TRANSFER | TABLE_TRANSFER |
| TABXFR_REPORT | TABXFR_REPORT |
| CHECK_LOGS_4 | CHECK_LOGS_4 |
| START_PRESWACT | START_PRESWACT |

**SWUPGRADE CA steps**

| without Message Controllers | with Message Controllers |
|---|---|
| PRESWACT_DIRP_AND_BILLING | PRESWACT_DIRP_AND_BILLING |
| PRINT_SPMS_INDICES | PRINT_SPMS_INDICES |
| GET_FIRST_SWACT_AGREEMENT | GET_FIRST_SWACT_AGREEMENT |
| PREPARE_FOR_SWACT | PREPARE_FOR_SWACT |
| STATUSCHECK | STATUSCHECK |
| CHECK_LOGS_5 | CHECK_LOGS_5 |
| TRANSFER_TIMINGS | TRANSFER_TIMINGS |
| SWACT | SWACT |
| DISPLAY_DATE | DISPLAY_DATE |
| RECOVER_DIRP_AND_BILLING | RECOVER_DIRP_AND_BILLING |
| PERFORM_TEST_CALLS_1 | PERFORM_TEST_CALLS_1 |
| START_POSTSWACT | START_POSTSWACT |
| RESTART_OLD_LOAD | RESTART_OLD_LOAD |
| DRTIME_PRINT | DRTIME_PRINT |
| PERFORM_TEST_CALLS_2 | PERFORM_TEST_CALLS_2 |
| LOAD_OLD_SIDE_BLADE | LOAD_OLD_SIDE_BLADE |
| SYNC_SWITCH | SYNC_SWITCH |
| FINISH_POSTSWACT | FINISH_POSTSWACT |
| RESTORE_PARMS | RESTORE_PARMS |
| RESET_DEVICES | RESET_DEVICES |
| COMPLETE_NEW_LOAD_INIT | COMPLETE_NEW_LOAD_INIT |
| RESET_LOGIN_BANNER | RESET_LOGIN_BANNER |
| DUMP_NEW_LOAD | DUMP_NEW_LOAD |

**SWUPGRADE CA steps**

| without Message Controllers | with Message Controllers |
|---|---|
| RESUME_REX_TEST | RESUME_REX_TEST |
| START_JOURNAL_FILE | START_JOURNAL_FILE |
| PRINT_SWUPGRADE_REPORT | PRINT_SWUPGRADE_REPORT |
| STOP_RECORD | STOP_RECORD |
| UPGRADE_COMPLETE | UPGRADE_COMPLETE |

***SDE — At the ACTIVECM window***

1 Enter the software upgrade level:

```
> SWUPGRADE CA
```

2 Press return twice to display the current office header message. Note the office header message for environment variable INACT_LOGMSG.

3 Begin the upgrade:

```
> START
```

4 Proceed to SETUP_ENV_VARS.

## Additional information

### How to insert, delete, or modify steps

To allow customization of the AutoONP, SWUPGRADE allows the user to change the steps that are normally performed. Commands are available to insert, delete, or otherwise modify the AutoONP steps.

Use the **INSERT** command to add a new step or copy an existing step into another location in the step list. The step list is printed with command **DISP STEPS**. **REMOVE** removes any step or pause that was added. **OVERRIDE** disables the execution of a step. **PAUSE** is used to halt the AutoONP process before or after a step until **RESUME** is entered.

### Use of the BULLETINS file

The BULLETINS file is maintained by Nortel Networks Global Software Delivery and is used to provide as much automation as possible when performing the application bulletins and workarounds. Since application bulletins and workarounds will vary depending on the "from and to" software loads, it is recommended that the BULLETINS file and all bulletins and workarounds be reviewed before starting the AutoONP.

When required, bulletins and workarounds should be followed and manually executed during the AutoONP.

**ATTENTION**

The BULLETINS file is a critical file that must be located in SFDEV for execution during the AutoONP.

If this file is missing from SFDEV or if it is named incorrectly, the AutoONP will fail. For assistance with the BULLETINS file contact the Global Software Delivery hotline for your market.

Step DOWNLOAD_FILES, towards the beginning of the AutoONP process, will remind the user to download the BULLETINS file (along with other required files). If desired, print a hard copy of the BULLETINS file and review the file contents.

Step READ_BULLETINS will read (that is, execute) the BULLETINS file during the AutoONP.

### Using the CANCEL command

The CANCEL command is used to terminate or abort the software upgrade and halt the execution of the SWUPGRADE process at any time during the AutoONP. This command reverts all SWUPGRADE steps and returns the switch to its original state.

### Getting help on AutoONP steps

The SWUPGRADE increment is used to perform the AutoONP. At any time within this increment you may type HELP for a list of the commands available. Also, the HELP command has options to obtain information about a command syntax, specific step, or variable.

**HELP** displays a brief description of the SWUPGRADE increment and a list of the available CI commands. **HELP <swupgrade command>** displays a brief description and syntax of the command. **HELP STEP <step>** displays a brief description of a step's functionality. **HELP VAR <variable>** displays a brief description and the current value of the variable.

For additional information about SWUPGRADE commands, refer to section "SWUPGRADE summary" of Appendix A in *Software Delivery One Night Process Software Delivery Procedures*, 297-8991-303.

## SETUP_ENV_VARS

***SDE — At the ACTIVECM window***

**1** Set variable TRACE_USER to ME:

**TRACE_USER (no default)**
Holds the USER name on whose console output messages are printed. Changing the value of this variable changes the value of the TRACE_DEVICE variable, and causes the output to be redirected to the new USER device.

Value: <user name> or ME - a user name, such as ADMIN, or ME which indicates the current user

***Note:*** For clarity purposes, it is recommended to set this variable to a user other than the current user.

The USER must be LOGGED IN when this variable is set. The current setting is: <none>

```
> ME
```

**2** Do not change the TRACE_DEVICE variable. Press the Enter key.

**TRACE_DEVICE**
Holds the device name on which output messages are printed. Changing the value of this variable causes the output to be redirected to the new device.

Value: <trace device name> - a string, such as MAP

***Note:*** For clarity purposes, it is recommended to set this variable to a device other than the currently logged on terminal.

The current setting is: <none>

*The selected device indicates "This device is selected for TRACing."*

**3** Do not change the PRINTER variable. Press the Enter key.

**PRINTER**
Holds the name of the printer on which output messages are recorded. The printer echoes all output sent to the trace device. Changing the value of this variable causes the recording to be directed to the new device.

Value: <printer name> or SINK where <printer name> is a device datafilled in table TERMDEV. Choosing SINK means choosing no printer output.

```
> SINK
```

4 Do not change the LOGS variable. Press the Enter key.

**LOGS**
Holds the names of the logs that are checked by the LOGS step. More than one log can be specified by entering log names separated by a blank.

**Example**
'SWERR TRAP' — Check traps and swerrs. Display a message if traps or swerrs are recorded.

The current setting is: TRAP SWERR

5 Enter the INACT_LOGMSG variable. Use the existing office header *except* update the new job order number, software level, and current date.

**INACT_LOGMSG**
Holds the log message that will be displayed on the inactive side of the switch.

**Example**
*** H1234 Office_Name SN000006 17/AUG/2003 ***

6 Enter the LDMATE_IMAGE variable:

**LDMATE_IMAGE**
Holds the volume name and filename used to load the inactive unit.

**Example**
SD00IMAGE0 CSN0007BG

***Note:*** The software checks to verify that a file with the specified name exists on the volume.

7 Enter the PADNDEVS variable. The default value is SFDEV. If the call processing application files were loaded into SFDEV, press the Enter key. Otherwise, enter up to three device names if the patches were loaded into a location other than SFDEV during procedure Transfer call processing application patch files.

8 Do not change the TABXFR_STOPIF variable. Press the Enter key.

**TABXFR_STOPIF**
Determines the threshold for the maximum number of failed tables allowed before halting TABXFR.

**9** Do not change the TABXFR_LIMIT variable. Press the Enter key.

**TABXFR_LIMIT**
Determines the threshold for the maximum number of tuple failures allowed before halting TABXFR.

**10** Do not change the TABXFR_INITIAL_PRINT variable. Press the Enter key.

**TABXFR_INITIAL_PRINT**
Determines the time interval for printing a single message containing the current table name.

**11** Set the TABXFR_INTERVAL_PRINT variable to 30 seconds:

**TABXFR_INTERVAL_PRINT**
Determines the time interval for printing regular table transfer status messages. This is particularly useful for large tables.

```
> 30 SECS
```

**12** Do not change the SPMS_OPTION variable. Press the Enter key.

**SPMS_OPTION**
Holds the date, or number of days, to generate the SPMS (Switch Performance Monitoring System) indices.

**13** Do not change the DRTIME_REPORT variable. Press the Enter key.

**DRTIME_REPORT**
Determines if the DRTIME report should be printed before SYNC. DRTIME provides statistics on the TABXFR process. Normally this information is not used unless this information is requested.

**14** Set the DUMP_NEW_LOAD variable:

**DUMP_NEW_LOAD**
Determines if an image dump of the new load should be taken.

```
> NO
```

***Note:*** If the value of this variable is set to NO, the Site is responsible for manually taking an image of the new software load immediately after the AutoONP is complete.

*The variables are printed to the terminal.*

```
WARNING: An ACTIVE VOLUME must be datafilled in table
         IMAGEDEV to use AUTODUMP.

SWUPGRADE variables for target CA:

Variable Name                                    Value
-------------------------------------------------------------------------
TRACE_USER                          =   USERNAME
TRACE_DEVICE                        =   TELNSVR00018
PRINTER                             =   SINK
LOGS                                =   TRAP SWERR
INACT_LOGMSG                        =   INACT_LOGIN_MESSAGE
LDMATE_IMAGE                        =   SD00IMAGE0 CSN0007BG
PADNDEVS                            =   SFDEV
TABXFR_STOPIF                       =   1
TABXFR_LIMIT                        =   25
TABXFR_INITIAL_PRINT                =   30 SECS
TABXFR_INTERVAL_PRINT               =   30 SECS
SPMS_OPTION                         =   NONE
DRTIME_REPORT                       =   NO
DUMP_NEW_LOAD                       =   NO
```

**15** Type **GO** and press the Enter key to proceed with the upgrade. Monitor messages on the TRACE_DEVICE.

*Step NOTIFY_USERS is automatically run. The notified usernames and environment variables are printed to the terminal.*

*Step SET_LOGIN_BANNER is automatically run.*

*Step DOWNLOAD_FILES begins, reminds the SDE to download optional application and BULLETINS file and then waits for the SDE to type GO.*

**16** After downloading any required files, type **GO** and press the Enter key.

**17** If a BULLETINS files is located in SFDEV, it is read and executed during step READ_BULLETINS.

If a BULLETINS file is not found in SFDEV, the step fails. If a BULLETINS file is not needed, type **OVERRIDE READ_BULLETINS**, press the Enter key, and confirm the override.

Type **GO** and press the Enter key to continue.

*The following steps are automatically run:*

- *VERIFY_DEVICES*
- *PRINT_PARMS_AND_SAVE*
- *CHECK_LOGS1*

  ***Note:** Display the contents of all logs listed. Use the **DISPLAY LOG <log_name> ALL <ACT or INACT>** command.*

- *STOP_JOURNAL_FILE*

*If the CS 2000 - Compact is equipped with Message Controller cards, step PRINT_MS_LOADS runs. Otherwise, step DISABLE_PRSM_AUDIT_ACT runs.*

***Note:** Step DISABLE_PRSM_AUDIT_ACT has several substeps.*

## Additional information

If any variables require correction, use the **SET** command to change the variable. If the variable consists of two or more words such as SD00PATCH and SD01PATCH, use quotation marks to enclose the words.

**Example**
SET PADNDEVS ‘SFDEV SD00PATCH SD01PATCH’

Variables can be displayed at any time with the **DISP VAR** command.

**Example**
DISP VAR PADNDEVS

# PRINT_MS_LOADS

**ATTENTION**
This step only runs if the CS 2000 - Compact is configured with Message Controller cards.

***SDE — At the ACTIVECM window***

**1** Step PRINT_MS_LOADS runs.

```
Starting step PRINT_MS_LOADS.
Please note that the displayed information corresponds
to the BASE layer of the MS load.
Load in MS 0 = MS-U21BC
Load in MS 1 = MS-U21BC

Please check the above MS loads for correctness.
Step PRINT_MS_LOADS is complete.

The SWUPGRADE process has paused. Enter GO.
```

***Note:*** MS-U21xx is the correct value for upgrading to SN07.

**2** If the value reported is not correct, do not proceed. Contact Nortel Networks support personnel immediately.

**3** Type **GO** and press the Enter key.

*Step PRINT_MS_LOADS completes.*

*Step DISABLE_PRSM_AUDIT_ACT runs and completes.*

# LOAD_MC0_BLADE

**ATTENTION**
This step only runs if the CS 2000 - Compact is configured with Message Controller cards.

***SDE — At the ACTIVECM window***

**1** Step LOAD_MC0_BLADE runs.

```
Starting step LOAD_MC0_BLADE.
Upgrade load of MC  0 at the SAM21 EM GUI
by using the following manual procedure:
  1) At the MAPCI;MTC;MS map level, verify that MS 1 is the
     master MS.
  2) If MS 1 is not the master, perform a SWMAST. If
     performed, soak 10 minutes.
  3) At SAM21 EM GUI, open Card View for MC 0
    a) Under Provisioning Tab, determine IP address of
       the card.
    b) Ensure IP address in GUI matches IP address of MC 0.
  4) Under the States Tab, Lock the card.
    a) Wait for the lock icon to appear.
  5) Under the Provisioning Tab, change the boot file:
    a) Click Modify.
    b) Change boot file name to new load.
    c) Click Save.
  6) Under the States Tab, Unlock the card
    a) Wait for the lock icon to disappear.
  7) At Active CCAMTC MAP; MC level, Validate newly booted
     load.
    a) QryLd command for MC0 must indicate new MC load
       version.
  8) Soak for 10 minutes, monitoring logs.

Type GO to continue SWUPGRADE when above steps are
successfully completed.

Step LOAD_MC0_BLADE is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2** At the MAPCI;MTC;MS level, ensure that MS 1 is the master MS.

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

 MS                Message Switch   Clock   Shelf  0       Inter-MS Link 0 1
  0 Quit       MS 0        .          Slave          F                    . .
  2            MS 1        .          M Free         F                    . .
  3
  4
  5
  6 Tst_
  7 Bsy_
  8 RTS_
  9
 10 LoadMS_
```

**3** If MS 1 is not the master MS, perform a **SWMAST**. If SWMAST is performed, then soak 10 minutes before continuing.

***At the active Call Agent Manager interface (CORE0 or CORE1)***

**4** At the MCMtc level, verify that both Message Controllers are in service (.) prior to Locking Message Controller 0 in the next step.

```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
     .             .         .         .          .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit       MC0    .       . Act      . Inact    open       open
 2            MC1    .       . Act      . Inact    open       open
 3
```

**5** Exit the Call Agent Manager interface and determine the IP address of Message Controller 0:

```
>0 ALL
[mtc@hostname mtc]$ grep mc0 /etc/hosts
```

*The grep command returns the address of Message Controller 0.*

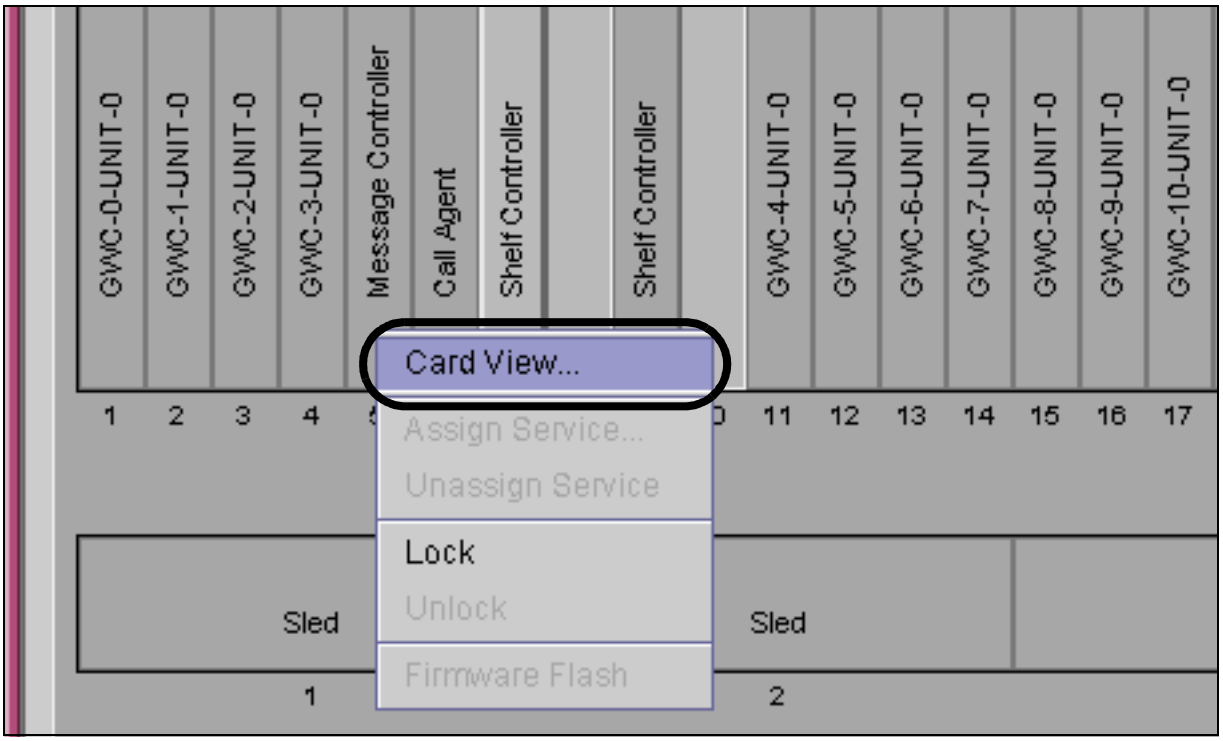
```
10.40.54.60 mc0
```

**6** Start the Call Agent Manager interface again:

```
[mtc@hostname mtc]$ ccamtc mcmtc
```

***At the CS 2000 SAM21 Manager client***

**7** From the Shelf View, right click on the card and select Card View.



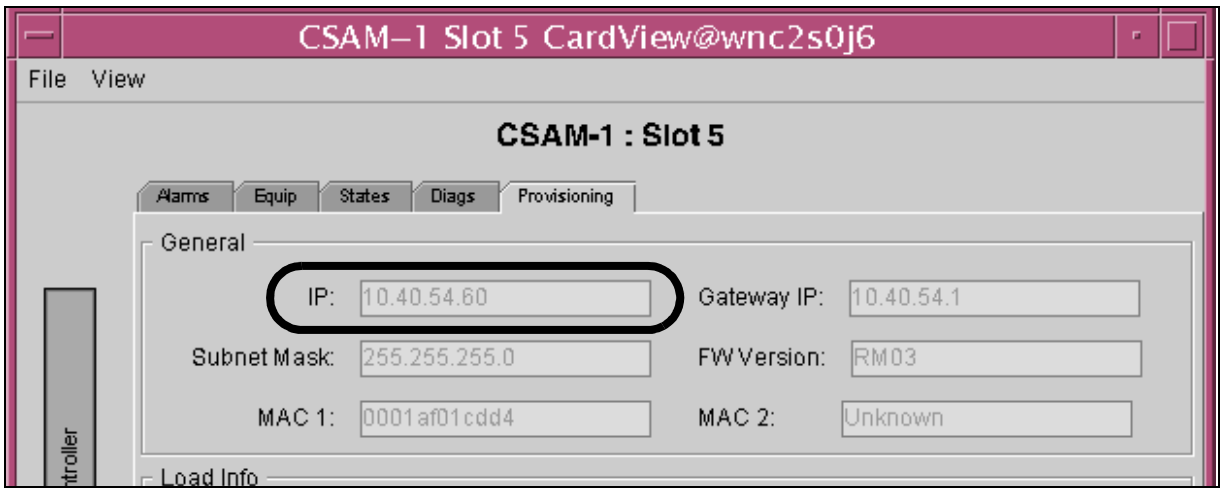

***Note:*** The Shelf View window will reflect office provisioning and the hardware configuration of the SAM21 shelf.

*The Card View window opens.*

**8** Select the Provisioning tab on the Card View window.

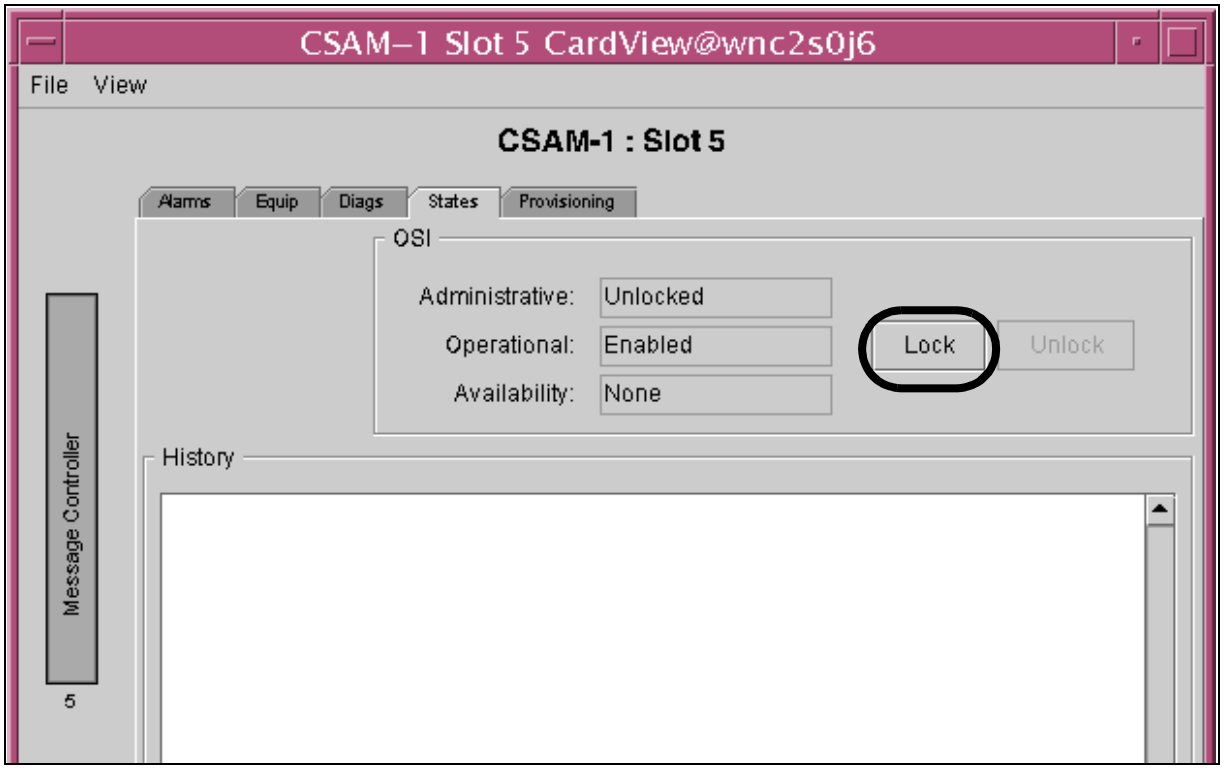
Ensure that the IP address specified in the IP field matches the IP address of Message Controller 0 from step 5. If the values do not match, open the other Shelf View from the CS 2000 SAM21

Manager and check the Message Controller provisioning for that shelf.



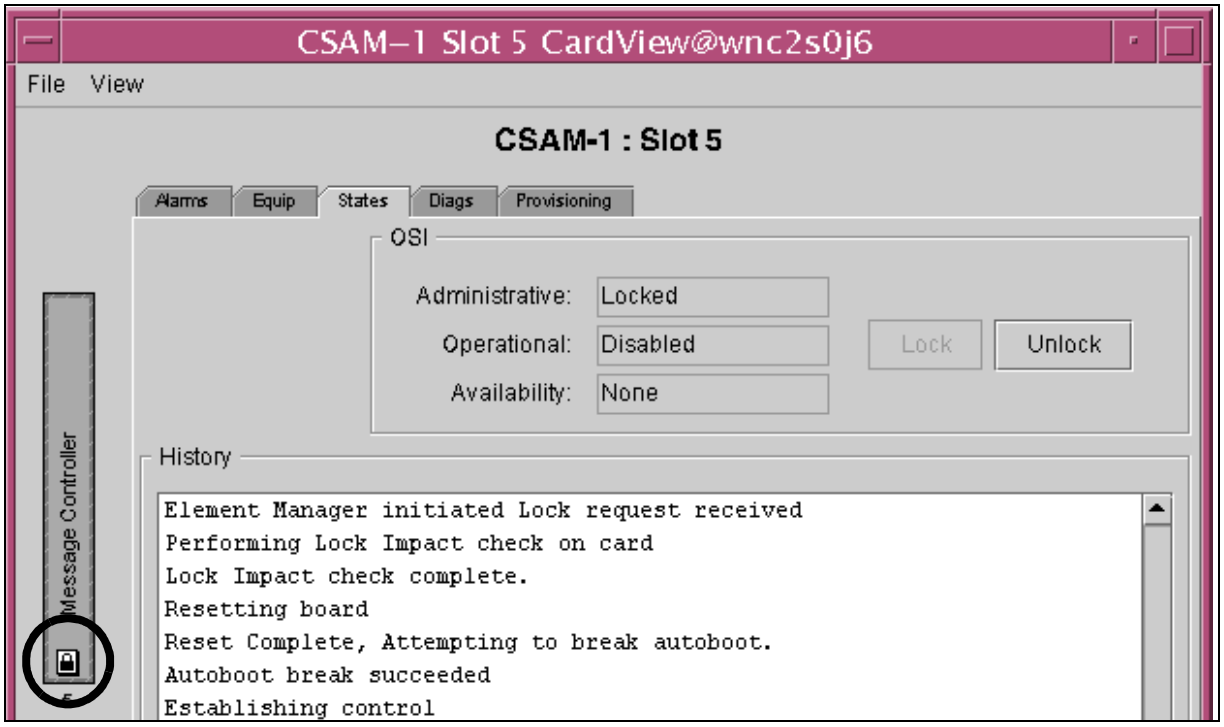

**9** Click on the States tab.

Click on the Lock button.



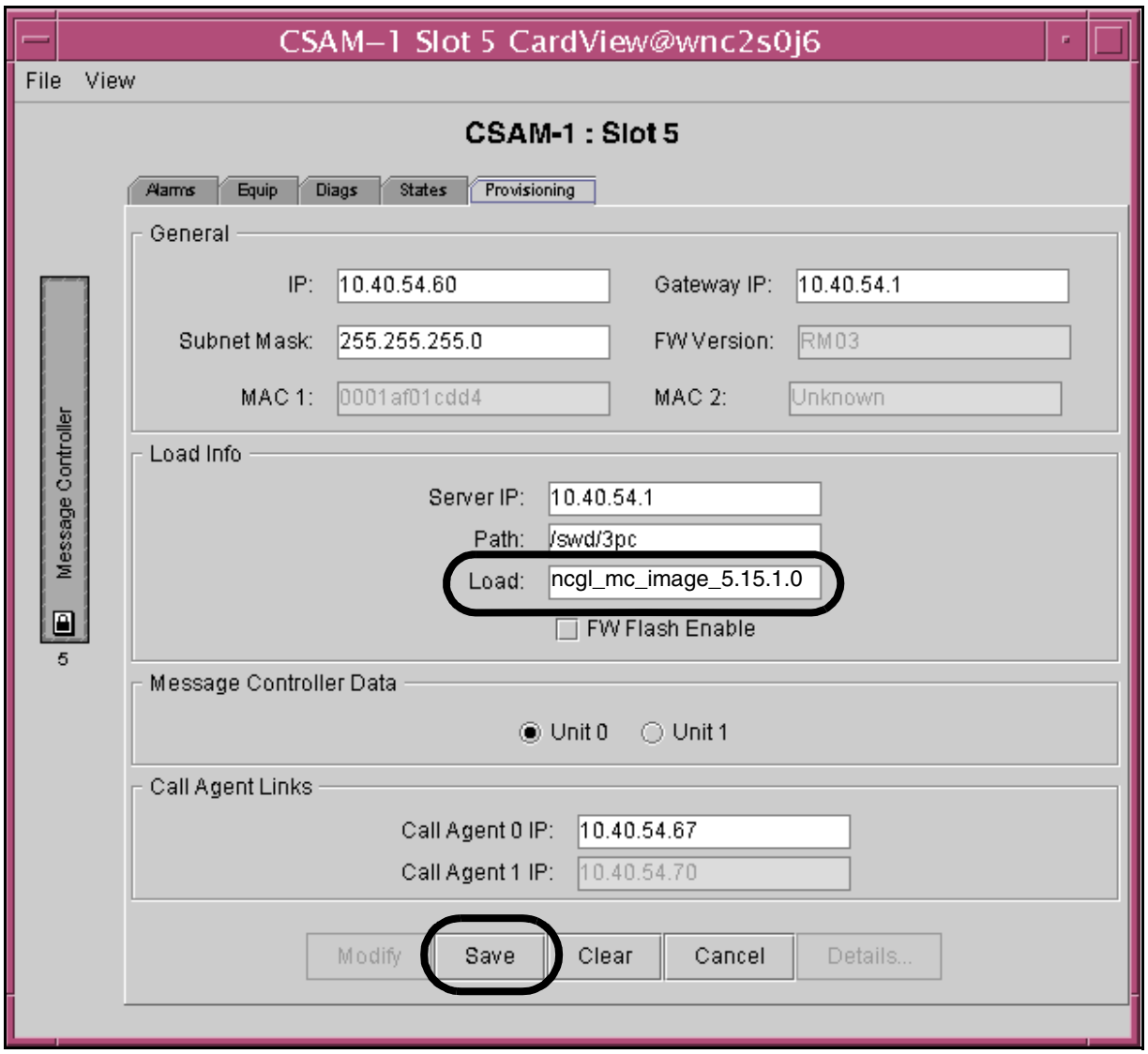

*A lock warning dialog window opens. Confirm the lock warning.*

**10** Wait for the lock icon to appear on the card icon.




*At the Call Agent Manager, a major ATM alarm is raised. The Message Controller enters the Remote Busy (R) state and is reported as out of service.*

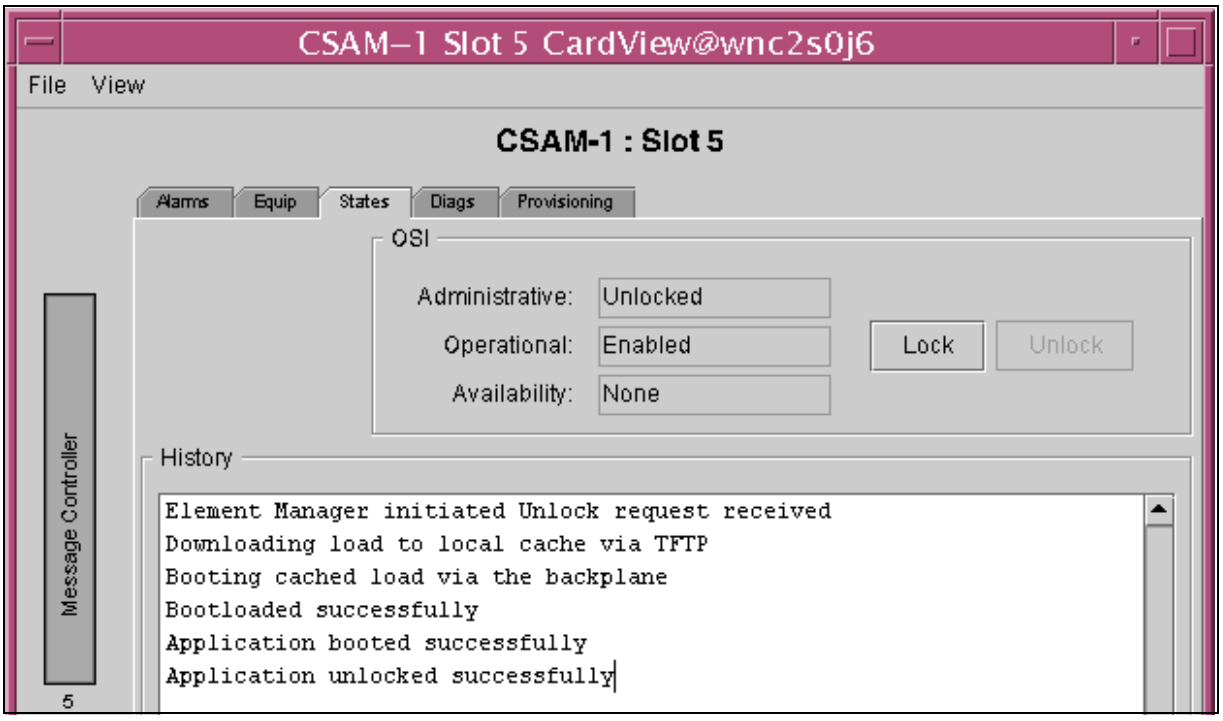
**11** Click on the Provisioning tab, change the Load value to the new software load name, and click Save.




*A warning dialog is generated indicating a load mismatch between the provisioning for the two Message Controller cards. Confirm the warning dialog by clicking OK.*

**12** Click on the States tab and click the Unlock button.

Wait for the lock icon to disappear.




*At the Call Agent Manager, the card enters the in service state (.), and the major ATM alarm clears. The Message Controller may raise a major MCTbl alarm while the Message Controller synchronizes to the NTP server.*

***At the active Call Agent Manager interface (CORE0 or CORE1)***

**13** Query the software load for Message Controller 0 and ensure that the new load is reported:

```
> MCMtc
> QryLd 0
```

```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
    .             .         .         .          .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit      MC0    .       . Act      . Inact    open       open
 2           MC1    .       . Act      . Inact    open       open
 3
 4
 5 QryLd
 6 QryHits
 7 ClrHits
 8 Trnsl
 9
10
11
12
13 LogQuery
14 Alarm
15
16           MC Load report retrieved on Thu Jun 19 13:48:45 2004:
17 Help
18 Refresh         Ramdisk ncgl_mc_image_5.15.1.0
  mtc
Time  13:48  >
```

*Soak the load for 10 minutes while monitoring log reports.*

***SDE — At the ACTIVECM window***

**14** Type **GO** and press the Enter key to continue.

# LOAD_MC1_BLADE

**ATTENTION**
This step only runs if the CS 2000 - Compact is configured with Message Controller cards.

***SDE — At the ACTIVECM window***

**1** Step LOAD_MC1_BLADE runs.

```
Starting step LOAD_MC1_BLADE.
Upgrade load of MC 1 at the SAM21 EM GUI
by using the following manual procedure:
  1) At the MAPCI;MTC;MS map level, verify that MS 0 is the
     master MS.
  2) If MS 0 is not the master, perform a SWMAST. If
     performed, soak 10 minutes.
  3) At SAM21 EM GUI, open Card View for MC 1
    a) Under Provisioning Tab, determine IP address of
       the card.
    b) Ensure IP address in GUI matches IP address of MC 1.
  4) Under the States Tab, Lock the card.
    a) Wait for the lock icon to appear.
  5) Under the Provisioning Tab, change the boot file:
    a) Click Modify.
    b) Change boot file name to new load.
    c) Click Save.
  6) Under the States Tab, Unlock the card
    a) Wait for the lock icon to disappear.
  7) At Active CCAMTC MAP; MC level, Validate newly booted
     load.
    a) QryLd command for MC 1 must indicate new MC load
       version.
  8) Soak for 10 minutes, monitoring logs.

Type GO to continue SWUPGRADE when above steps are
successfully completed.

Step LOAD_MC1_BLADE is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2** At the MAPCI;MTC;MS level, ensure that MS 0 is the master MS.

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

 MS                  Message Switch   Clock   Shelf  0       Inter-MS Link 0 1
  0 Quit       MS 0        .          M Free          F                    . .
  2            MS 1        .          Slave           F                    . .
  3
  4
  5
  6 Tst_
  7 Bsy_
  8 RTS_
  9
 10 LoadMS_
```

**3** If MS 1 is not the master MS, perform a **SWMAST**. If SWMAST is performed, then soak 10 minutes before continuing.

***At the active Call Agent Manager interface (CORE0 or CORE1)***

**4** At the MCMtc level, verify that both Message Controllers are in service (.) prior to Locking Message Controller 1 in the next step.

```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
     .             .         .         .         .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit       MC0    .      . Act      . Inact    open       open
 2            MC1    .      . Act      . Inact    open       open
 3
```

**5** Exit the Call Agent Manager interface and determine the IP address of Message Controller 0:

```
>0 ALL
[mtc@hostname mtc]$ grep mc1 /etc/hosts
```

*The grep command returns the address of Message Controller 1.*

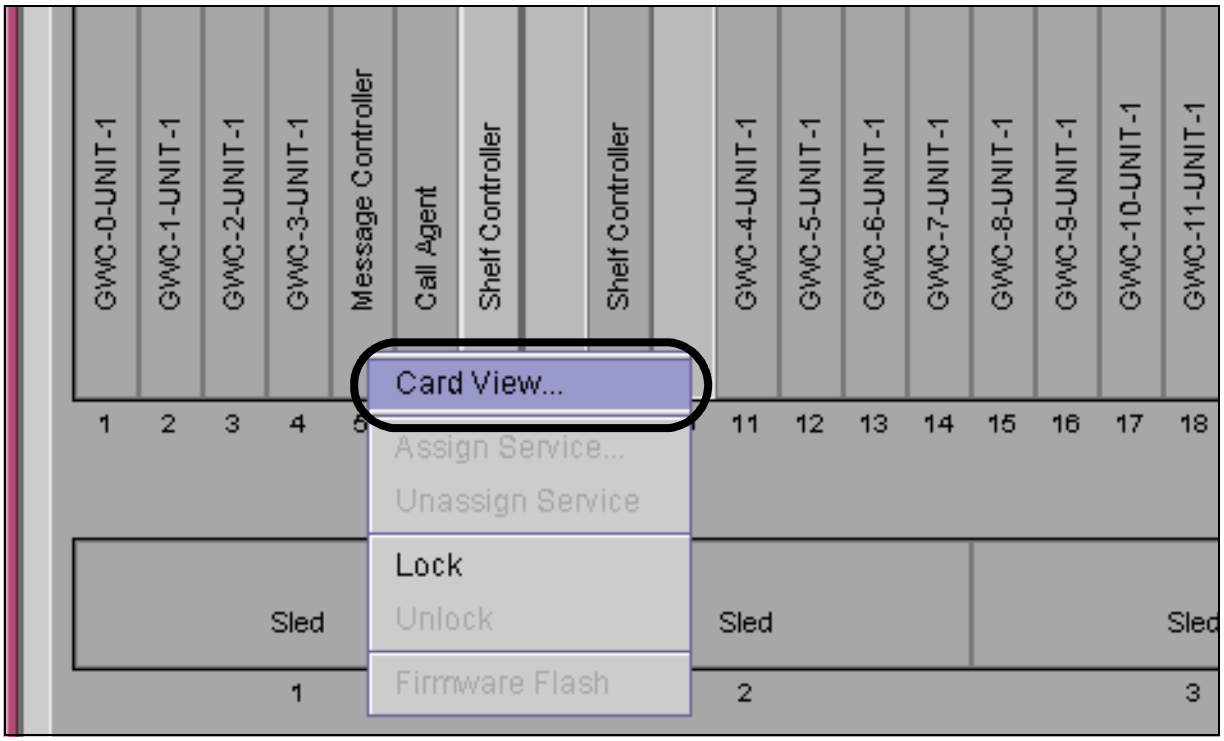
```
10.40.54.61 mc1
```

**6** Start the Call Agent Manager interface again:

```
[mtc@hostname mtc]$ ccamtc mcmtc
```

***At the CS 2000 SAM21 Manager client***

**7** From the Shelf View, right click on the card and select Card View.

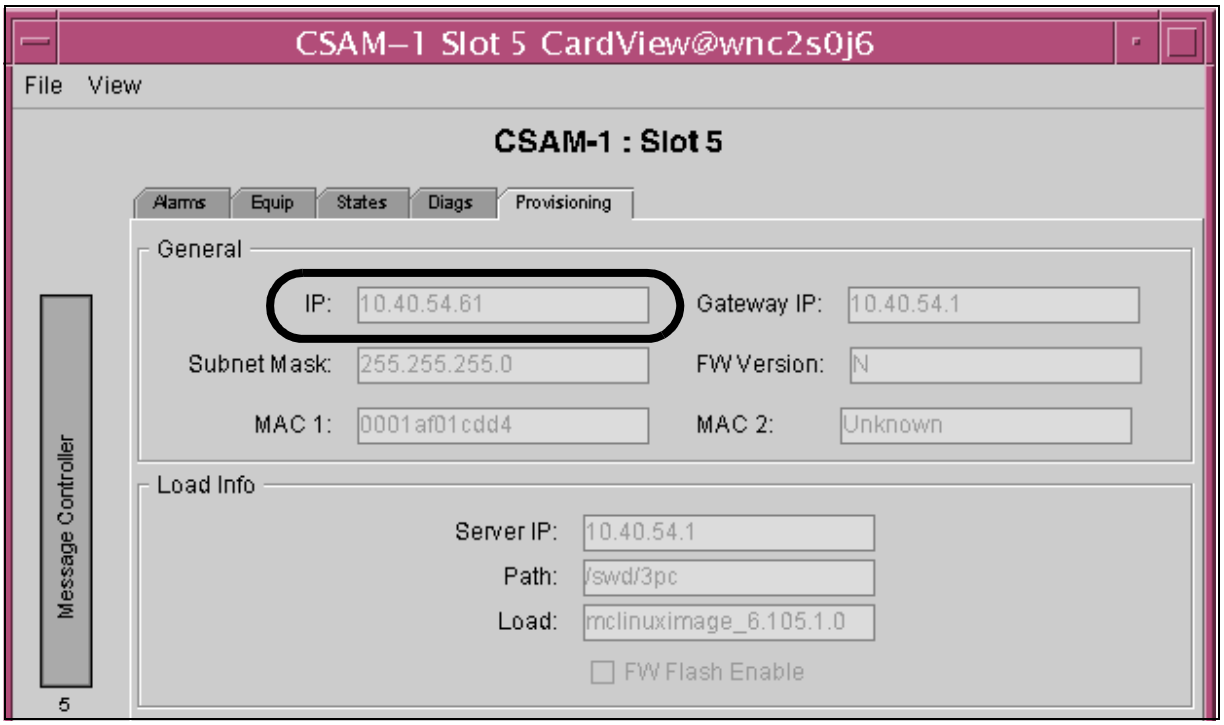



***Note:*** Message Controller 1 is located in slot 12 for some markets.

*The Card View window opens.*

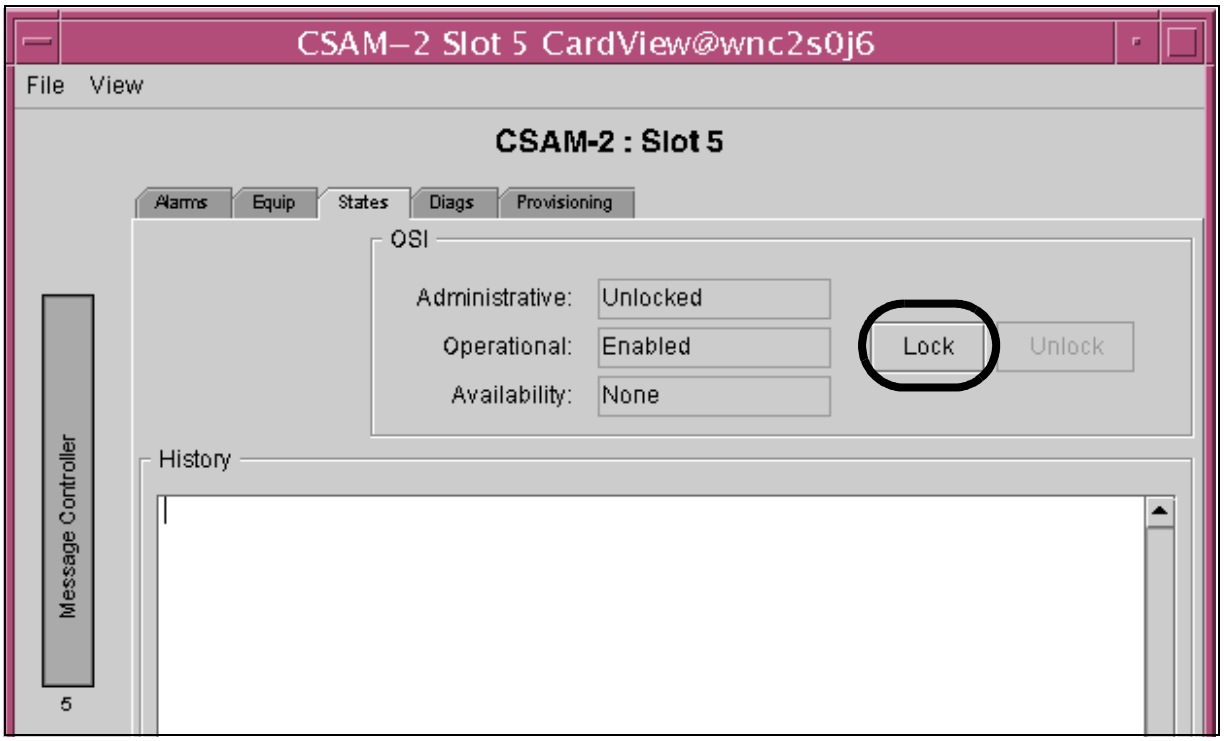
**8** Select the Provisioning tab on the Card View window.

Ensure that the IP address specified in the IP field matches the IP address of Message Controller 1. If the values do not match, open the other Shelf View from the CS 2000 SAM21 Manager and check the Message Controller provisioning for that shelf.



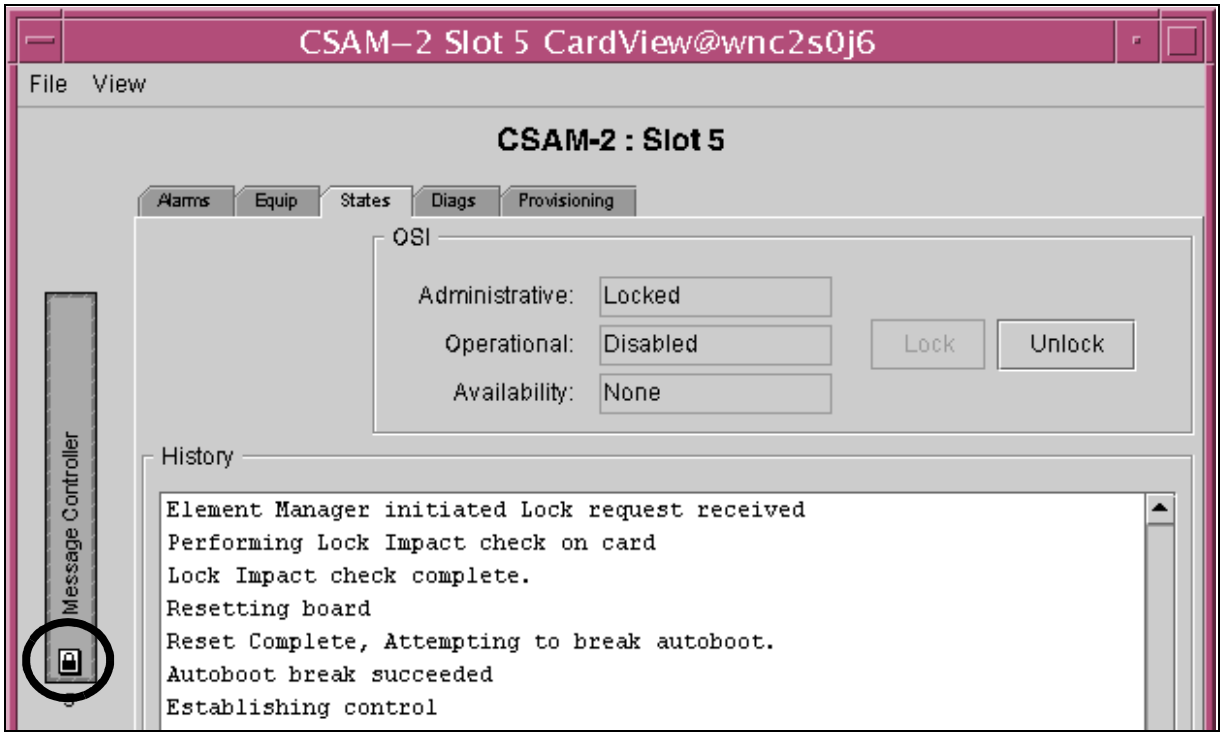
**9** Click on the States tab.

Click on the Lock button.



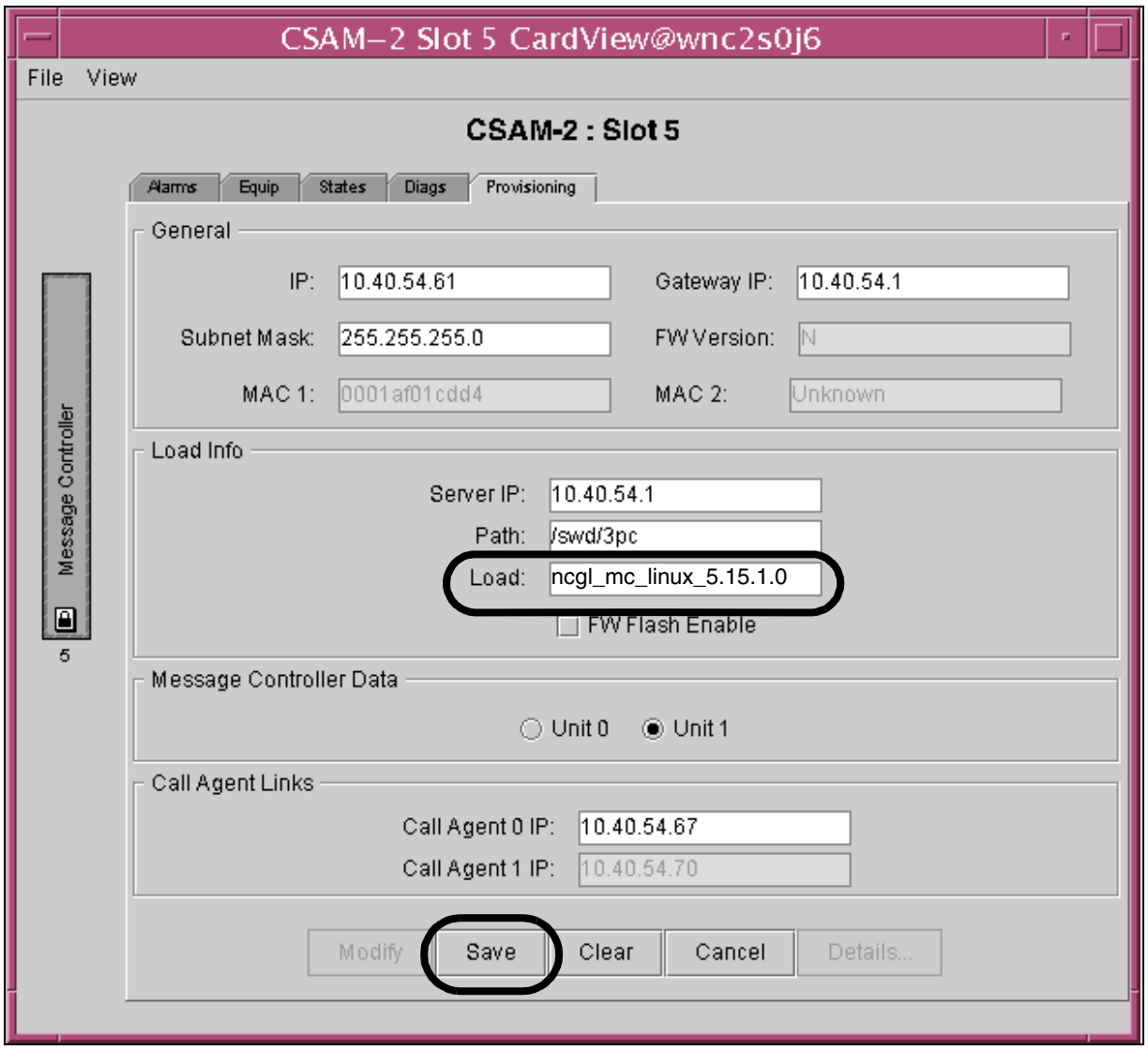

*A lock warning dialog window opens. Confirm the lock warning.*

**10** Wait for the lock icon to appear on the card icon.



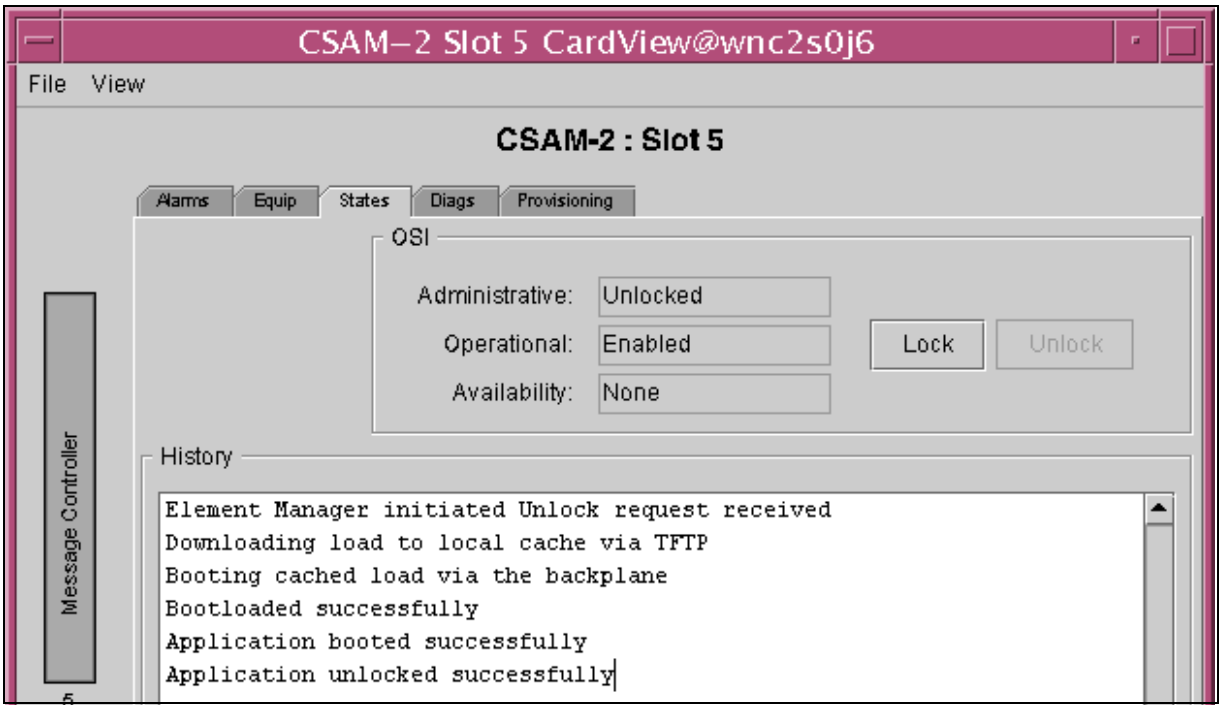

*At the Call Agent Manager, a major ATM alarm is raised, the Message Controller enters the Remote Busy (R) state and is reported as out of service.*

**11** Click on the Provisioning tab, click on Modify, change the Load value to the new software load name, and click Save.



**12** Click on the States tab and click the Unlock button.

Wait for the lock icon to disappear.




*At the Call Agent Manager, the card enters the in service state (.), and the major ATM alarm clears. The Message Controller may raise a major MCTbl alarm while the Message Controller synchronizes to the NTP server.*

***At the active Call Agent Manager interface (CORE0 or CORE1)***

**13** Query the software load for Message Controller 1 and ensure that the new load is reported:

```
> MCMtc
> QryLd 1
```

```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
    .             .         .         .          .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit      MC0    .       . Act      . Inact    open       open
 2           MC1    .       . Act      . Inact    open       open
 3
 4
 5 QryLd
 6 QryHits
 7 ClrHits
 8 Trnsl
 9
10
11
12
13 LogQuery
14 Alarm
15
16           MC Load report retrieved on Thu Jun 19 14:15:54 2004:
17 Help
18 Refresh         Ramdisk ncgl_mc_image_5.15.1.0
  mtc
Time  13:48  >
```

*Soak the load for 10 minutes while monitoring log reports.*

***SDE — At the ACTIVECM window***

**14** Type **GO** and press the Enter key to continue.

## DROP_SYNC

Step DROP_SYNC requires jamming the inactive Call Agent from the active Call Agent Manager.

***SDE — At the ACTIVECM window***

1 Obtain approval to drop synchronization of the call processing application.

2 Type **GO** and press the Enter key to continue.

```
Starting step DROP_SYNC.
Please JAM the Inactive CA Application and confirm when complete:
At the Active TPCMTC MAP; CAMtc Level:
  1) JAM - Jam the Inactive application
Type GO to continue the SWUPGRADE when JAM is completed
Step DROP_SYNC is not complete.
The SWUPGRADE process has paused. Enter GO.
```

***SDE — At the CORE0 or CORE1 window***

3 Jam the inactive Call Agent from the active Call Agent Manager window.

```
> CoreMtc;CAMtc;Jam
```

4 Monitor the jam and verify that a JInact alarm is raised.

***SDE — At the ACTIVECM window***

5 Type **GO** and press the Enter key to continue.

6 Proceed to LOAD_NEW_SIDE_BLADE and LOAD_MATE.

# LOAD_NEW_SIDE_BLADE and LOAD_MATE

This procedure requires the SDE to perform the following actions:

- lock the inactive Call Agent card
- reprovision the platform software load
- unlock the inactive Call Agent

***SDE — At the ACTIVECM window***

**1** Review the message printed to the terminal.

```
Starting step LOAD_NEW_SIDE_BLADE.
Upgrade the New Side Call Agent load at the SAM21 EM GUI
by using the following manual procedure:
  1) At Active COREMTC MAP (ccamtc coremtc), query the Inact blade IP addr
    a) Use QueryIP command to determine the IP address of mate blade.
  2) At SAM21 EM GUI, open Card View for Inact Call Agent Card:
    a) Under the Provisioning Tab, determine IP address of the card.
    b) Ensure IP address in GUI matches inactive card IP address.
  3) Under the States Tab, Lock the card.
  4) Under the Provisioning Tab, change the boot file:
    a) Click Modify.
    b) Change boot file name to new load.
    c) Click Save.
  5) Under the States Tab, Unlock the card.
    a) Monitor the boot progress in the History pane.
  6) At Active COREMTC MAP, monitor Inact load initialization:
    a) Inact status begins with "/booting"
    b) Wait until the status becomes "/waiting"
  7) At Inactive COREMTC map (ccamtc coremtc), Validate newly booted load:
    a) Telnet/Login to the Inact Blade
    b) Under the Sys level, QryLd must indicate the new load version
Type GO to continue the SWUPGRADE when above steps are successfully complet
Step LOAD_NEW_SIDE_BLADE is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2** Perform the instructions listed in the output. Refer to the following procedures for assistance:

- Lock the inactive Call Agent — Call Agent Lock.
- Change the boot file — Reprovision Call Agent platform load.
- Unlock the inactive Call Agent — Call Agent Unlock.

**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 227 for assistance with the platform software patching procedure.

**3** After patching is complete, or if no patches are available, type **GO** and press the Enter key.

*Step PATCH_NEW_SIDE_BLADE completes.*

*Step MATELINK_RTS runs and completes. This step verifies the communication path between the active call processing application and the upgraded, inactive call processing application.*

*Step UPDATE_STEPS_AND_VARS runs and completes. This step automatically provisions environment variables and updates the list of steps on the inactive call processing application. The active and inactive call processing application data for the ONP is synchronized.*

*Step CHECK_NEW_LOAD runs and completes. This step verifies that the inactive call processing application on the inactive Call Agent has no datafill. The software verifies that this load has no datafill by checking that table TERMDEV has a single tuple.*

*Step SET_DATE_AND_LOGMSG runs and completes. This step sets the inactive side time and date from the active side. The login message is set from variable INACT_LOGMSG.*

*Step CHECK_LOGS_2 runs and completes. This step displays the count of logs in the LOGUTIL buffer since the start of the process. The log report types displayed are determined by the variable LOGS.*

*Step CLEAR_TRAPINFO runs and completes. This steps clears all traps on the upgraded inactive call processing application. By clearing the traps now, it is easier to differentiate between old and new traps that are caused by subsequent steps.*

*Step TRANSFER_DEVICES_INFO runs and completes. This step copies data from variable VERIFY_DEVICES on the active call processing application to the inactive call processing application.*

*If the CS 2000 - Compact is configured with Message Controllers, step MS_CHECK runs. This step checks that the software load in the Message Switch is the correct load for the upgraded call processing application load.*

*Step DISABLE_AUTOIMAGE runs and completes. This step disables the automatic image dump process since the automatic image dump process could interfere with the ONP.*

*Step SET_OFFICE_TUPLES runs and completes. This step retains the current state of office parameters NODEREXCONTROL, LCDREX_CONTROL, and GUARANTEED_TERMINAL_CPU_SHARE and then sets both NODEREXCONTROL and LCDREX_CONTROL to OFF. GUARANTEED_TERMINAL_CPU_SHARE is set to its maximum value.*

*Step SET_PADNDEV runs and completes. This step saves the tuples in table PADNDEV, deletes all the tuples, and then adds tuples according to variable PADNDEVS.*

*Step SEND_PATCHES runs and completes. This step copies the patch files for the upgraded inactive call processing application from the location specified by variable PADNDEVS to the inactive call processing application.*

*Step APPLY_PATCHES runs and completes. The patches that were copied in step SEND_PATCHES are applied.*

*Step CHECK_LOGS_3 runs and completes. This step displays the count of log reports stored in the LOGUTIL buffer.*

*Step RESTORE_PADNDEV runs and completes. This step restores table PADNDEV to contain the exact tuples it contained before step SET_PADNDEV.*

**4** Proceed to TABLE_TRANSFER.

# TABLE_TRANSFER

This step copies table provisioning data from the active call processing application to the undatafilled, inactive call processing application.

Step TABLE_TRANSFER is automated. Manual intervention is needed only if some of the table data fails to transfer. The table transfer stops according to variables STOPIF and LIMIT.

For any failed tables, compare the old, active side data to the new, inactive side data to identify and correct any tuples. If necessary, contact your translations engineer or Nortel Networks support personnel for assistance.

For some offices, it may be necessary or preferred to change office variables and parameters on the inactive side after this step completes. One possible parameter to change is field LOG_OFFICE_ID in table OFCVAR. Change this parameter after TABLE_TRANSFER completes and before step START_PRESWACT. Use the procedure below for logging into the inactive call processing application.

**ATTENTION**

If it is necessary to access the inactive call processing application to correct a problem, use the following procedure.

If it is necessary to abort the upgrade at this point, issue the CANCEL command at the ACTIVECM window.

### *At the INACTIVECM window*

1 Log in to the active call processing application by telnetting to the CS 2000 Core Manager as user cmusr.

2 Enter the mate input/output level and log in to the inactive call processing application:

```
>MATEIO;MATELOG ME;SLEEP 240 MINS
```

***Note 1:*** The `Mate>` prompt indicates that the command is sent to the inactive call processing application.

***Note 2:*** If the **MATELOG ME** command fails, enter **MATELINK RTS** and retry the **MATELOG ME** command.

```
>mateio
MATEIO -- MATECOM link not available. Attempt RTS.
>matelink rts
RTS PASSED
```

3 At the Mate> prompt, log in to the inactive call processing application:

**Mate> username password**

4 Use the table editor to correct any datafill problems.

5 Use the LOGOUT command at the Mate> prompt to exit the inactive call processing application:

**Mate> LOGOUT**

***Note:*** Do not log out of the active call processing application. Verify that the prompt is the Mate> prompt.

### *At the ACTIVECM window*

6 Type **GO** and press the Enter key to continue.

*Step TABXFR_REPORT runs and completes. This step prints a report of all table failures to the trace device.*

*Step CHECK_LOGS_4 runs and completes.*

7 Proceed to START_PRESWACT.

## START_PRESWACT

Step START_PRESWACT has several sub steps. If any sub step fails to complete, make corrections according to the error message and continue the START_PRESWACT step by typing **GO** and pressing the Enter key. START_PRESWACT re-executes the failed step and continues.

Read the following notes while step START_PRESWACT executes:

START_PRESWACT sub step TABLE_DELTA displays the changes, additions, and deletions between the old and new call processing application software loads for the following tables:

- OFCENG
- OFCSTD
- OFCVAR
- OFCOPT
- DATASIZE
- TCAPTRID
- OPTCTL

For any tables with differences, compare the OLD/NEW and ADDED tuples to identify and correct any errors.

> ***Note:*** Errors stop sub step TABLE_DELTA from completing with the message "`TABLE_DELTA not complete`." The software also provides informative messages such as "Table ATTCONS Checksum incorrect, keys match." The informative messages do not stop the step from completing and do not require any manual action. At a convenient point during the upgrade, compare the old and new loads to understand and validate the differences.

If office parameter changes were made after step TABLE_TRANSFER on the inactive call processing application, then TABLE_DELTA displays the change.

Proceed to PRESWACT_DIRP_AND_BILLING.

# PRESWACT_DIRP_AND_BILLING

### *SDE — At the ACTIVECM window*

1 Step PRESWACT_DIRP_AND_BILLING runs and completes, but pauses the process. The CS 2000 - Compact requires no manual action for DIRP and billing.

```
Starting step PRESWACT_DIRP_AND_BILLING.

       MTD Billing subsystem information
       ---------------------------------
MAPCI:
MTC:
IOD:
DIRP:
MTD  TapeName  Status    IOC.CARD/PORT

        TRANSFERING table DIRPPOOL to inactive side.
        ----------------------------------------.
ACT - WARNING: If any DIRP actions other than those described in this step
               occur between now and SWACT, the user may need to manually
               correct any discrepancies in table DIRPPOOL.
D/R DART#     689 ->              DIRPPOOL : Restored       7 , Failed   0

        To prepare DIRP billing subsystems for the SWACT, please follow
        instructions in the NTP 'One Night Process Software Dellivery Pro-
cedure's.
        This verifies that all DIRP billing subsystems have been properly
        prepared for the upcoming SWACT and DIRP information is readily
available
       for timely restoration to minimize the loss of existing data, should
DIRP
        file storage devices become corrupted during the transition.

        These measures may include, but are not limited to:

           - DIRP rotation of disk primary billing.
           - DIRP rotation of tape primary billing.
           - close existing DPP billing file and open a new one.
           - prepare tape billing standby volumes.
           - prepare tape parallel standby volumes.
           - copy unprocessed disk billing file to backup tape.
           - copy disk parallel files to backup.
           - match DIRPPOOL volumes between active and inactive.
Step PRESWACT_DIRP_AND_BILLING is complete.
The SWUPGRADE process has paused. Enter GO.
```

2 Type **GO** and press the Enter key to confirm PRESWACT_DIRP_AND_BILLING.

*Step PRINT_SPMS_INDICES runs and completes.*

3 Step GET_FIRST_SWACT_AGREEMENT begins and pauses the process. The SDE must receive agreement from the customer to proceed with the SWACT.

***Note:*** If a delay of longer than 15 minutes is expected before the SWACT, the SDE should wait until all preparations are made before continuing.

```
Starting step GET_FIRST_SWACT_AGREEMENT.
NORESTARTSWACT will be used for initiating a CC Warm SWACT.
Do you wish to proceed with the preparation for the CC warm swact?
Step GET_FIRST_SWACT_AGREEMENT is complete.
The SWUPGRADE process has paused. Enter GO.
```

4 Type **GO** and press the Enter key to confirm GET_FIRST_SWACT_AGREEMENT.

5 Step PREPARE_FOR_SWACT begins.

```
Starting step PREPARE_FOR_SWACT.
DISPLAY_NOP_USERS                executing
SESSION  STATE  APPL.   ID      NODE
   0     IDLE
   1     IDLE
         2     IDLE
         3     IDLE
         4     IDLE
         5     IDLE
         6     IDLE
         7     IDLE
         8     IDLE
         9     IDLE
        10     IDLE
        11     IDLE
        12     IDLE
        13     IDLE
        14     IDLE
DISPLAY_NOP_USERS                      complete
        Please perform the following:
           - Remind the Telco personnel to inform 'active' NOP users
             listed above (if any) to log out of their session(s)
             before the S/W upgrade can continue.
           - Remind the Telco personnel to contact the high profile
             customers to ensure that they are not in emergency call
             processing mode and inform them of the approximate SWACT
             time.
           - Disable all polling and periodic testing. There is to
             be no activity on the Core, MS and CLOCK until cleared
             by the software delivery engineer.

             WARNING: FAILURE TO COMPLY MAY RESULT IN A SYSTEM RESTART.

           - Ensure no further activity is performed on the DPP,
             including DPP polling or disk backup, and inform the
             downstream processing center.
           - Dump all special logs so they can be restored onto the
             new load after postswact has completed.

Step PREPARE_FOR_SWACT is complete.
The SWUPGRADE process has paused. Enter GO.
```

6 Type **GO** and press the Enter key to confirm PREPARE_FOR_SWACT.

*Step STATUSCHECK runs and completes.*

*Step CHECK_LOGS_5 runs and completes.*

*Step TRANSFER_TIMINGS runs and completes.*

7 Proceed to SWACT.

# SWACT

***SDE — At the ACTIVECM window***

**1** Review the instructions for step SWACT.

```
Starting step SWACT.
Confirm that the Inactive CA Application is NOT JAMmed,
-or- RELEASE the JAM and confirm when complete:
At the Active TPCMTC MAP; CAMtc Level:
       1) RELJAM - Release the Jam on the Inactive application
Type GO to confirm, and to continue the SWUPGRADE
Step SWACT is not complete.
The SWUPGRADE process has paused. Enter GO.
```

***SDE — At the CORE0 or CORE1 window***

**2** Confirm that inactive Call Agent is not jammed or release the jam.

***SDE — At the ACTIVECM window***

**3** Type **GO** and press the Enter key to continue with the SWACT.

*The process performs final checks and pauses for a final NORESTARTSWACT confirmation.*

```
Beginning SWACT checks:
All the SWACT checks have finished successfully.

The VR_PRESWACT_TRANSFER step completed successfully.
All INSV and ISTB series 1 PMs will have execs loaded after the SWACT.

****************** FINAL SWACT CONFIRMATION *****************
Do you wish to proceed with the NORESTARTSWACT CC warm swact?
Step SWACT is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**4** Receive final agreement from the telephone operating company personnel to proceed with the SWACT. Type **GO** and press the Enter key once confirmation is received.

**5** Monitor the messages printed to the terminal and verify that activity does switch at the CORE0 or CORE1 windows.

```
Starting step SWACT.
After the completion of the CC warm swact, please log
both the TRACE user and the ACT user
onto the new active side and enter SWUPGRADE;GO.
All Pre-SWACT checks completed. Starting Warm SWACT now.
********        The cursor will not be returned  ********
********       unless a critical failure occurs. ********
******** Now monitoring Warm SWACT messages.********

Pre-initialization done

Communication established

Exchange of data with the mate done

Transfer of data done (FASPECT)

Data estimation done

Store allocated on active CC

Store allocated on inactive CC

AMA processing completed

         SWACT Inactive Procs running, this may take a few minutes

Before_callp_stopped procs completed

Call processing in PM stopped

Call processing I/O in CC stopped

Call data extracted

Data transfer completed
```

*Activity switches to the upgrade call processing application. The connection at the ACTIVECM window is dropped.*

**6** Log in to the upgraded call processing application by telnetting to the CS 2000 Core Manager or CBM as user cmusr from the ACTIVECM and INACTIVECM windows.

***Note:*** The switch provides a prompt to perform test calls after step RECOVER_DIRP_AND_BILLING.

**7** Continue the software upgrade.

```
> SWUPGRADE;GO
```

**8**

**ATTENTION**

Instruct the operating company to perform a 911 test call. If the test call fails to complete, contact Nortel Networks Emergency Recovery immediately. **Do not continue.** If the test call is successful, continue with the software upgrade and ensure the following actions take place:

— system recovery of all DIRP and billing subsystems

— system recovery of any critical alarms

— operating company begins test calls

— system logs are monitored for office stability

*Tracing begins and the software upgrade continues.*

*Step DISPLAY_DATE completes.*

*Step RECOVER_DIRP_AND_BILLING begins.*

```
2002/07/08 09:52 INACT_LOGMSG
>SWUPGRADE;GO
SWUPGRADE:
This device is selected for TRACEing
Variable TRACE_DEVICE has been set to TELNSVR00001.

Starting step DISPLAY_DATE.
Date: 2002/07/08, Time: 10:18:17
Finished step DISPLAY_DATE.

Starting step RECOVER_DIRP_AND_BILLING.

 To recover DIRP billing subsystems after the SWACT, please follow
 instructions in the NTP 'One Night Process Software Delivery Procedures'.

 This verifies that all DIRP billing subsystems have properly recovered
 from the SWACT.

 Check these devices for proper operation.

 The DIRP increment of the IOD MAPCI level provides a QUERY command to
 verify the resulting disposition of these subsystems (i.e. QUERY AMA)
 and the DPP increment of the IOD MAP level allows the applicator to
 display the alarm status for the DPP active and standby units (command
 ERRMAP ALARMS) and also provides the ability to list DPP active files
        (command LSTACT).
Step RECOVER_DIRP_AND_BILLING is complete.
The SWUPGRADE process has paused. Enter GO.
```

Determine the next action.

| If | Do |
|---|---|
| reversion to the old call processing application load is required | Type **CANCEL**, press the Enter key, and refer to Revert and Abort on page 155 |
| 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 on page 155 |
| reversion is not required | proceed to START_POSTSWACT on page 147 |

## 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 on page 155 |
| 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
- Reprovision Call Agent platform load
- Call Agent Unlock

***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.
SWUPGRADE has now reached the SYNC_SWITCH step.
Are you ready to SYNC the switch?
Step SYNC_SWITCH is not complete.
The SWUPGRADE process has paused. Enter GO.
```

**2** Type **GO** and press the Enter key.

*Step SYNC_SWITCH completes. Optionally, monitor the synchronization from the CORE0 or CORE1 windows.*

*Step FINISH_POSTSWACT runs and completes. This step executes any remaining POSTSWACT steps. Several reports about the software upgrade are printed to the terminal. If a step fails to complete, follow the instructions given; type **GO** and press the enter key to continue.*

*Step RESTORE_PARMS runs and completes. This step restores the office parameters NODEREXCONTROL, LCDREX_CONTROL, GUARANTEED_TERMINAL_CPU_SHARE, and DUMP_RESTORE_IN_PROGRESS that were saved in step PRINT_PARMS_AND_SAVE.*

*Step RESET_DEVICES runs and completes. This step verifies that all devices used during the software upgrade are set to their original values.*

*Step COMPLETE_NEW_LOAD_INIT runs and completes. This step prints messages as a reminder to SITE that need to be performed after POSTSWACT is complete.*

```
Starting step COMPLETE_NEW_LOAD_INIT.

        1) Re-input any data changes made prior to the software
           update but not captured on journal file, if any.

        2) Notify NOP end users to log back in.

        3) Reassign all current PROFILE information (LOGIN or
           RESTART) in SFDEV.

        4) Restore any special logs (listreps special).

        5) Reassign any temporary log ROUTING setup via LOGUTIL.

        6) Reassign any changes in the INTEG level of the MAP
           (for example, UPTH, BUFFSEL, FILTER and others).

        7) If Network Management code blocking was removed earlier, have
           Network Maintenance personnel restore code blocking active.

Step COMPLETE_NEW_LOAD_INIT is complete.
The SWUPGRADE process has paused. Enter GO.
```

***SITE — At the ACTIVECM window***

**3** Perform any actions specified in step COMPLETE_NEW_LOAD_INIT.

***SDE — At the ACTIVECM window***

**4** Type **GO** and press the Enter key to complete step COMPLETE_NEW_LOAD_INIT.

*Step COMPLETE_NEW_LOAD_INIT completes.*

*Step RESET_LOGIN_BANNER runs and completes. This step erases the software upgrade banner.*

*Step DUMP_NEW_LOAD runs and completes.*

*Step RESUME_REX_TEST runs and completes.*

*Step START_JOURNAL_FILE runs and completes.*

*Step PRINT_SWUPGRADE_REPORT runs and completes. This step prints the start and stop time for each step in the software upgrade.*

*Step STOP_RECORD runs and completes.*

*Step UPGRADE_COMPLETE begins.*

```
Starting step UPGRADE_COMPLETE.
   Process complete. You may now QUIT out of the SWUPGRADE increment.
Finished step UPGRADE_COMPLETE.

SWUPGRADE Process complete - all steps have been executed.
>QUIT
CI:
```

**5** Type **QUIT** and press the Enter key.

**6** The Call Agent software upgrade is complete.

# DUMP_OFFICE_IMAGE

***SITE — At the ACTIVECM window***

**1** Nortel Networks 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 79.

# Appendix A Revert and Abort

Perform these procedures only if it is necessary to abort (CANCEL) the SWUPGRADE.

***SDE — At the ACTIVECM window***

**1** Type the following commands to abort the upgrade:

```
> SWUPGRADE
> CANCEL
```

*Two confirmations are required to continue.*

**> Y** (enter twice)

**Example**
The following is an example of the messages generated when the CANCEL command is entered at the ACTIVECM window and confirmed twice.

```
*********************************************
**                  WARNING!!                **
**                                           **
** The CANCEL command cancels all work done **
** by SWUPGRADE so far. Once cancelled       **
** SWUPGRADE has to be re-started.           **
** To halt temporarily, use the PAUSE        **
** command. Type:                           **
**       HELP PAUSE                          **
** for more information.                     **
**                                           **
** Do you wish to CANCEL the SWUPGRADE?      **
*********************************************
Please confirm ("YES", "Y", "NO", or "N"):
>YES


*********************************************
**                   WARNING!!
**
** CANCEL will rollback all completed steps.
** The switch is not in sync.
** Do you want to sync the switch during
** the rollback?
*********************************************
Please confirm ("YES", "Y", "NO", or "N"):
> YES
```

***End of example***

**2**

**ATTENTION**
Watch the output messages on the TRACE DEVICE!

The TRACE DEVICE will output messages informing the operator what steps are being rolled back (see below). Upon getting the messages:

*The SWUPGRADE process has paused. Enter GO or type GO to resume CANCEL*

The operator must follow the instructions printed to the TRACE DEVICE and type "GO" and press return on the ACTIVECM window until getting the message:

*SWUPGRADE CANCEL is completed.*
*You may now QUIT out of the SWUPGRADE increment.*

**3** After the SWACT, log in to the old load by typing the following in the ACTIVECM window. If using a terminal window as the trace device, repeat this step at a second terminal window.

```
> telnet <cs_2000_core_mgr_ip_addr>
```

and logging in as "cmuser." This action towards the connection to the login prompt on the call processing application. Log in with a username and password:

```
> <username> <password>
```

or

```
> <username>
> <password>
```

***IMPORTANT!*** Immediately after logging in to the old load and before continuing the CANCEL, type the following:

```
> TABXFR;CANCEL

**WARNING: This command cancels the data move.
Once cancelled it cannot be restarted without
rebooting the new BCS image. If a temporary halt
is desired please use the HALT or STOPXFR
commands. Do you wish to CANCEL the data move?

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

> Y
> QUIT
```

4 Ensure the trace device is still set:

```
> SWUPGRADE;DISP VAR TRACE_DEVICE
```

If the tracing is not set to a device, or if it is set to the wrong device, set the trace device as follows:

```
> SET TRACE_DEVICE <device_name>
```

**device_name**
is a value like TELNSVR00445. Use the QUSER command to determine the correct device to use.

5 Continue the CANCEL to conclusion:

```
> SWUPGRADE;GO
```

6 Enter the following when SWUPGRADE CANCEL is complete:

```
> QUIT ALL
```

### Example session of SWUPGRADE CANCEL

```
WARNING: The rollback of software upgrade steps is
         about to start.
Messages sent to 1 user.

Executing the step RESTART_OLD_LOAD.
The step RESTART_OLD_LOAD is completed.

Executing the step STATUSCHECK.
Checking Nodes Status
Checking DS1 Carriers Status
Checking MS Interface Cards Status
Checking LIU Status
Checking MS FBUS Status
Checking Integrated Node Maintenance
STATUSCHECK successful.
The step STATUSCHECK is completed.

Executing the roll back for step recover_dirp_and_billing.

Configure the DIRP billing subsystems for revert SWACT to
the old load.

Note: For details for completing the following refer to
"PRESWACT DIRP and billing" procedure.
  a. ACT Take down billing tapes and format new standby
     volumes in DIRP. Leave these demounted, they will
     become the active volumes after SWACT.
     Disk volumes will rotate and recover automatically
     after SWACT.
```

## Example session of SWUPGRADE CANCEL

```
     Parallel volumes on tape (or DPP/BMC) can be
     recovered manually after SWACT.

  b. INACT Ensure datafill is correct on the inactive side for
     table DIRPPOOL.

  c. INACT if DIRP_REC file is present on the inactive SFDEV,
     ensure each entry in DIRP_REC is correct for the
     revert SWACT.
     Note: In DIRP_REC the parallel volume assignments
     for DIRPPOOL should be set to nil ($) for all pools.
Execution completed.
The SWUPGRADE process has paused. Enter GO.

WARNING: SWUPGRADE is about to execute the ABORTSWACT step.
         Do you which to proceed?

Execution completed.
The SWUPGRADE process has paused. Enter GO.

Executing the step PRELOAD_EXECS.
Successfully fetched: KSETEX
Preloading lineup KSETEX to XPMs
This may take a couple of minutes

Successfully fetched: DTCEX
Preloading lineup DTCEX to XPMs
This may take a couple of minutes

Successfully fetched: POTSEX
Preloading lineup POTSEX to XPMs
This may take a couple of minutes

PRELOAD_EXECS                    complete

Executing the step SWACT.
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
Execution is not complete.
The SWUPGRADE process has paused. Enter GO.

Executing the step SWACT.
Beginning SWACT checks:
All the SWACT checks have finished successfully.
```

## Example session of SWUPGRADE CANCEL

```
****************** FINAL SWACT CONFIRMATION *****************
Do you wish to proceed with the ABORTSWACT CC warm swact?
Execution is not complete.
The SWUPGRADE process has paused. Enter GO.

Executing the 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

>
Connection closed by foreign host.
username@host:~$
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% Telnet to the CS 2000 Core Manager and log in as user cmusr  %%
%% The CS 2000 Core Manager forwards the connection to the      %%
%% old PCL. Log in with <username> <password>                   %%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

### Example session of SWUPGRADE CANCEL

```
*******************************************************
**                                                   **
**    WARNING...WARNING...WARNING...WARNING.         **
**                                                   **
**                                                   **
** ......In LINEMODE,To Enter into BREAK........     **
**                                                   **
** Press ^B, Type the Command and Press <Enter>      **
**                                                   **
** Example: ^Bhx <Enter>                             **
**                                                   **
**                                                   **
*******************************************************
Telnet LINEMODE.

Enter username and password
MIB variable CharOptionAllowed must be set first to allow CHAR MODE.
><username> <password>
MIKEM Logged in on 2003/10/21 at 11:11:14.
************************************************************
**                                                        **
**            This is a private database.                  **
**       All activity is subject to monitoring.            **
**   Any UNAUTHORIZED access or use is PROHIBITED, and     **
**            may result in PROSECUTION.                   **
**                                                        **
************************************************************
************************************************************
**                                                        **
**       WARNING: SOFTWARE UPGRADE IS IN PROGRESS         **
**       ----------------------------------------         **
**                                                        **
**   Please refrain from using SERVORD or TABLE EDITOR or  **
**     CI commands that may interfere with the process.    **
**                                                        **
**      Under no circumstances is SYNC to be done !!!     **
**                                                        **
************************************************************
2003/10/06 14:32 swupgrade rollback doc
This device is selected for TRACEing

Executing the step DISPLAY_DATE
This device is selected for TRACEing
Variable TRACE_DEVICE has been set to TELNSVR00002.

Starting step DISPLAY_DATE.
Date: 2003/10/21, Time: 11:11:33
The step DISPLAY_DATE is completed
```

### Example session of SWUPGRADE CANCEL

```
Resetting the default tabxfr platform.
Tabxfr platform has been reset to XACORE.

Executing the step START_POSTSWACT

REACTIVATE_TRIGASGN              executing
REACTIVATE_TRIGASGN              complete

DIRP_RECOVERY                    executing
DIRP_RECOVERY                    complete

DIRP_AUDIT                       executing
DIRP_AUDIT                       complete

HARDWARE_CHECK                   executing
HARDWARE_CHECK                   complete

...

BEGIN_TESTING                    executing
BEGIN_TESTING                    complete
Enter Postswact after office testing has been completed
The step START_POSTSWACT is completed

Executing the step CHECK_LOGS_1
New logs on ACTIVE unit since 2003/10/21 11:00:04:
   TRAP    : 0
   SWERR   : 1
Use command DISPLAY LOG <log name> <n or ALL> [Act or Inact]
to see the content of a log.
Execution completed.
The SWUPGRADE process has paused. Enter GO.
Executing the rollback for step PRESWACT_DIRP_AND_BILLING.

Please follow the step Recover billing from the ONP MOP
procedure Revert to old load to perform the rollback
of the step PRESWACT_DIRP_AND_BILLING.
Execution completed.
The SWUPGRADE process has paused. Enter GO.

Executing the step RESTORE_PARMS
The step RESTORE_PARMS is completed.

Executing the step PERFORM_TEST_CALLS.
   AMAB has been added to the LOGS variable for
   automatic monitoring during the execution of the
   test calls for possible AMA test call failures.
```

## Example session of SWUPGRADE CANCEL

```
   If not already done, please perform test calls.
Execution is not complete.
The SWUPGRADE process has paused. Enter GO.

Executing the step PERFORM_TEST_CALLS.
AMAB has been removed from the LOGS variable.
The step PERFORM_TEST_CALLS is completed.
Reload the original 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
address:
     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) Restore the boot file name to the original load file.
     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 original load version
Type GO to continue the SWUPGRADE when complete
Execution is not complete.
The SWUPGRADE process has paused. Enter GO.

Executing the step SYNC_SWITCH.
SWUPGRADE has now reached the SYNC_SWITCH step.
Are you ready to SYNC the switch?
Execution is not complete.
The SWUPGRADE process has paused. Enter GO.

Executing the step SYNC_SWITCH.
The step SYNC_SWITCH is completed.

Executing the step FINISH_POSTSWACT

XA_UNSPLIT                        executing
XA_UNSPLIT                        complete
...
Executing the step RESET_DEVICES
The step RESET_DEVICES is completed.
```

### Example session of SWUPGRADE CANCEL

```
If any abort actions are required for step READ_BULLETINS,
please perform them now.

Execution completed.
The SWUPGRADE process has paused. Enter GO.

Executing the ABORT_PRESWACT.
REACTIVATE_DCT                    executing
REACTIVATE_DCT                    complete
REACTIVATE_TRIGASGN               executing
REACTIVATE_TRIGASGN               complete
NBD_ABORT_PRESWACT                executing
NBD_ABORT_PRESWACT                complete
RESET_OFFICE_TUPLES               executing
WARNING: Guaranteed_Terminal_CPU_Share already restored.
WARNING: Auxcp_Cpu_Share already restored.
RESET_OFFICE_TUPLES               complete
ENABLE_AUTOIMAGE                  executing
ENABLE_AUTOIMAGE                  complete
ENABLE_PES_AUDIT                  executing
ENABLE_PES_AUDIT                  complete
RESUME_ATT                        executing
RESUME_ATT                        complete
RESET_SIS_ROUTING_DATA            executing
RESET_SIS_ROUTING_DATA            complete
CLEANUP_VR_MATE_DATA              executing
CLEANUP_VR_MATE_DATA              complete
ABORT_PRESWACT has completed.
Execution completed.

Executing the step STOP_RECORD
The step STOP_RECORD is completed.

The rollback of SWUPGRADE steps is completed.

SWUPGRADE CANCEL is completed.
You may now QUIT out of the SWUPGRADE increment.
>
%%%%%%%%%%%%%%%%
%% > QUIT ALL  %%
%%%%%%%%%%%%%%%%
```

*End of example.*

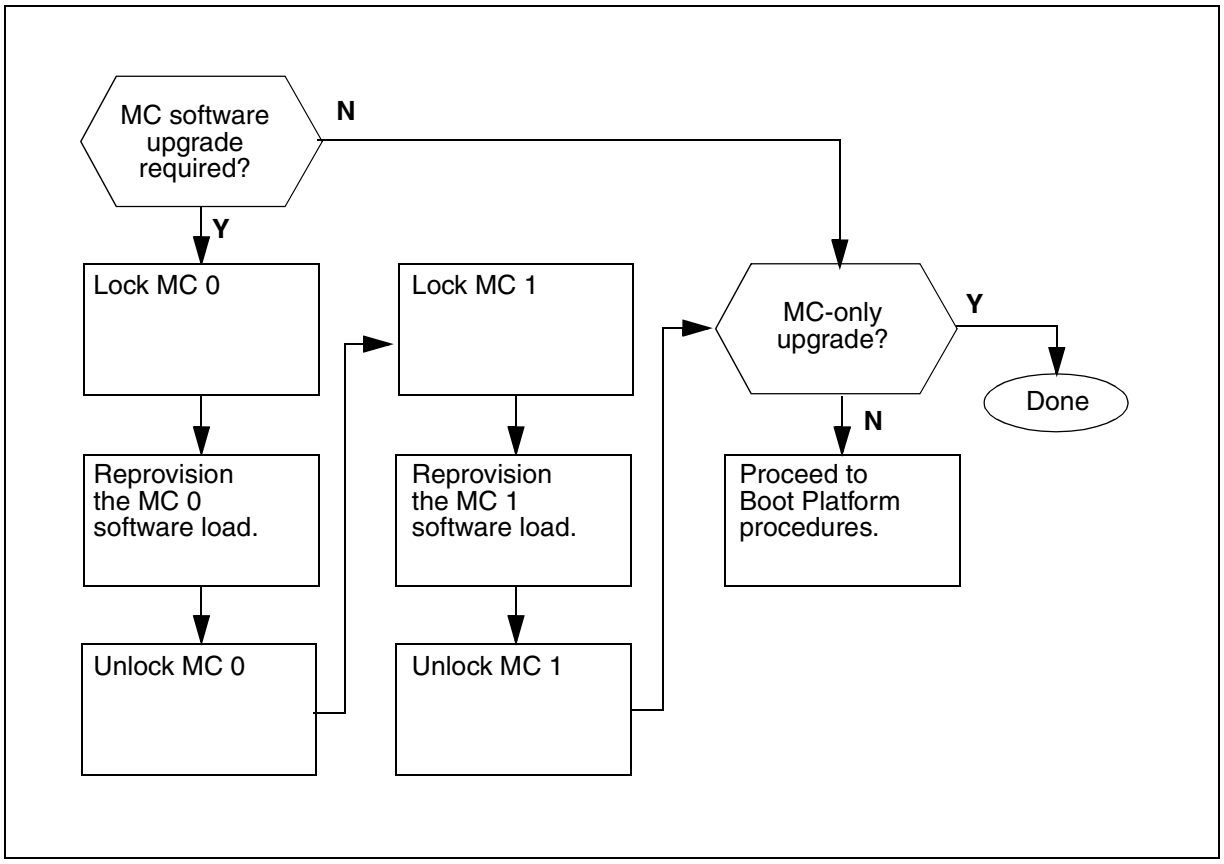
# Appendix B Manual procedures

The procedures in this appendix do not apply to the automatic software upgrade (SWUPGRADE) process.

# Upgrade Message Controller software

Perform the procedures in this section to upgrade the software on the Message Controllers. The units are upgraded one at a time to maintain service.

### Upgrade Message Controller software



# Load Message Controller 0

**ATTENTION**
Perform this step only if the CS 2000 - Compact is configured with Message Controller cards.

***At the MAP***

**1** 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_
```

**2** 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***

**3** 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
```

4 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.*

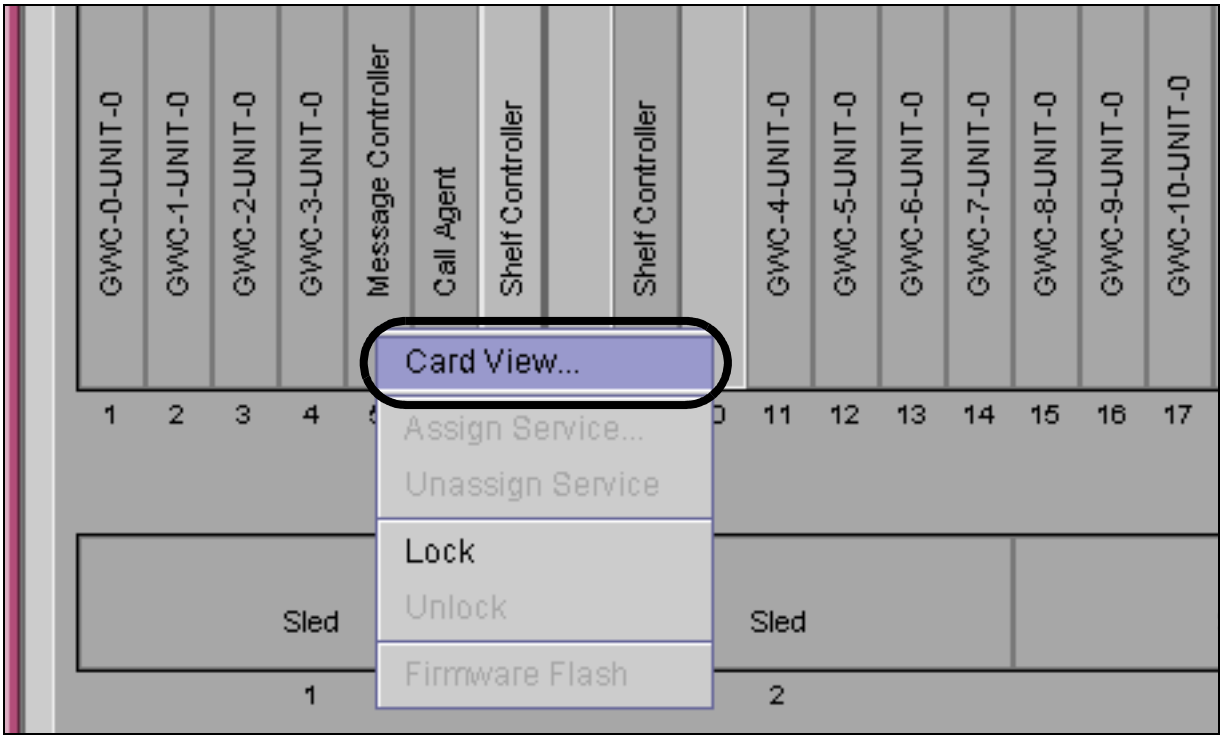
```
10.40.54.60 mc0
```

5 Start the Call Agent Manager interface again:

```
[mtc@hostname mtc]$ ccamtc mcmtc
```

***At the CS 2000 SAM21 Manager client***

6 From the Shelf View, right click on the card and select Card View.

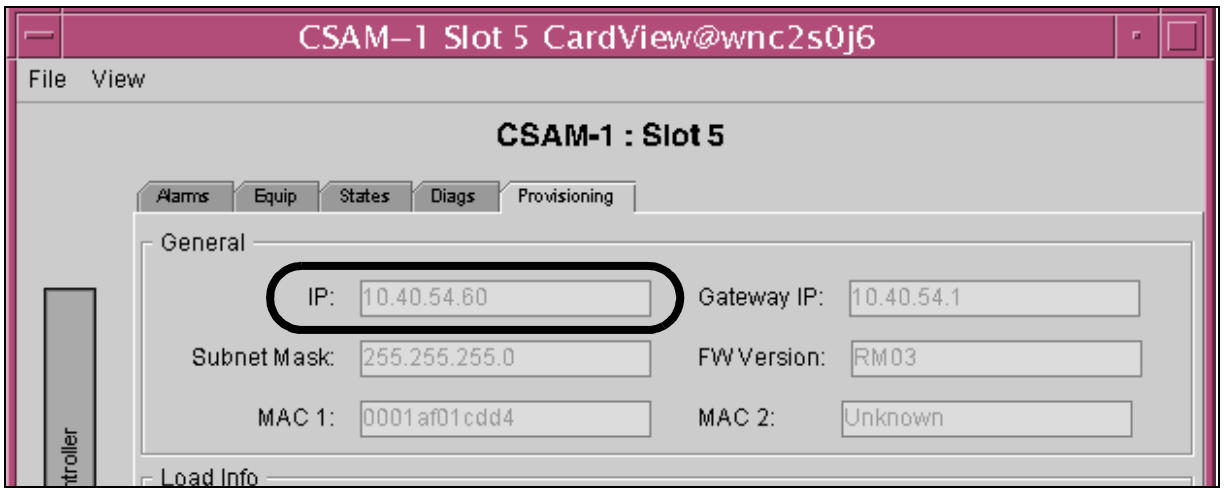



*The Card View window opens.*

7 Select the Provisioning tab on the Card View window.

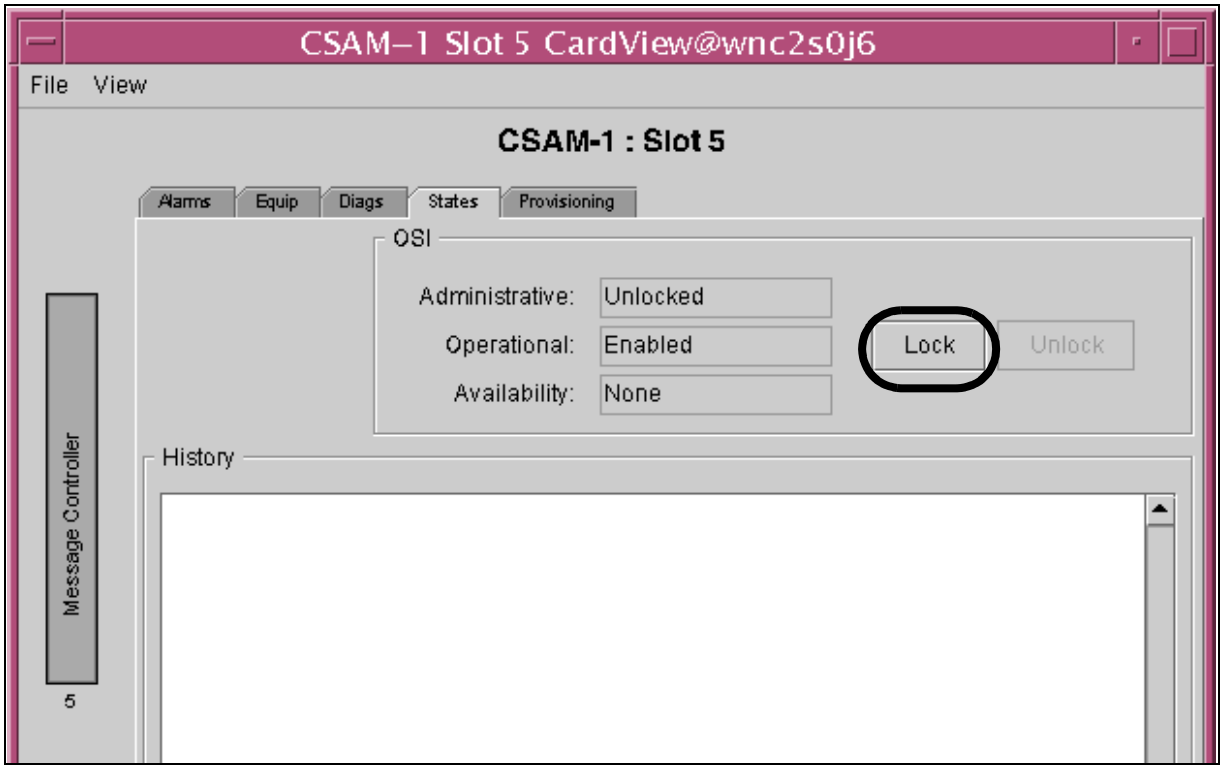
Ensure that the IP address specified in the IP field matches the IP address of Message Controller 0. If the values do not match,

open a different Shelf View from the CS 2000 SAM21 Manager and check the Message Controller provisioning for that shelf.



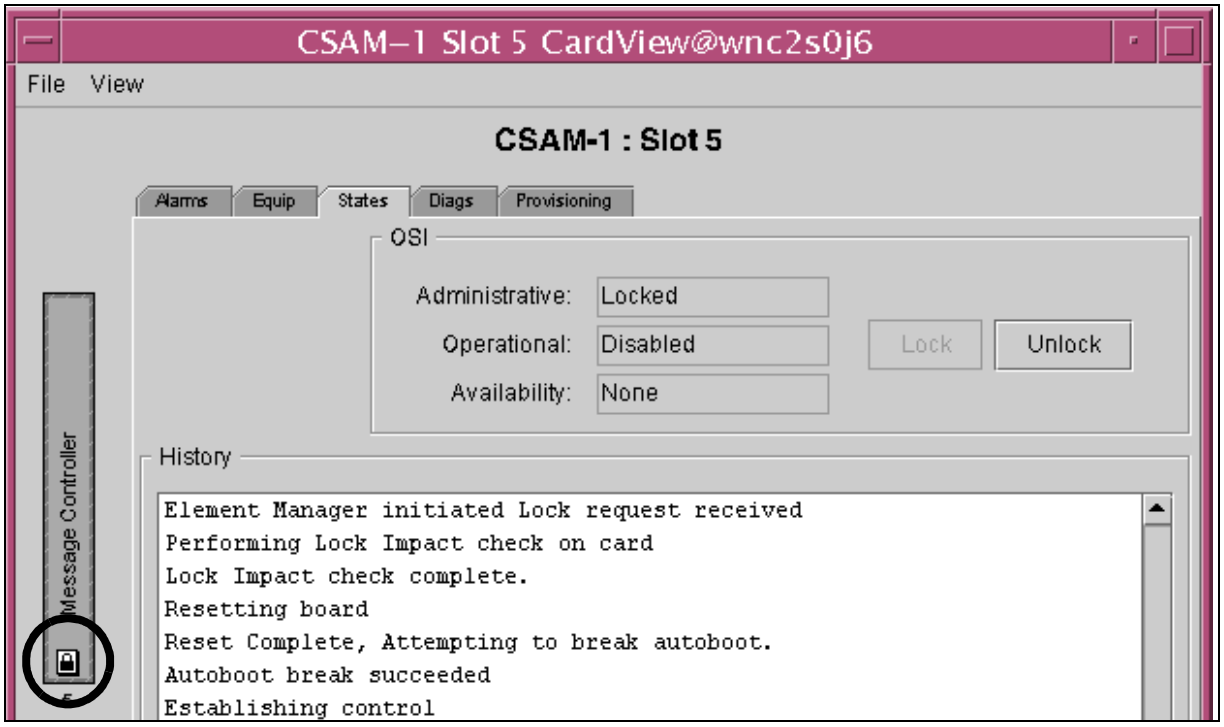

**8** Click on the States tab.

Click on the Lock button.



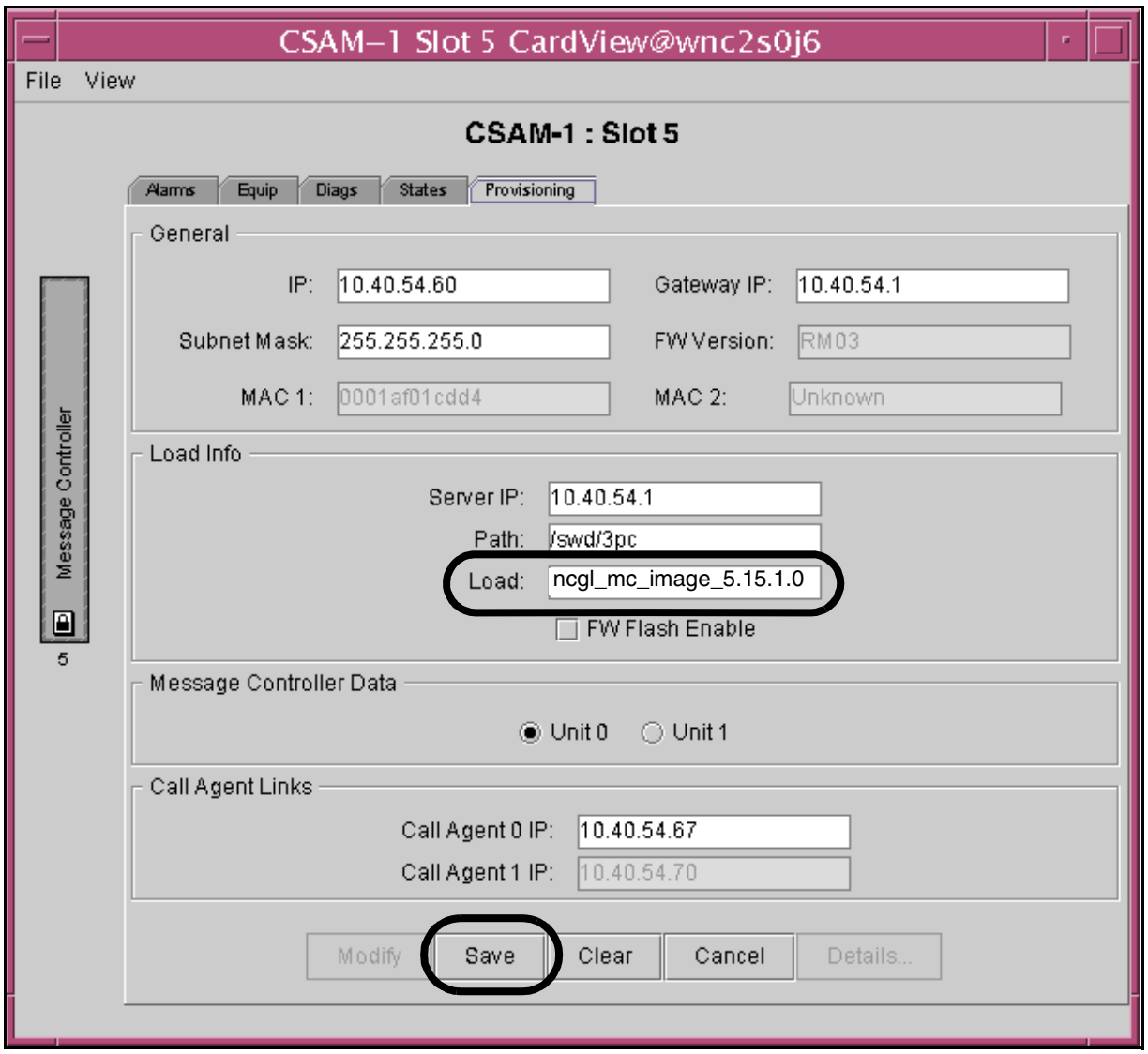

*A lock warning dialog window opens. Confirm the lock warning.*

**9** Wait for the lock icon to appear on the card icon.



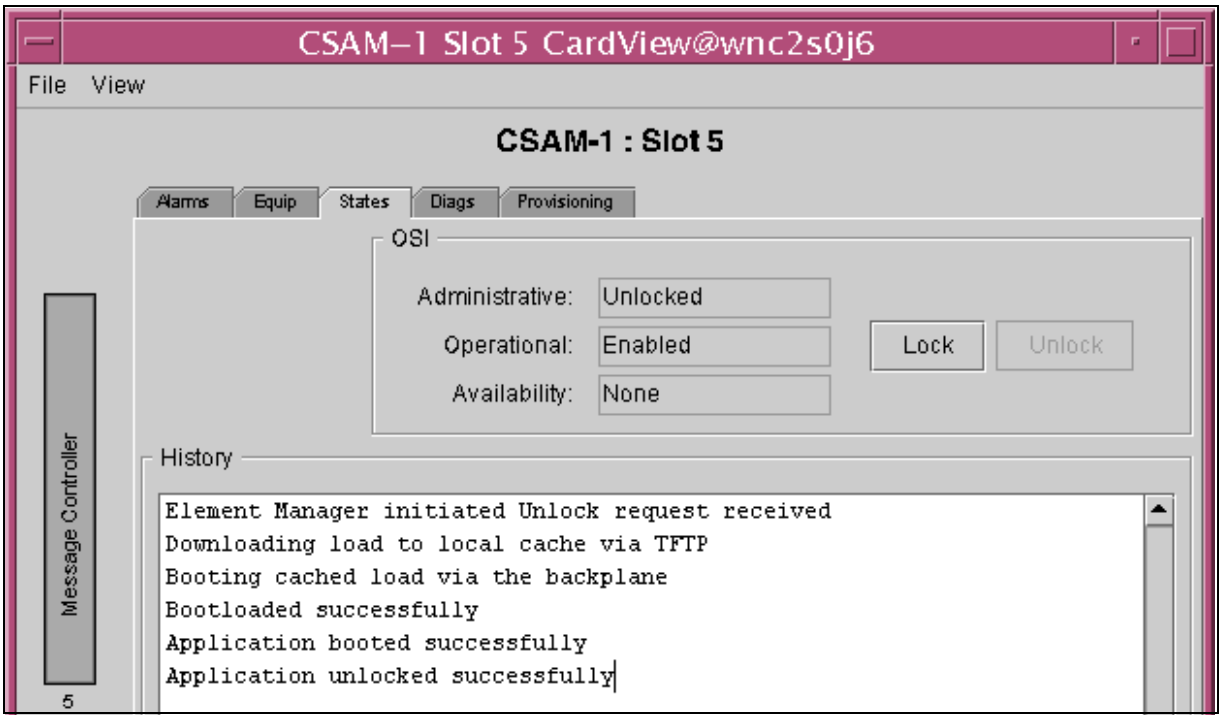

*At the Call Agent Manager, a major ATM alarm is raised, the Message Controller enters the Remote Busy (R) state and is reported as out of service.*

**10** Click on the Provisioning tab, change the Load value to the new software load name, and click Save.



**11** 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***

**12** Query the software load for Message Controller 0 and ensure that the new load is reported:

```
>QryLd 0
```

```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
    .             .         .         .          .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit      MC0    .       . Act      . Inact    open       open
 2           MC1    .       . Act      . Inact    open       open
 3
 4
 5 QryLd
 6 QryHits
 7 ClrHits
 8 Trnsl
 9
10
11
12
13 LogQuery
14 Alarm
15
16           MC Load report retrieved on Thu Jun 19 13:48:45 2004:
17 Help
18 Refresh         Ramdisk ncgl_mc_image_5.15.1.0
  mtc
Time  13:48  >
```

*Soak the load for 10 minutes while monitoring log reports.*

# Load Message Controller 1

**ATTENTION**
Perform this step only if the CS 2000 - Compact is configured with Message Controller cards.

***At the MAP***

**1** 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_
```

**2** 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***

**3** 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
```

4 Exit the Call Agent Manager interface and determine the IP address of Message Controller 1:

```
>0 ALL
[mtc@hostname mtc]$ grep mc1 /etc/hosts
```

*The grep command returns the address of Message Controller 1.*

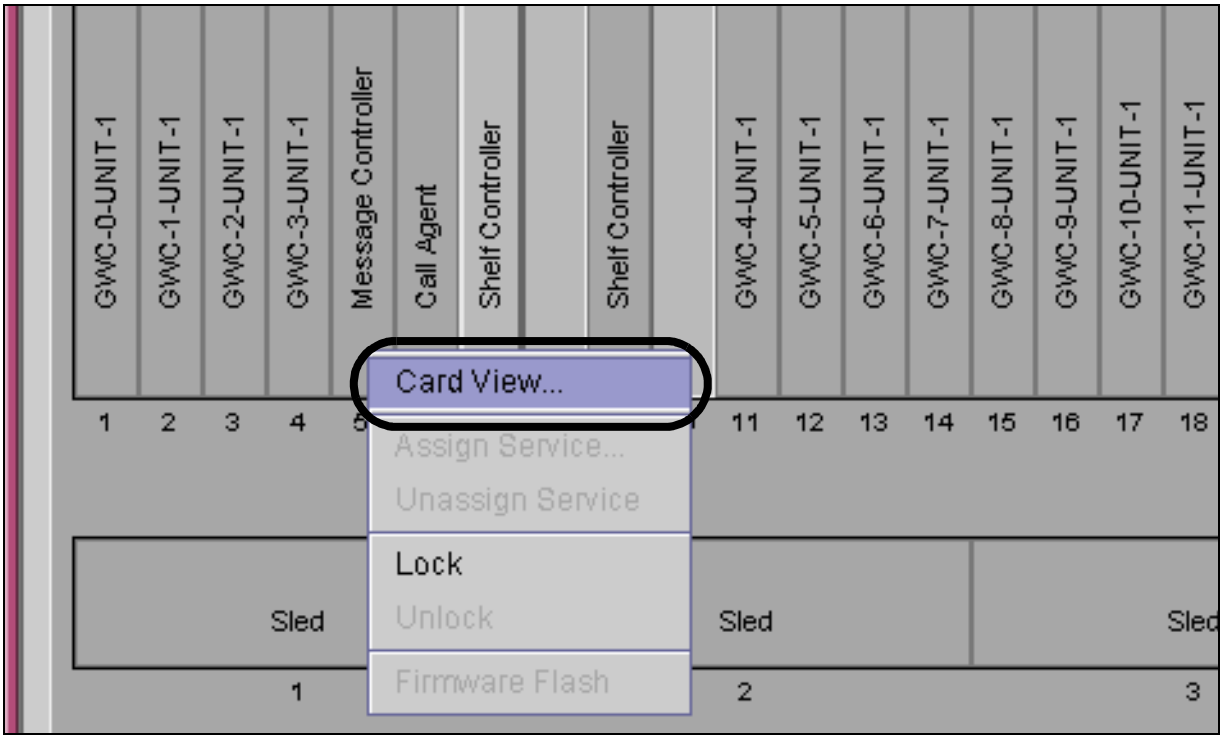
```
10.40.54.61 mc1
```

5 Start the Call Agent Manager interface again:

```
[mtc@hostname mtc]$ ccamtc mcmtc
```

***At the CS 2000 SAM21 Manager client***

6 From the Shelf View, right click on the card and select Card View.

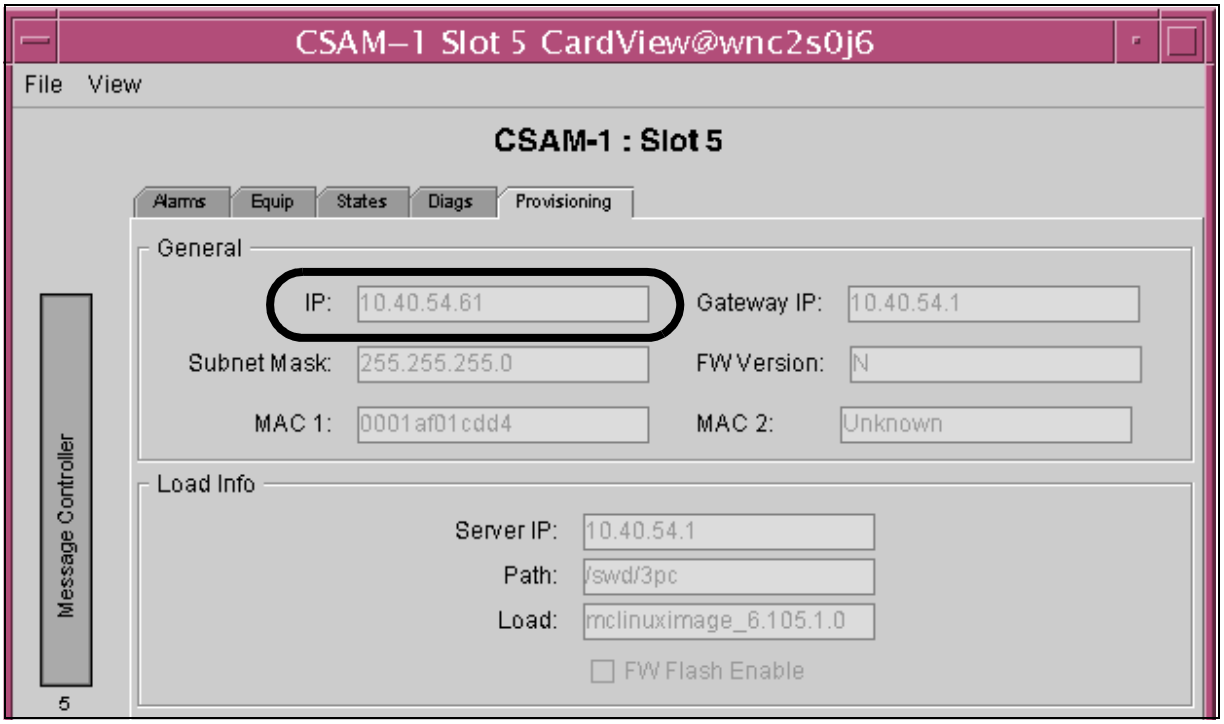



*The Card View window opens.*

7 Select the Provisioning tab on the Card View window.

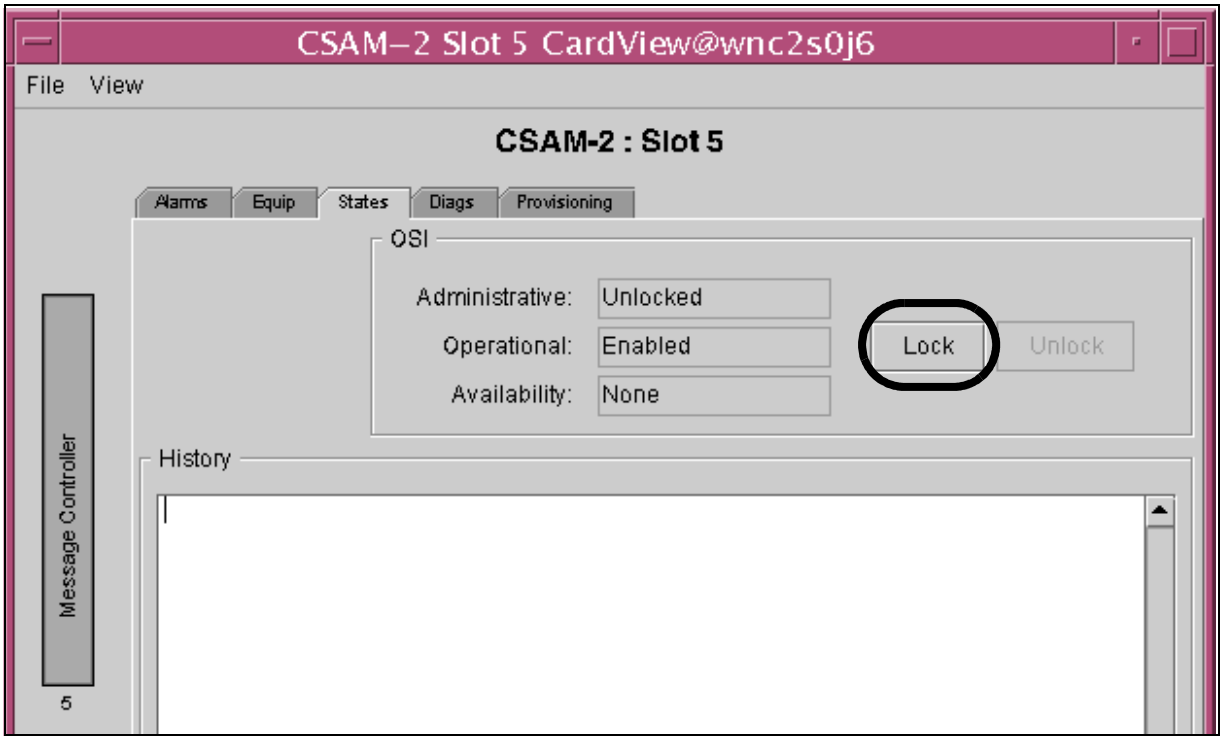
Ensure that the IP address specified in the IP field matches the IP address of Message Controller 1. If the values do not match,

open a different Shelf View from the CS 2000 SAM21 Manager and check the Message Controller provisioning for that shelf.



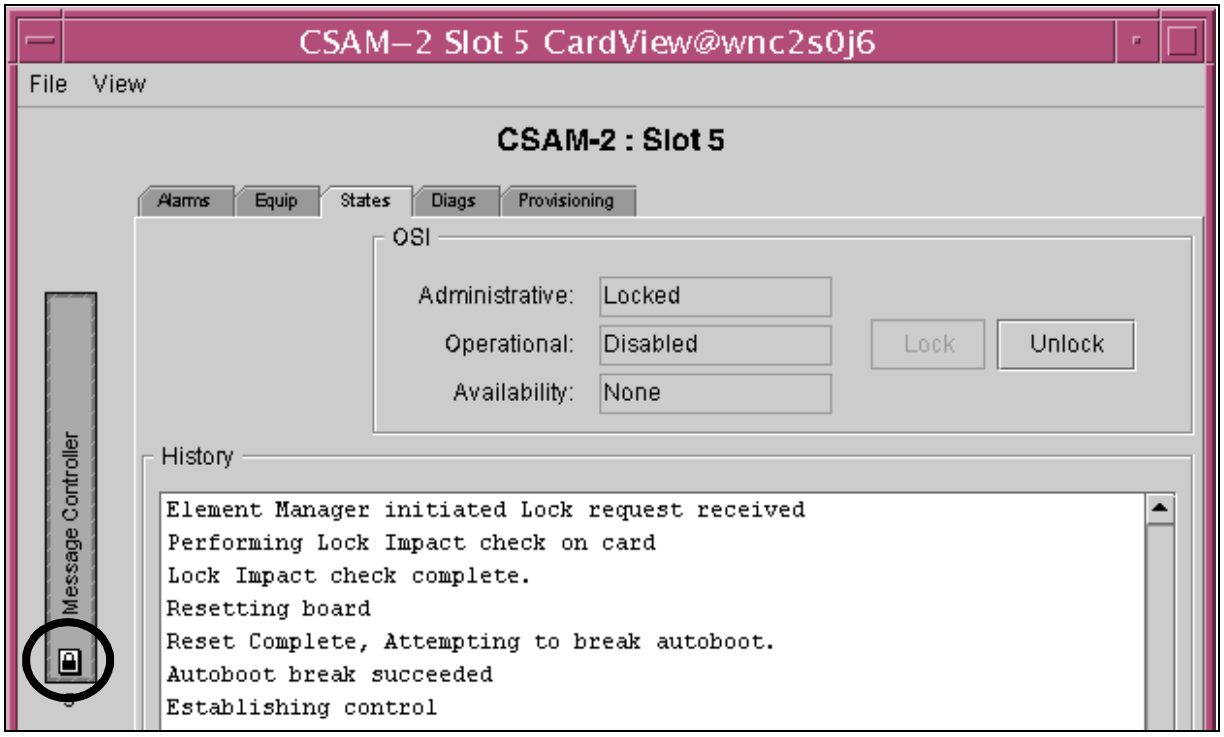

**8** Click on the States tab.

Click on the Lock button.



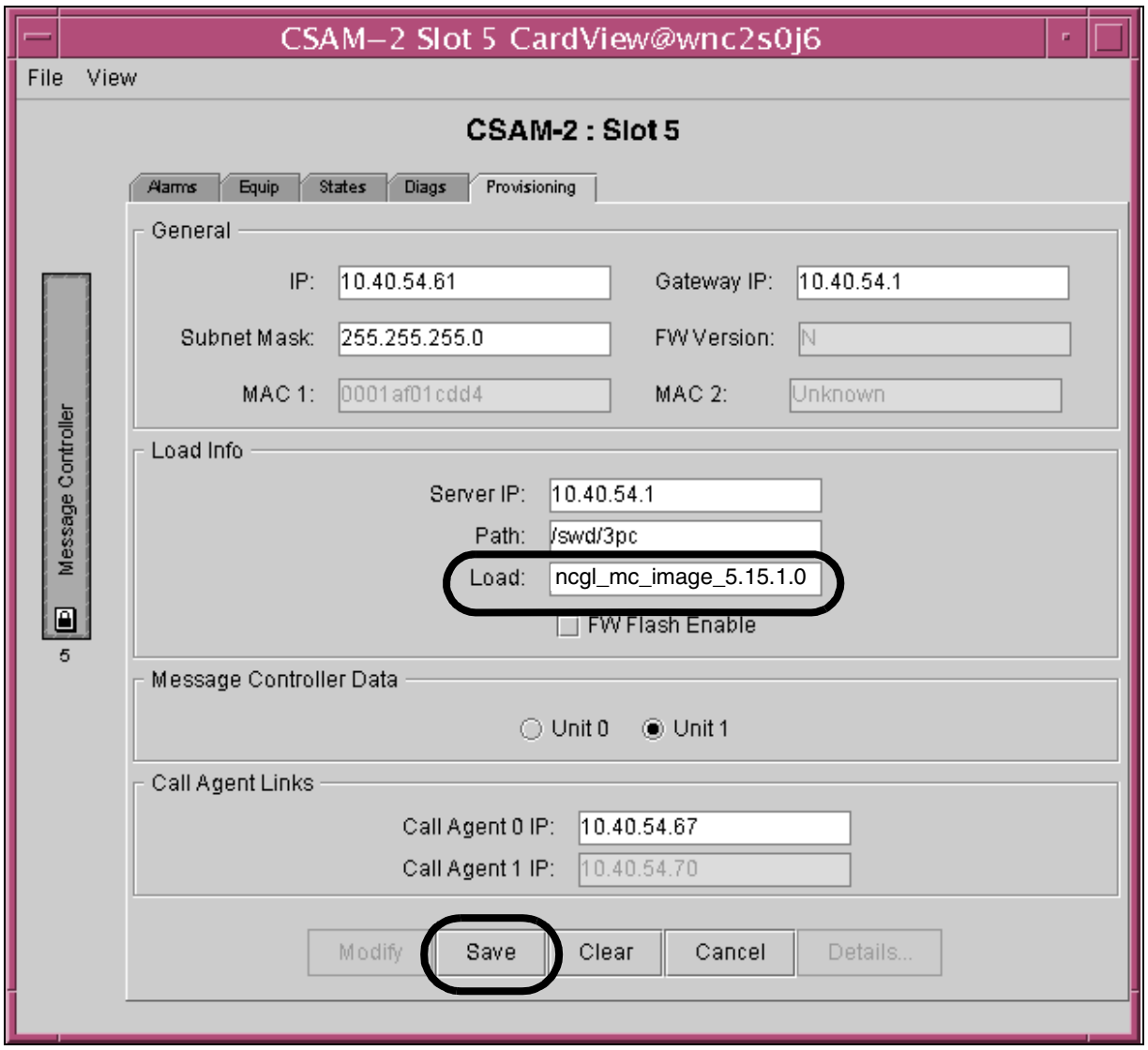

*A lock warning dialog window opens. Confirm the lock warning.*

**9** Wait for the lock icon to appear on the card icon.



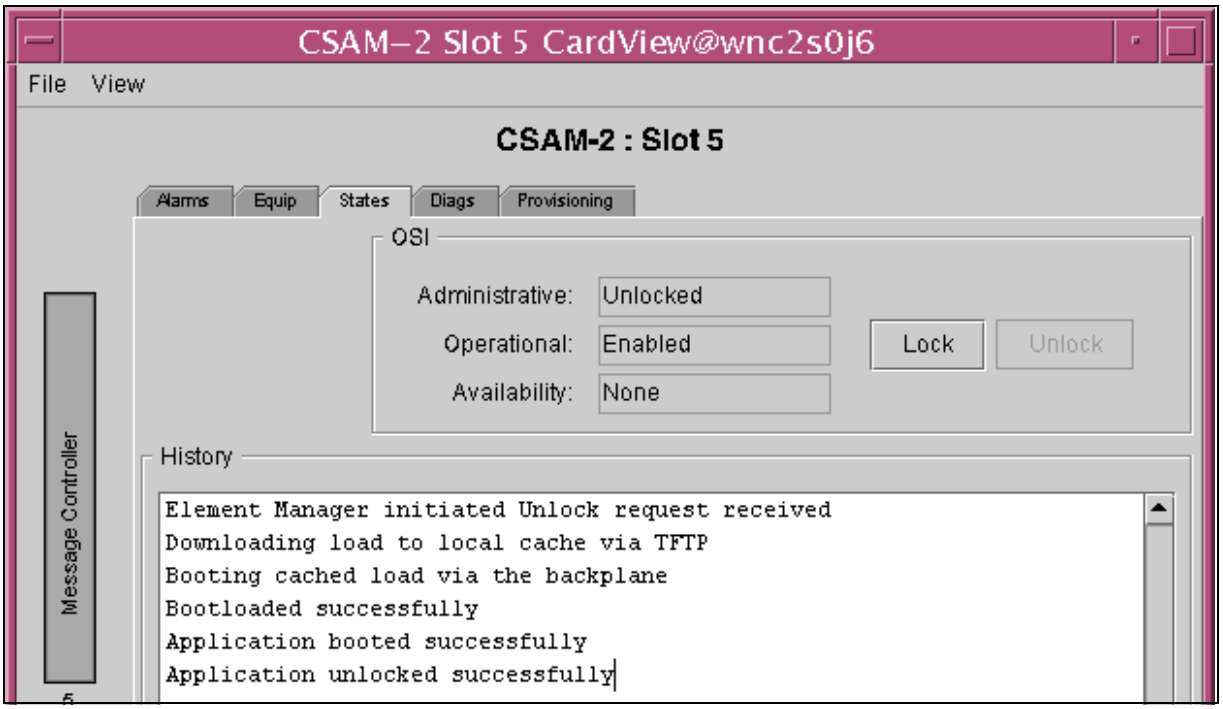

*At the Call Agent Manager, a major ATM alarm is raised, the Message Controller enters the Remote Busy (R) state and is reported as out of service.*

**10** Click on the Provisioning tab, click on Modify, change the Load value to the new software load name, and click Save.



**11** 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***

**12** Query the software load for Message Controller 1 and ensure that the new load is reported:

```
>QryLd 1
```

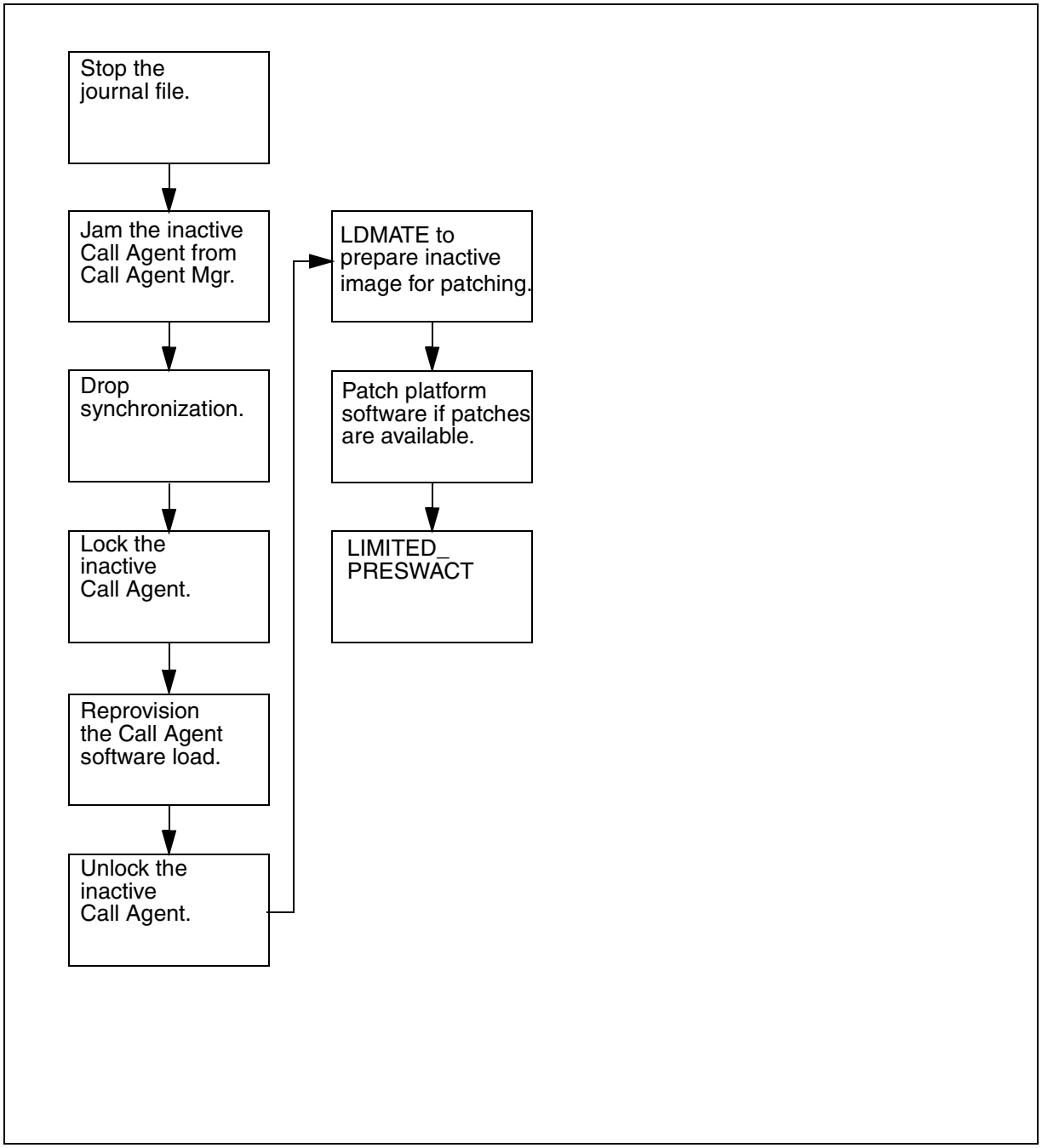
```
  CallAgent       SYS       CON       APPL       MC      Unit: 0
    .             .         .         .          .

MCMtc             Blade:    Eth0:      Eth1:      Atm0:      Atm1:
 0 Quit      MC0    .       . Act      . Inact    open       open
 2           MC1    .       . Act      . Inact    open       open
 3
 4
 5 QryLd
 6 QryHits
 7 ClrHits
 8 Trnsl
 9
10
11
12
13 LogQuery
14 Alarm
15
16           MC Load report retrieved on Thu Jun 19 14:15:54 2004:
17 Help
18 Refresh         Ramdisk: ncgl_mc_image_5.15.1.0
  mtc
Time  13:48  >
```

*Soak the load for 10 minutes while monitoring log reports.*

# Boot new platform software

Perform the procedures in this section as a part of a platform only MR upgrade.

**Boot new platform software**



## Stop the journal file

***At the MAP***

1 Enter the device independent recording package (DIRP) level and query journal file activity:

```
> MAPCI;MTC;IOD;DIRP;QUERY JF ALL
```

2 Stop all journal file activity:

```
> JF STOP
```

3 Close the active journal file and confirm the prompt:

```
> CLOSE JF ACTIVE
> YES
```

4 Query the journal file again to verify rotation of the storage:

```
> QUERY JF ALL
```

5

**ATTENTION**

SERVORD activity, OSSgate activity, and table changes are not permitted.

Inform all operating company personnel that data changes such as SERVORD, OSSgate, and table changes must be halted until after the upgrade is completed. Data changes made during the software upgrade can cause ONP process problems and may result in lost data on the restored side.

This procedure is complete.

# Jam the inactive Call Agent

***At the active Call Agent Manager***

**1** Issue the Jam command:

```
> CoreMtc
> CAMtc
> Jam
```

```
CallAgent       SYS       CON       APPL              Unit: 0
 JInact          .         .         .

CAMtc                      Jam:  Link0:  Link1:  Ser: FC: Appl:
 0 Quit       Unit0  Act    no    . Inact . Act    .   .   insync .
 2 Jam        Unit1  Inact  yes   . Inact . Act    .   .   insync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16          Jam:      Jam the inactive unit, to prevent it taking activity.
17 Help                Parms: [FORCE]
18 Refresh                FORCE     - bypass system stability checks
  mtc
Time  10:38  >
```

*A JInact alarm appears in the alarm banner under CallAgent.*

**2** This procedure is complete.

# Drop application image synchronization

***At the active Call Agent Manager***

**1** Enter the DpSync command:

```
> CoreMtc
> Appl
> DpSync
```

```
CallAgent       SYS       CON       APPL              Unit: 0
 JInact          .         .       simplx
                                     M
Appl                        Jam:  Link0:  Link1:  Ser: FC: Appl:
 0 Quit       Unit0  Act    no     . Inact . Act     .   NA  nosync .
 2 ImgTst     Unit1  Inact  yes    . Act   . Inact   .   NA  nosync /restart
 3 Sync
 4 DpSync
 5
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP   DpSync:   Drop application synchronization.
16                     Parms: [RestartType]
17 Help                   Restart   - ( WARM | COLD | RELOAD | NORESTART )
18 Refresh                (default) -  COLD
  mtc
Time  12:25
```

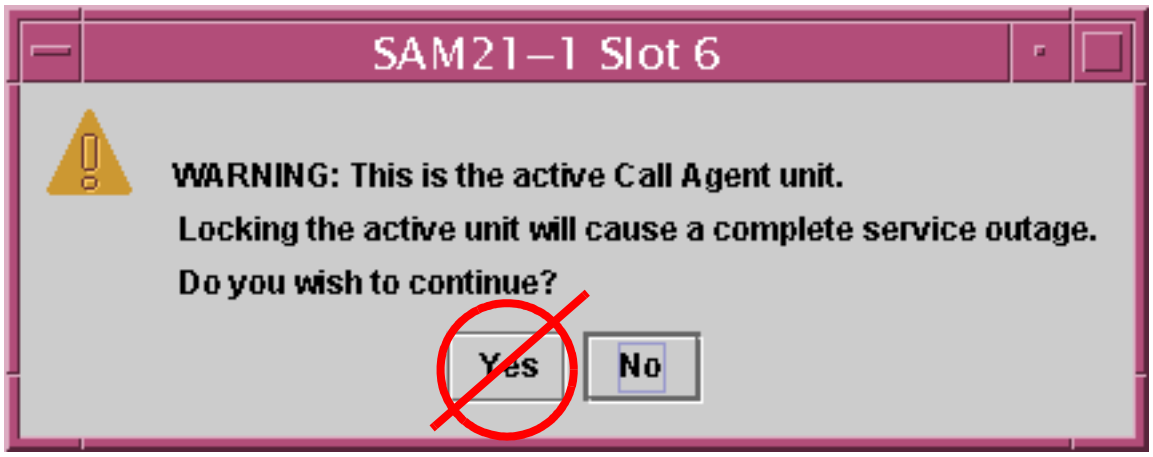
**2** This procedure is complete.

# Call Agent Lock

**CAUTION**
**Possible service interruption**
Do not lock the active Call Agent.

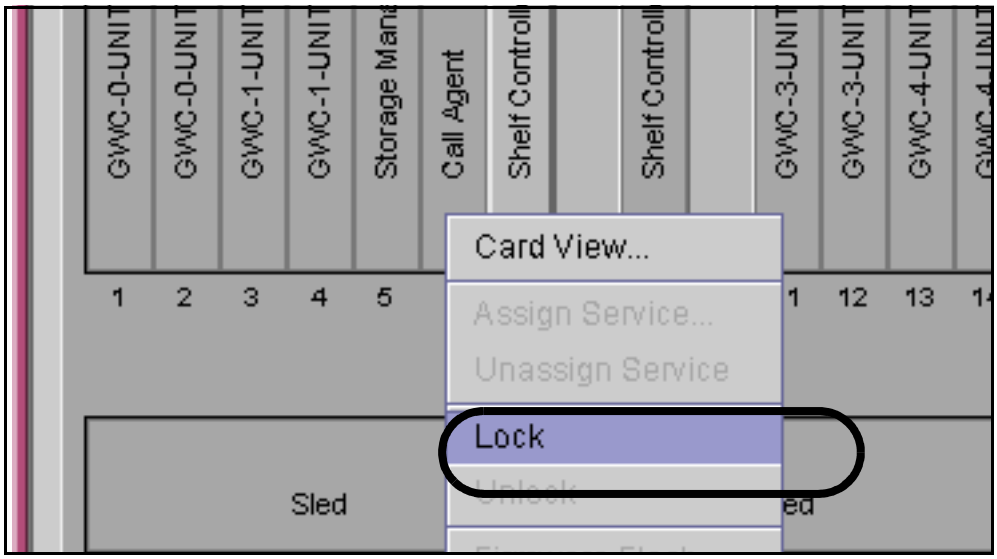
The CS 2000 SAM21 Manager client responds to an active Call Agent lock with the prompt show in figure Call Agent lock warning. Do not click Yes. The inactive Call Agent is located in the other CS 2000 SAM21 Manager shelf and a lock request does not provide a prompt when the Call Agent is inactive.

**Call Agent lock warning**



***At the CS 2000 SAM21 Manager client***

**1** From the Shelf View, right click on the card and select Lock from the context menu.




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

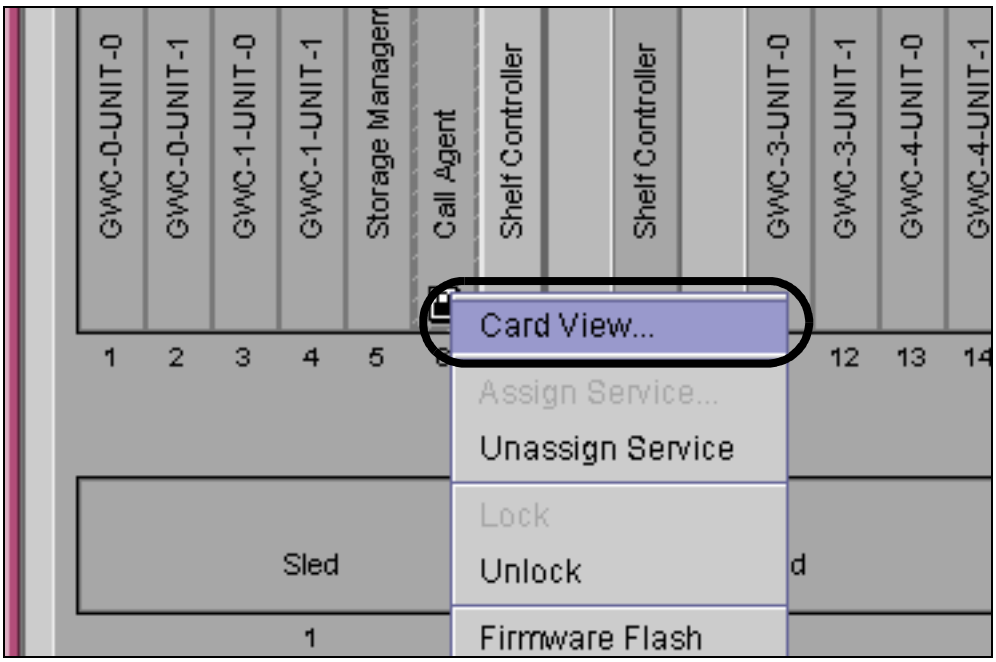
**2** Do not confirm a lock warning. The warning is only available for the active Call Agent. Wait for the lock icon to appear on the selected card.

**3** This procedure is complete.

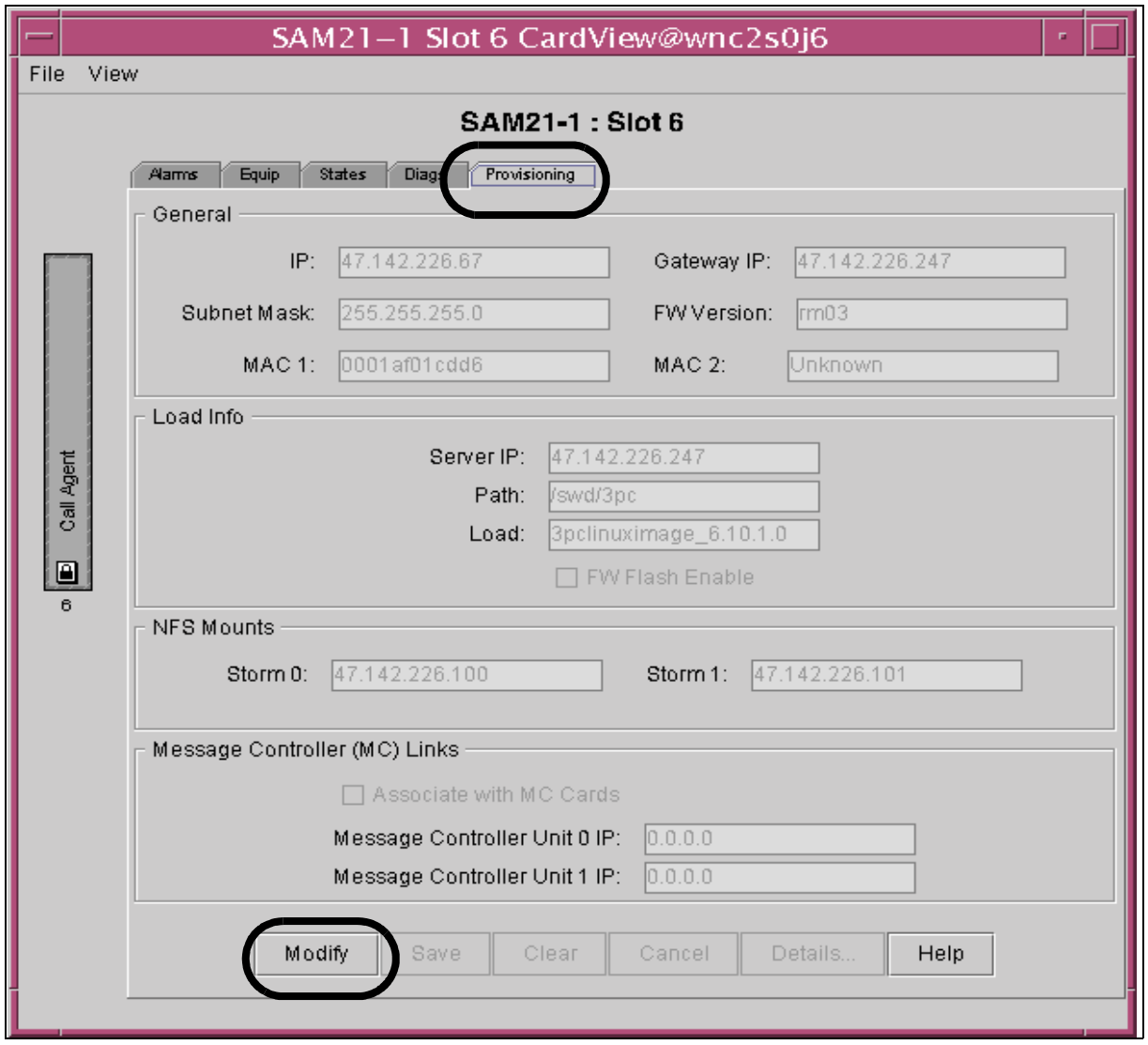
# Reprovision Call Agent platform load

***At the CS 2000 SAM21 Manager client***

**1** From the Shelf View, right click on the card and select Card View from the context menu to open the Card View window.

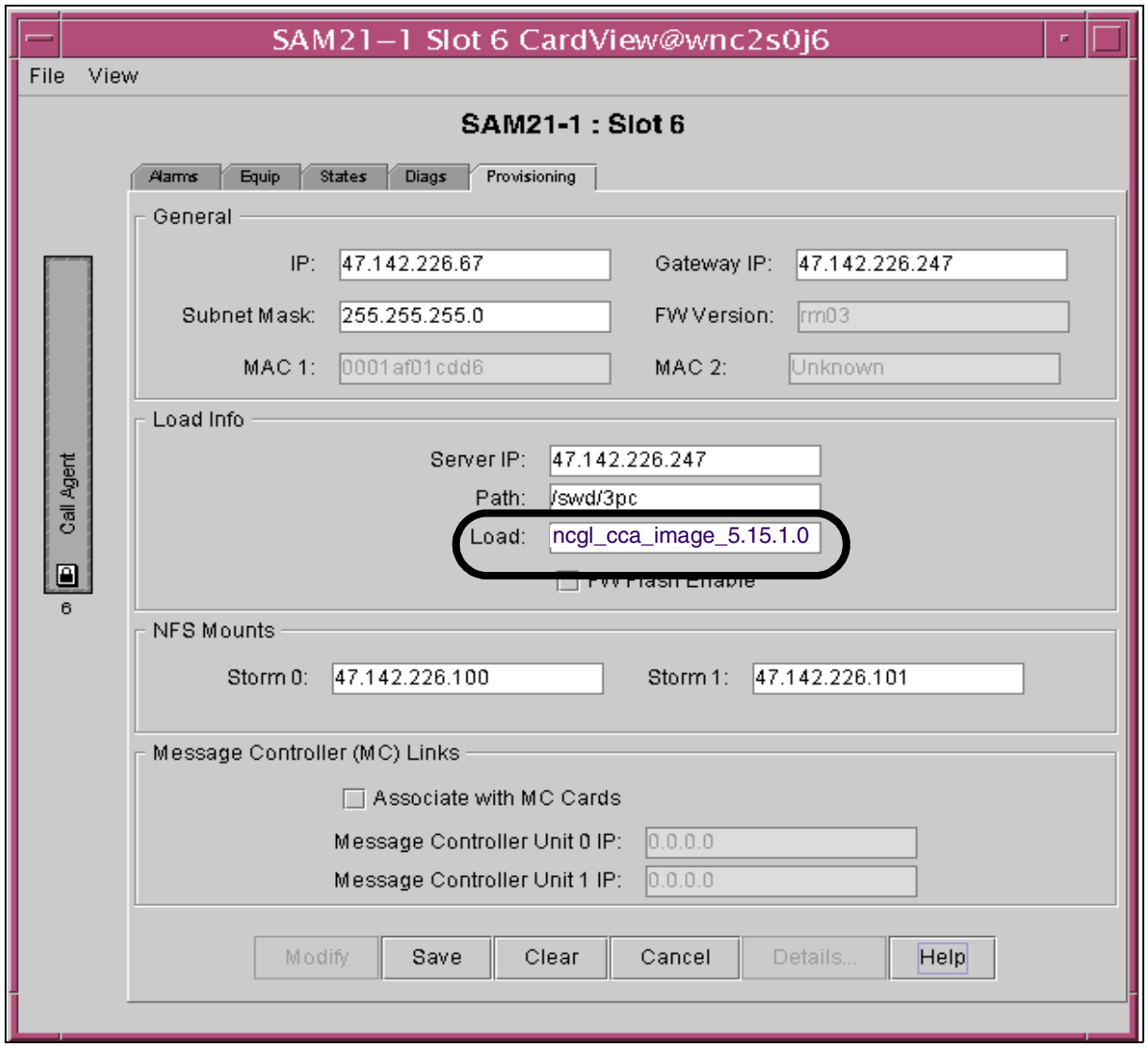


**2** Click the Provisioning tab from the Card View window.




**3** Click the Modify button.

**4** Enter the new load file name in the load field.




***Note:*** Click the firmware flash enable (FW Flash Enable) checkbox if the *SAM21 Platform Base Release Notes* indicate a firmware upgrade is available. However, there is no consequence if the checkbox is enabled and firmware is not available. If a firmware flash upgrade is available, verify that "Firmware flash: succeeded" is reported in the History area of the States tab during the Unlock.

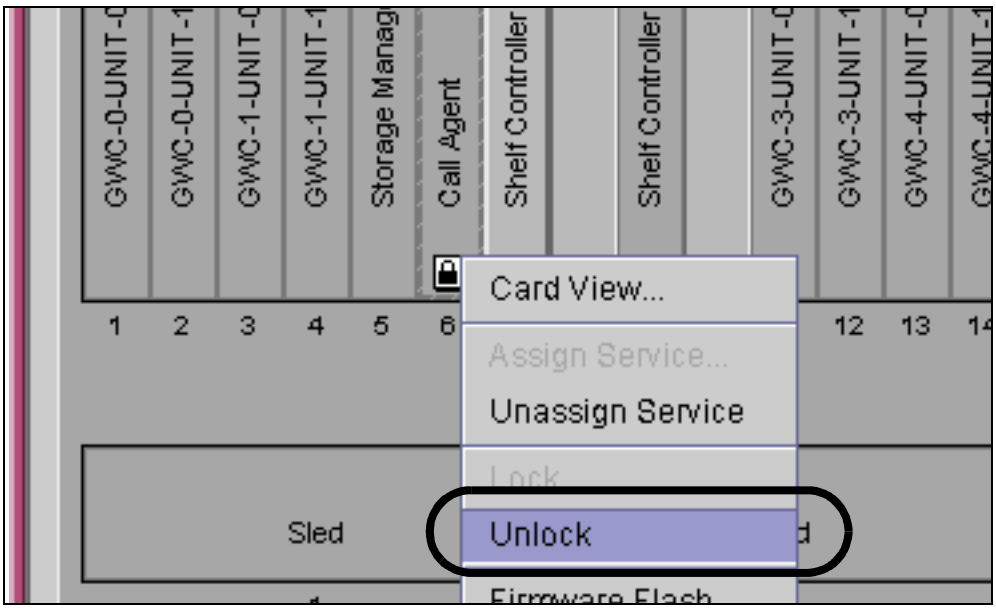
**5** Click the Save button.

**6** This procedure is complete.

# Call Agent Unlock

***At the CS 2000 SAM21 Manager client***

**1** From the Shelf View, right click on the card and select Unlock from the context menu.




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

The card resets, downloads software, and reboots.

**2** Wait for the lock icon to disappear.

***Note:*** Do not perform any patching activities on the Call Agent until ten minutes have passed.

**3** This procedure is complete.

# LDMATE (Load inactive)

This procedure is used for a platform only MR upgrade. Use the LDMATE command to load the currently running and active call processing application onto the inactive Call Agent.

***At the active Call Agent Manager***

**1**

**ATTENTION**

Wait for the synchronization flag to change to `/waiting` before proceeding.

**CAUTION**

**Possible data loss**

When performing the LDMATE command, ensure that the image dump taken during procedure Dump call processing application image on page 77 is the image that is loaded.

Loading any other image may result in a data loss.

Verify that the call processing application is set to `/waiting`:

```
CoreMtc                 Jam:    Link0:  Link1:  Blnk: FC: Appl:
 0 Quit    Unit0 Inact yes      . Act   . Inact   .   S   nosync /waiting
 2 CAMtc   Unit1 Act   no       . Act   . Inact   .   S   nosync
```

***SDE — At the ACTIVECM window***

**2** Make the call processing application file available by listing the image volume:

**`> SCANF <volume_name>`**

**volume_name**
is the name of the volume that contains the image dump. For example, SD00IMAGE.

3 Load the image that was dumped during step 3, page 77 onto the inactive Call Agent:

```
> LDMATE <filename>
```

**filename**
is the name of the call processing application image that was dumped earlier

**Example**
**> LDMATE S040210210503_CM**

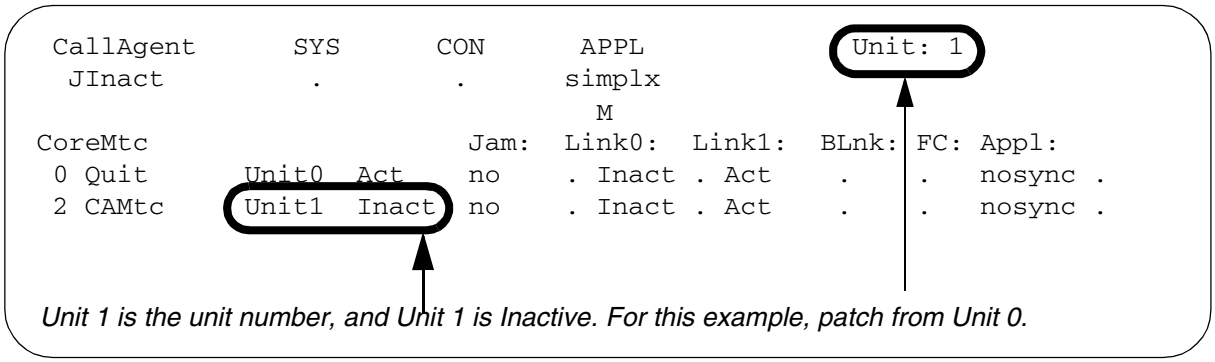
4 Monitor the progress at the MAP and Call Agent Manager windows. At the Call Agent Manager, the synchronization flag for the inactive Call Agent should change from `/booting` to `/restart`.

5 This procedure is complete.

# Patch platform software

***At the inactive Call Agent Manager***

**1** At the CoreMtc level, ensure that this unit is the inactive unit.




*Unit 1 is the unit number, and Unit 1 is Inactive. For this example, patch from Unit 0.*

**2** Enter the Transfer level and display the list of available patches.

```
> Transfer
```

*The Call Agent Manager enters the **Transfer** level and the list of available patches is retrieved and displayed.*

```
 CallAgent       SYS       CON       APPL             Unit: 0
  JInact          .         .       simplx
                                      M
Transfer      Current Load : 5.15.1.0
 0 Quit       Source       : /3pc/patch
 2 Select
 3 Fetch       # Patch Description                    Version
 4 Source      1 ncgl_cca_patch                      5.15.1.35
 5             2 ncgl_cca_patch                      5.15.1.34
 6
 7
 8
 9
10
11 Up
12 Down
13 LogQuery
14 Alarm
15                                  Filesets on the source: 1 to 2 of 2
16
17 Help
18 Refresh
  mtc
Time  10:52  >
```

**3** If no patches are listed, verify that the selected source, `/3pc/patch` in the example, is correct. If the source is correct and no patches are available, this procedure is complete.

**4** For each patch to be transferred, select the patch by number and transfer the patch to the inactive unit.

```
> Select <num>
> Fetch INA
```

**5** Enter the Patch level.

```
> Patch
```

*The Call Agent Manager enters the **Patch** level and the patches are listed as NEW.*

```
 CallAgent       SYS       CON       APPL             Unit: 0
  JInact          .         .       simplx
                                       M
Patch          Current Load : 5.15.1.0
 0 Quit        Filter       : ALL
 2 Select
 3 Apply        # Patch Description                    Version        Status
 4 Delete       1 Patch description                    5.15.1.35      NEW
 5 Commit       2 Patch description                    5.15.1.34      NEW
```

**6** For each patch file, select the patch, apply the patch to the inactive unit, select it again, and commit it.

```
> Select <num>
> Apply INA FORCE
> Select <num>
> Commit INA
```

*Each patch is applied and committed to the inactive Call Agent unit. The Status for each patch changes from NEW to COMMITTED.*

**7** The application of patches is complete.

## Perform LIMITED_PRESWACT

This procedure is used for a platform only MR upgrade. For an ONP, Nortel Networks supports the SWUPGRADE process.

LIMITED_PRESWACT executes a series of steps required before the office switch of activity (SWACT). If a step fails to complete, LIMITED_PRESWACT stops and gives additional information. Whenever LIMITED_PRESWACT stops, use the information given to investigate and correct the problem. All LIMITED_PRESWACT steps must be completed before SWACT.

***At the MAP***

**1** Execute LIMITED_PRESWACT:

```
> BCSUPDATE; LIMITED_PRESWACT
```

*The LIMITED_PRESWACT command presents a warning:*

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

**2** Confirm the warning with a **Y**.

*A series of steps execute and complete. LIMITED_PRESWACT stops at step MATE_RESART_RELOAD:*

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

**3** Reenter LIMITED_PRESWACT to continue:

```
> LIMITED_PRESWACT
```

*Another warning is printed:*

```
MATE_RESTART_RELOAD                executing
There are users still logged on the Inactive. Do
you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
```

**4** Confirm the warning with a **Y**.

*The inactive unit indicates* `/restart` *at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated as follows:*

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

**5** This procedure is complete.

# Release jam on the inactive Call Agent

***At the active Call Agent Manager***

**1** Enter the RelJam command:

```
> CoreMtc
> CAMtc
> RelJam
```

```
 CallAgent       SYS       CON       APPL              Unit: 0
    .             .         .       simplx
                                       M
CAMtc                        Jam:  Link0:  Link1: BLnk: FC: Appl:
 0 Quit       Unit0  Act     no     . Inact . Act     .    .   nosync .
 2 Jam        Unit1  Inact   no     . Inact . Act     .    .   nosync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh    RelJam:   Release jam on the inactive unit.
  mtc
Time  10:38  >
```

**2** This procedure is complete.

# Execute NORESTARTSWACT

**CAUTION**
**Possible loss of service**
NORESTARTSWACT does not check if the inactive Call Agent is unjammed. If the inactive Call Agent is jammed and a NORESTARTSWACT is requested, service is affected. Verify that the inactive Call Agent is not jammed.

**CAUTION**
**Possible loss of service**
Use the Call Agent Manager to verify that the inactive Call Agent does not have any critical alarms. A critical alarm causes the NORESTARTSWACT to fail.

***At the MAP***

**1** Check status:

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

*Success is indicated as follows:*

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

**2** Execute the NORESTARTSWACT:

```
> NORESTARTSWACT
```

***Note 1:*** Only simple two-port and echo calls that are in a stable talking state (that is, not in a transition state such as dialing) survive a CC WarmSWACT. Survival means that the call is kept up until the next signaling message is received (usually, for example, a terminate message, but on any other message as well, such as an attempt to use the conference feature).

***Note 2:*** Attendant Consoles will be in night service after the SWACT if the INSV field is set to Y in table ATTCONS (Attendant Consoles).

*Progress is printed and the process stops to verify that the inactive Call Agent is not jammed:*

```
Beginning SWACT checks:
All the SWACT checks have finished successfully.
The VR_PRESWACT_TRANSFER step completed
successfully.
All INSV and ISTB series 1 PMs will have execs
loaded after the SWACT.
Device Checking Status:
NOMATCH option is set to OFF <default setting>.
Device matching during CC WARM SWACT Enabled.
Do you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
>
```

**3** Confirm the warning with a **Y** if the only alarm is an APPL simplx.

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

```
Please confirm ("YES", "Y", "NO", or "N"):
>Y
All Pre-SWACT checks completed. Starting Warm
SWACT now.
*****   The cursor will not be returned  *****
*****  unless a critical failure occurs. *****
***** Now monitoring Warm SWACT messages.*****

Pre-initialization done
Communication established
Exchange of data with the mate done
Transfer of data done (FASPECT)
Data estimation done
```

**4** The telnet sessions to the active and inactive call processing applications are lost. Reestablish the connection. Refer to the Interface setup in this Upgrades document for procedures.

5 This procedure is complete.

**ATTENTION**

**ABORT PROCEDURE**

Reversion to the previous software release is possible until procedure Lock the inactive Call Agent. If this is a PCL upgrade with the SWUPGRADE tool, reversion is started with the CANCEL command. If this is a platform only MR upgrade, refer to ABORTSWACT on page 218.

# Jam the inactive Call Agent

***At the active Call Agent Manager***

**1** Enter the Jam command:

```
> CoreMtc
> CAMtc
> Jam
```

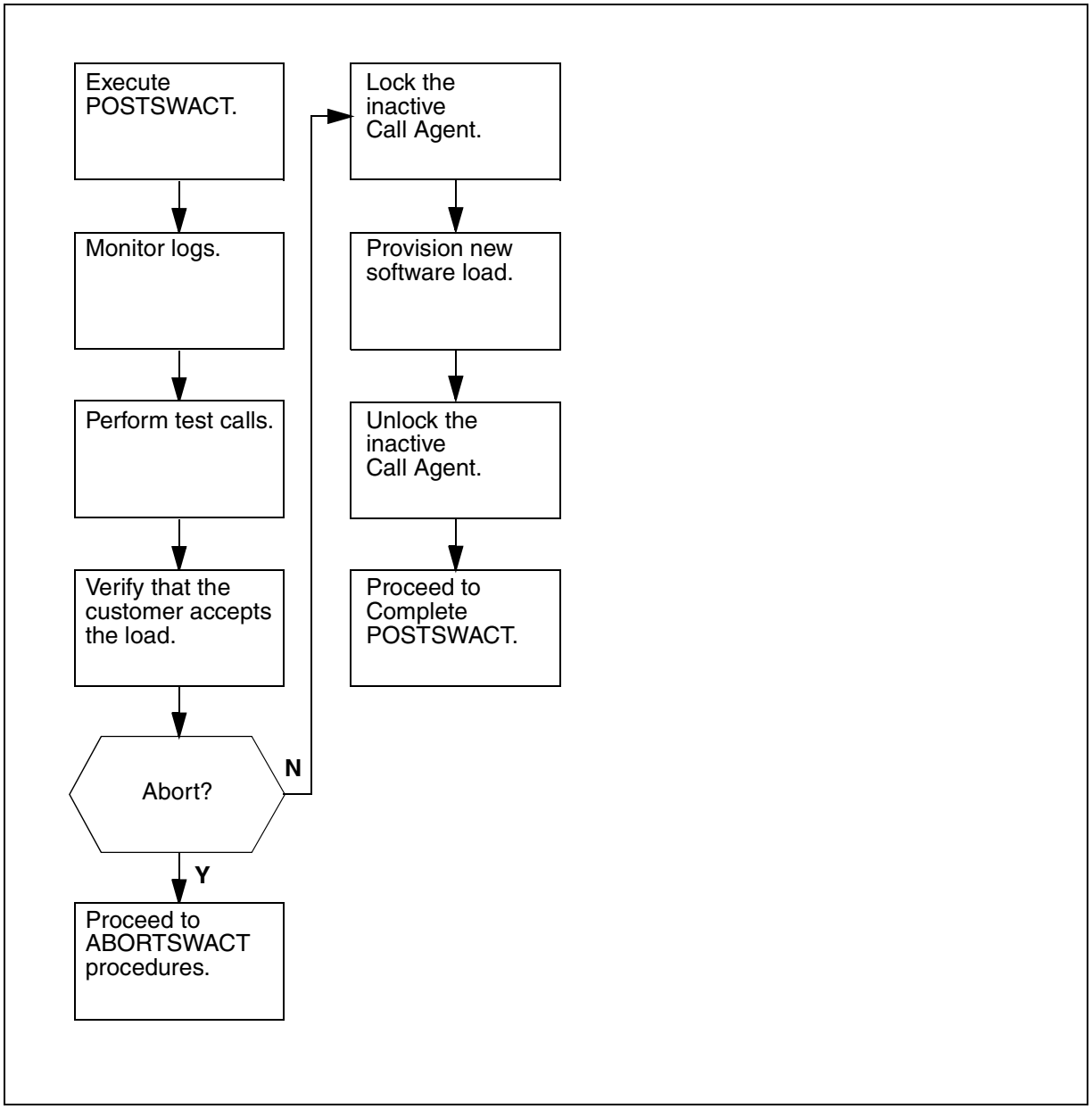
```
CallAgent       SYS       CON       APPL              Unit: 1
 JInact          .         .       simplx
                                     M
CAMtc                       Jam:  Link0:  Link1:  BLnk: FC: Appl:
 0 Quit       Unit0  Inact  yes    . Inact . Act     .    .   nosync .
 2 Jam        Unit1  Act    no     . Inact . Act     .    .   nosync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16           Jam:      Jam the inactive unit, to prevent it taking activity.
17 Help                 Parms: [FORCE]
18 Refresh                 FORCE     - bypass system stability checks
  mtc
Time  10:38  >
```

**2** This procedure is complete.

# Start POSTSWACT

Perform the procedures in this section to verify the stability of the new platform software load.

**Start POSTSWACT procedure**



# Execute POSTSWACT

***At the MAP***

**1** Execute POSTSWACT:

```
> BCSUPDATE;POSTSWACT
```

*POSTSWACT begins, steps execute, and complete. POSTSWACT stops at step BEGIN_TESTING:*

```
REACTIVATE_TRIGASGN                executing
REACTIVATE_TRIGASGN                   complete

DIRP_RECOVERY                      executing
DIRP_RECOVERY                      complete
...
BEGIN_TESTING                      executing
BEGIN_TESTING                      complete
Enter Postswact after office testing has been
completed
```

**2** Proceed to Monitor logs on page 205 and Test calls and acceptance on page 207 before reentering the **POSTSWACT** command on page 214.

## Monitor logs

***At the inactive MAP***

1 Log in to the mate image, refer to How to log in to the mate image.

2 Review previous log reports:

```
> LOGUTIL;OPEN SWCT;BACK ALL
```

3 Set the terminal to receive logs:

```
> LOGUTIL;START;QUIT
```

or

```
> STARTDEV <device>
```

**device**
is a different terminal device

4 Let logs run for 30 minutes and then run LOGCHECK:

```
> LOGUTIL;STOP;QUIT
> BCSUPDATE;LOGCHECK;QUIT
```

5 When LOGCHECK completes. Set the terminal to receive logs again.

6 This procedure is complete.

## How to log in to the mate image

***At the MAP***

1 Use MATELINK, MATIO, and MATELOG to log in.

```
> MATELINK RTS
> MATEIO
> MATELOG ME; SLEEP <nn> MINS
```

**nn**
is the number of minutes to sleep. Allow at least 30 minutes.

2

**ATTENTION**
While logged into the inactive call processing application, the system prompt changes to `Mate>`.

Log in to the inactive call processing application with a username and password.

3 This procedure is complete.

## Test calls and acceptance

***At the MAP***

1 Make sure all emergency services are functioning.

2 Refer to the Test Call Scripts and perform the required test calls.

3 Confirm that the customer accepts the new load.

4 This procedure is complete.

Determine the next action.

| If | Do |
|---|---|
| abort is required | proceed to ABORTSWACT on page 218 |
| abort is not required | set the boot file pointer, as described below, and then proceed to Lock the inactive Call Agent on page 208 |

Take an image dump.

Set the boot file pointer to the new software load if this was not done when the software was transferred to storage.

***At the MAP***

1 Dump the new call processing application image.

```
> AUTODUMP MANUAL
```

*or*

```
> DUMP MANUAL image_name disk_vol ACTIVE UPDATE
```

2 Enter the ITOCCI level.

```
> ITOCCI
```

3 Set the boot file pointer to the new software load.

```
> SA CM image_name
```

**image_name**
is the name of the new call processing application image from step 1

4 This procedure is complete.

## Lock the inactive Call Agent

**ATTENTION**

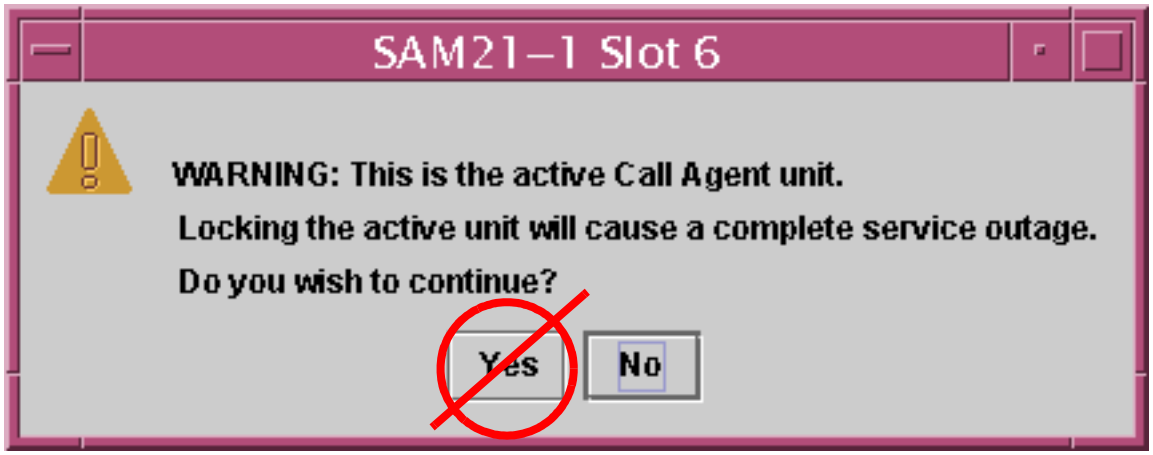
Verify that the customer accepts the new load.

ABORTSWACT is no longer available after this procedure. ABORTSWACT is the preferred method to revert a platform only upgrade. Reversion is still possible after this procedure, but requires assistance from Nortel Networks support personnel.

**CAUTION**
**Possible service interruption**
Do not lock the active Call Agent.

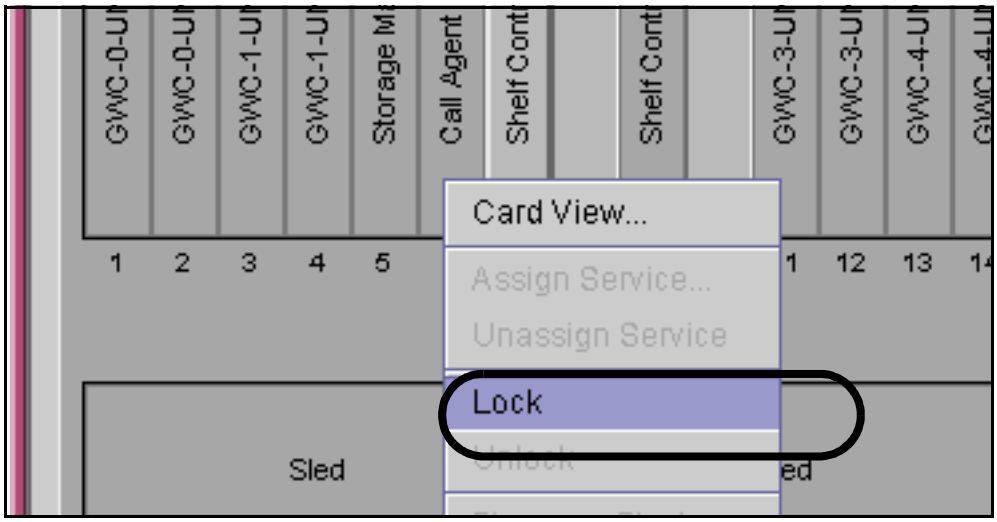
The CS 2000 SAM21 Manager client responds to an active Call Agent lock with the prompt shown in figure Call Agent lock warning. Do not click Yes. The inactive Call Agent is located in the other SAM21 shelf and a lock request does not provide a prompt when the Call Agent is inactive.

**Call Agent lock warning**



***At the CS 2000 SAM21 Manager client***

**1** From the Shelf View, right click on the card and select Lock from the context menu.




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

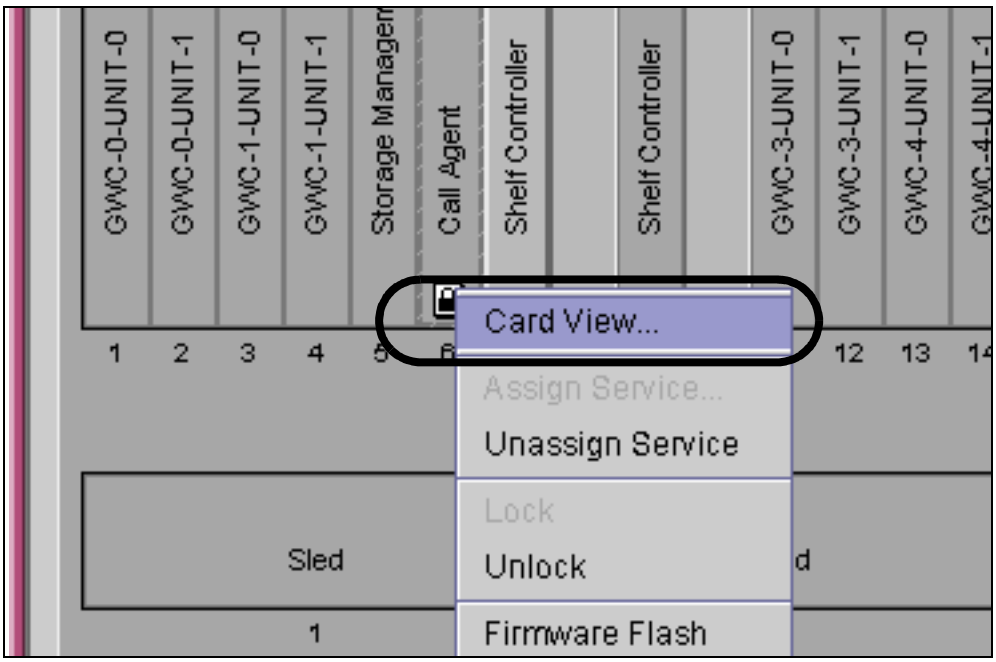
**2** Wait for the lock icon to appear on the selected card.

**3** This procedure is complete.

## Provision new software load

***At the CS 2000 SAM21 Manager client***

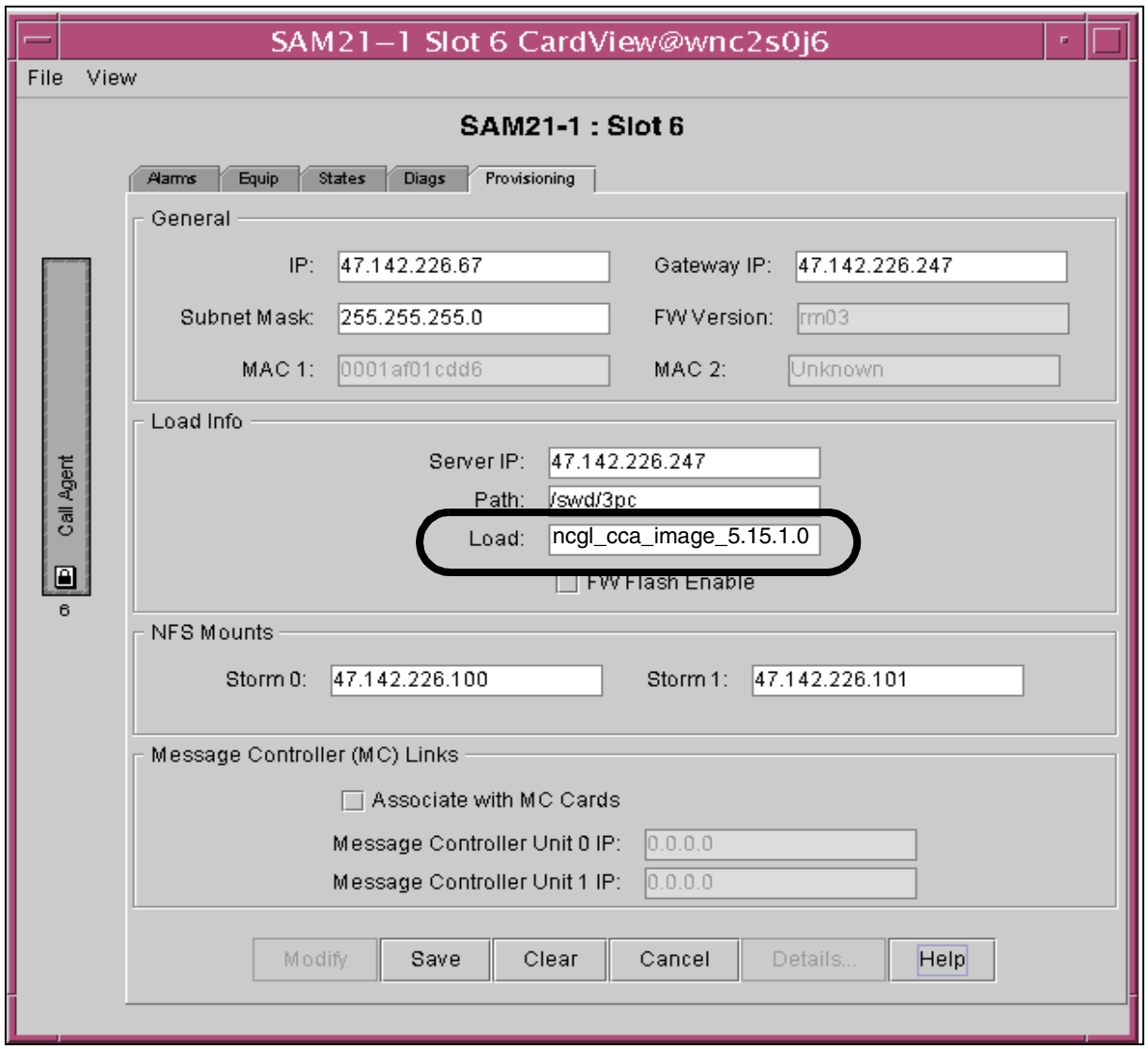
**1** From the Shelf View, right click on the card and select Card View from the context menu to open the Card View window.




**2** Click the Provisioning tab from the Card View window.

**3** Click the Modify button.

4 Enter the new load file name in the load field.




***Note:*** Click the firmware flash enable (FW Flash Enable) checkbox if the *SAM21 Platform Base Release Notes*, SAM2006 indicate a firmware upgrade is available. However, there is no consequence if the checkbox is enabled and firmware is not available. If a firmware flash upgrade is available, verify that “Firmware flash: succeeded” is reported in the History area of the States tab.

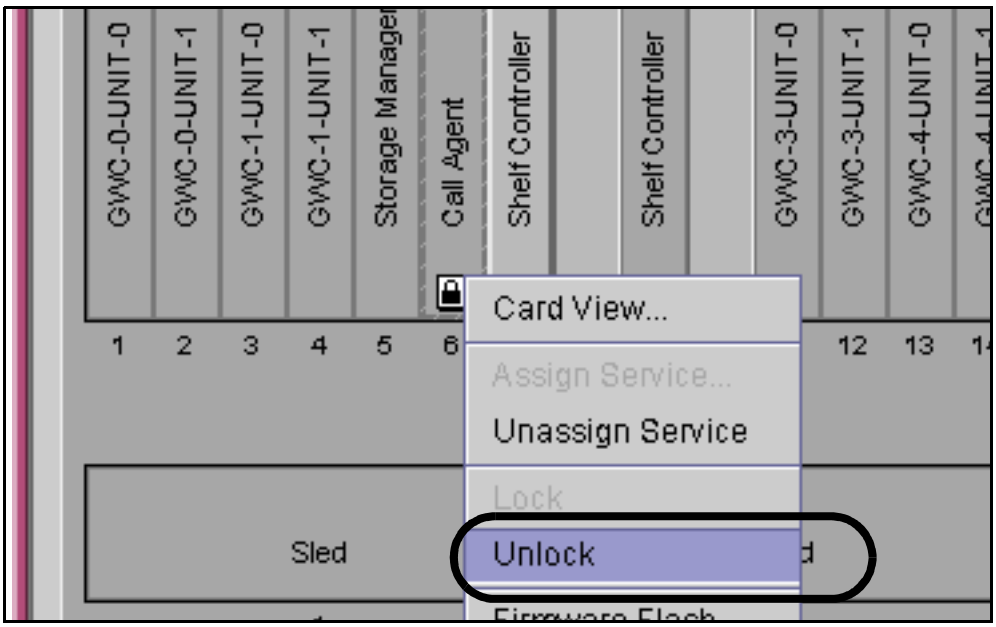
5 Click the Save button.

6 This procedure is complete.

# Unlock the inactive Call Agent

***At the CS 2000 SAM21 Manager client***

**1** From the Shelf View, right click on the card and select Unlock from the context menu.




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

The card resets, downloads software, and reboots.

**2** Wait for the lock icon to disappear.

***At the active Call Agent Manager***

**3** Verify that the call processing application loads successfully and waits for synchronization.

```
CoreMtc                  Jam:    Link0:  Link1:   BLnk: FC: Appl:
 0 Quit    Unit0 Inact yes      . Act   . Inact    S    S   nosync /waiting
 2 CAMtc   Unit1 Act   no       . Act   . Inact    S    S   nosync
```

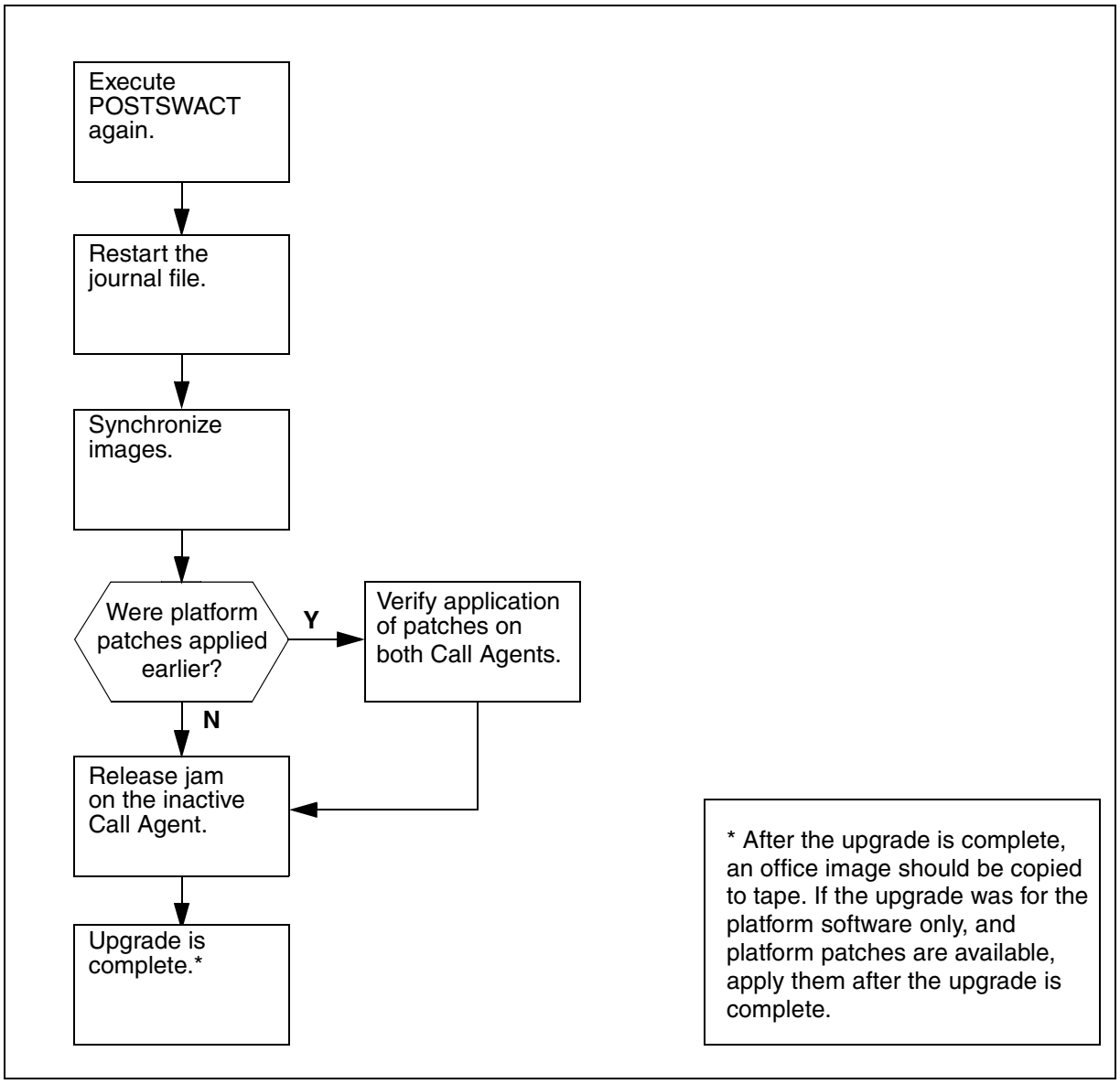
***Note:*** The figure above is used only to show the waiting flag. Disregard the values for activity and jam state.

**4** This procedure is complete.

# Complete POSTSWACT

Perform the procedures in this section to commit the new load. If a revert was required, the procedures in this section complete the reversion.

### Complete POSTSWACT procedure



## Execute POSTSWACT again

***At the MAP***

1 Execute POSTSWACT:

```
> BCSUPDATE;POSTSWACT
```

2 Confirm the prompt to XA_UNSPLIT:

```
> Y
```

3 Clean up SFDEV by erasing any application-related files, such as FEATDATA, SITEINFO, and DIRP_INAC.

Have telephone operating company personnel perform the following procedure.

***At the MAP***

1 Verify passwords for users ADMIN and OPERATOR.

2 Reassign all current PROFILE information (LOGIN or RESTART) in SFDEV.

3 Reassign any temporary log ROUTING setup using LOGUTIL.

4 If table PADNDEV was altered, restore the original values.

5 This procedure is complete.

# Restart journal file

***At the MAP***

1 Access the DIRP level of the MAP:

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

2 Start the journal file:

```
> JF START
```

3 This procedure is complete.

## Verify platform patches

Perform this procedure only if platform patches were applied earlier to the first Call Agent.

***At the active Call Agent Manager***

1. If platform patches are available, platform patches may need to be applied to this Call Agent unit:
2. At the TRANSFER level (**ccamtc transfer** ) a list of available patches is displayed. For each patch:
   - **a** SELECT the patch by number
   - **b** FETCH INA the patch to the INACTIVE unit
3. At the PATCH level, for each patch to be applied and committed:
   - **a** SELECT the patch by number
   - **b** DISADMIN the patch and follow any special instructions
   - **c** APPLY INA the patch to the INACTIVE unit
   - **d** SELECT the patch by number
   - **e** COMMIT INA the patch to the INACTIVE unit
4. Verify that the reported load information is the same for both Call Agents.
5. This procedure is complete.

# Release jam on the inactive Call Agent

***At the active Call Agent Manager***

**1** Enter the RelJam command:

```
> CoreMtc
> CAMtc
> RelJam
```

```
CallAgent       SYS       CON       APPL              Unit: 1
    .            .         .         .

CAMtc                      Jam:  Link0:  Link1:  BLnk: FC: Appl:
 0 Quit       Unit0  Inact  no    . Inact . Act    .    .   insync .
 2 Jam        Unit1  Act    no    . Inact . Act    .    .   insync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh   RelJam:   Release jam on the inactive unit.
  mtc
Time  10:38  >
```

**2** This procedure is complete.

The upgrade is complete. Backup the image taken during procedure Test calls and acceptance on page 207. For the details of how to make the backup, refer to section Backup image on page 79.

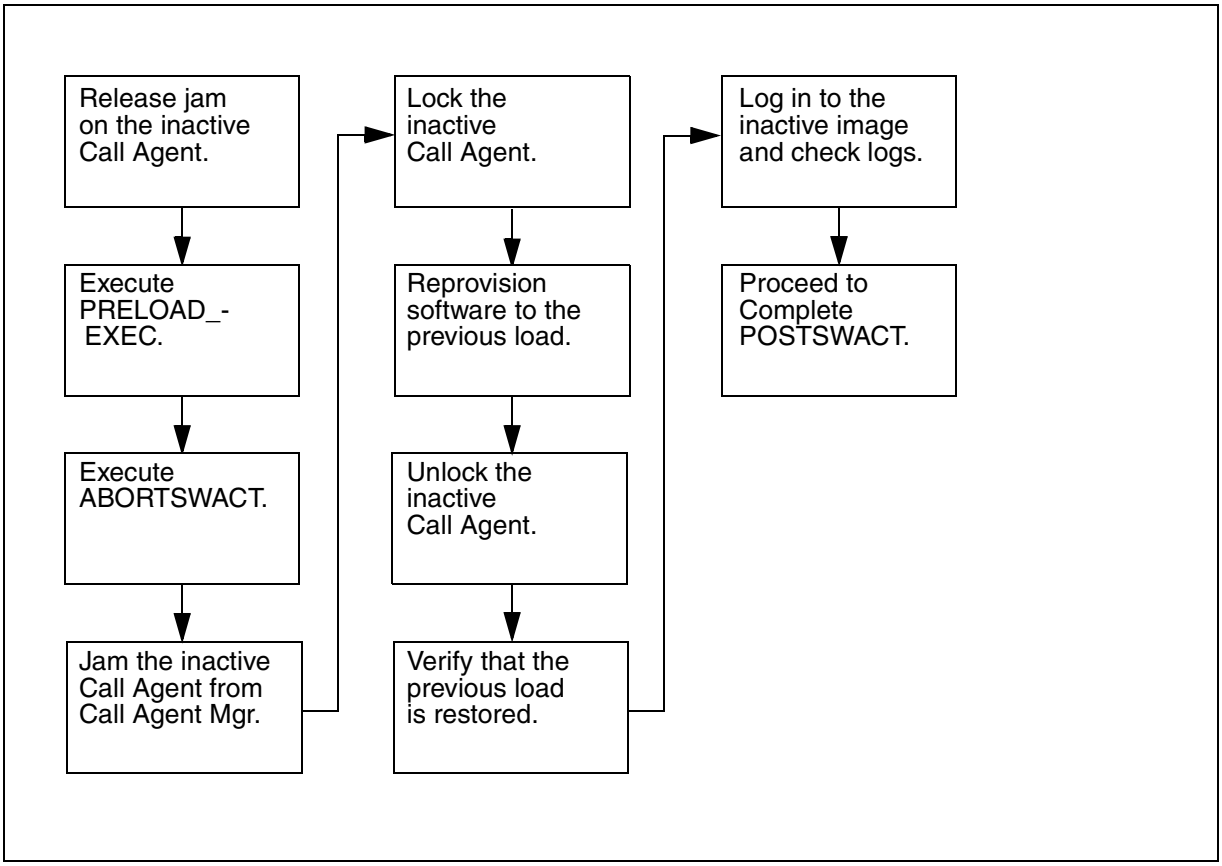
# ABORTSWACT

**CAUTION**
**Possible loss of service**
Reversion with ABORTSWACT is only available if the inactive Call Agent was not locked during “Start POSTSWACT.”

If the inactive Call Agent was unlocked, contact Nortel Networks support personnel for assistance.

Only perform the procedures in this section if the software upgrade fails.

## ABORTSWACT procedure



# ABORT: Release jam on the inactive Call Agent

***At the active Call Agent Manager***

**1** Enter the RelJam command:

```
> CoreMtc
> CAMtc
> RelJam
```

```
CallAgent       SYS       CON       APPL              Unit: 0
    .            .         .       simplx
                                       M
CAMtc                        Jam:  Link0:  Link1:  BLnk: FC: Appl:
 0 Quit       Unit0  Act     no     . Inact . Act     .    .   nosync .
 2 Jam        Unit1  Inact   no     . Inact . Act     .    .   nosync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh    RelJam:   Release jam on the inactive unit.
  mtc
Time  10:38  >
```

**2** This procedure is complete.

# ABORT: Execute PRELOAD_EXECS and ABORTSWACT

### *At the MAP*

**1** Preload the PM executables:

```
> BCSUPDATE;RUNSTEP PRELOAD_EXECS
> SWACTCI;ABORTSWACT
```

### *At the active Call Agent Manager*

**2** Monitor the SWACT.

Verify that the synchronization flags begin with `/restart`, proceed to `/loading`, and then `/waiting`.

Verify that activity switches from active to inactive.

**Before ABORTSWACT**

```
CoreMtc                  Jam:  Link0:  Link1:  BLnk: FC: Appl:
 0 Quit      Unit0  Act  no    . Inact . Act    .    .   insync .
 2 CAMtc     Unit1  Inact no    . Act   . Inact  .    .   insync .
```

**After ABORTSWACT**

```
CoreMtc                  Jam:  Link0:  Link1:  BLnk: FC: Appl:
 0 Quit      Unit0  Inact no    . Inact . Act    .    .   insync .
 2 CAMtc     Unit1  Act   no    . Act   . Inact  .    .   insync .
```

**3** The telnet sessions to the active and inactive call processing applications are lost. Re-establish the connection. Refer to the Interface setup in this Upgrades document for procedures.

**4** This procedure is complete.

# ABORT: Jam the inactive Call Agent

***SDE — At the active maintenance window (CORE0 or CORE1)***

**1** Enter the CoreMtc level:

```
> CoreMtc
```

**2** Enter the CAMtc level:

```
> CAMtc
```

**3** Enter the Jam command:

```
> Jam
```

```
CallAgent       SYS       CON       APPL              Unit: 0
 JInact          .         .         .

CAMtc                      Jam:  Link0:  Link1:  BLnk: FC: Appl:
 0 Quit       Unit0  Act    no    . Inact . Act     .    .   insync .
 2 Jam        Unit1  Inact  yes   . Inact . Act     .    .   insync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16           Jam:      Jam the inactive unit, to prevent it taking activity.
17 Help                 Parms: [FORCE]
18 Refresh                 FORCE     - bypass system stability checks
  mtc
Time  10:38  >
```

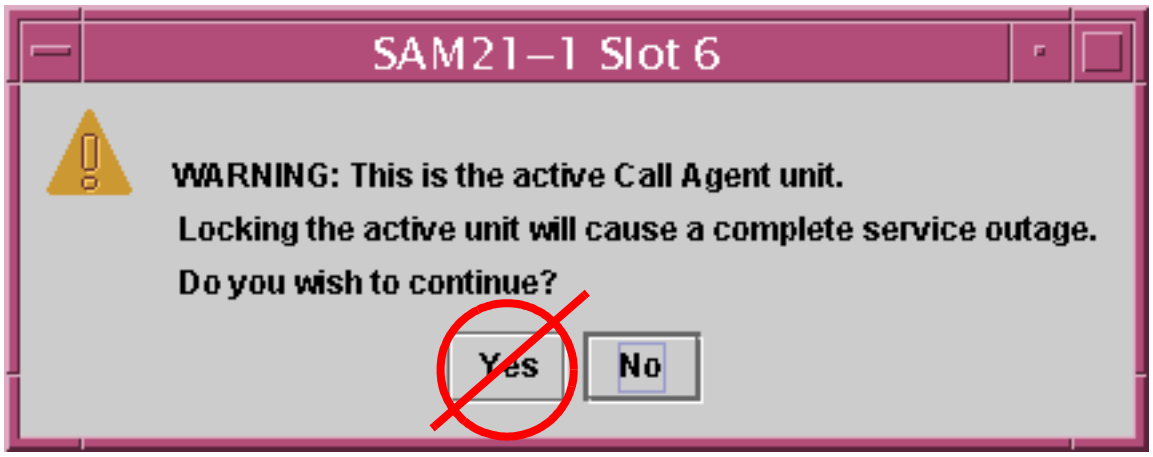
**4** This procedure is complete.

# ABORT: Lock the inactive Call Agent

**CAUTION**
**Possible service interruption**
Do not lock the active Call Agent.

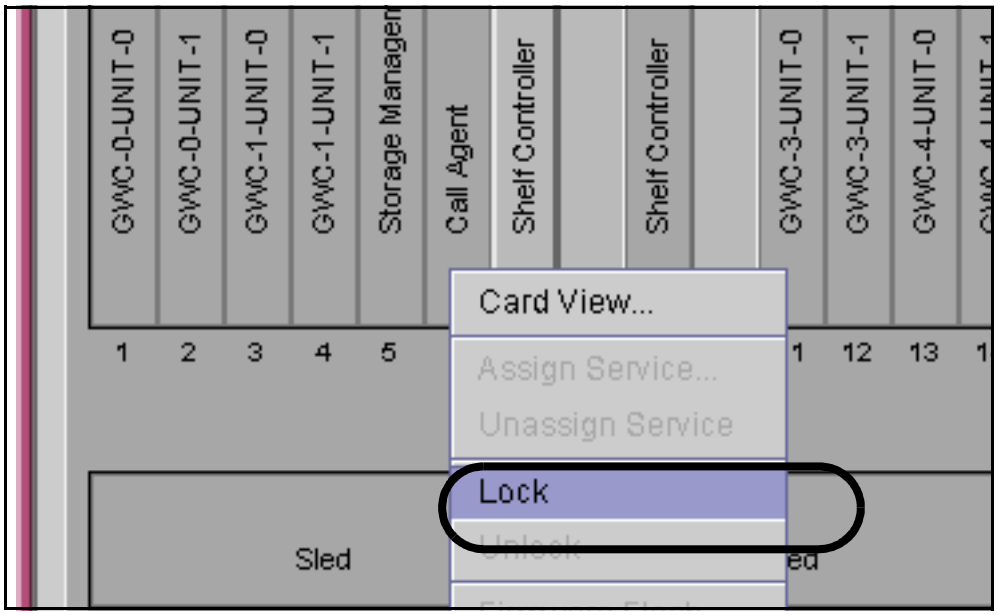
The CS 2000 SAM21 Manager client responds to an active Call Agent lock with the prompt shown in figure Call Agent lock warning. Do not click Yes. The inactive Call Agent is located in the other SAM21 shelf and a lock request does not provide a prompt when the Call Agent is inactive.

**Call Agent lock warning**



***At the CS 2000 SAM21 Manager client***

**1** From the Shelf View, right click on the card and select Lock from the context menu.




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

**2** Wait for the lock icon to appear on the selected card.

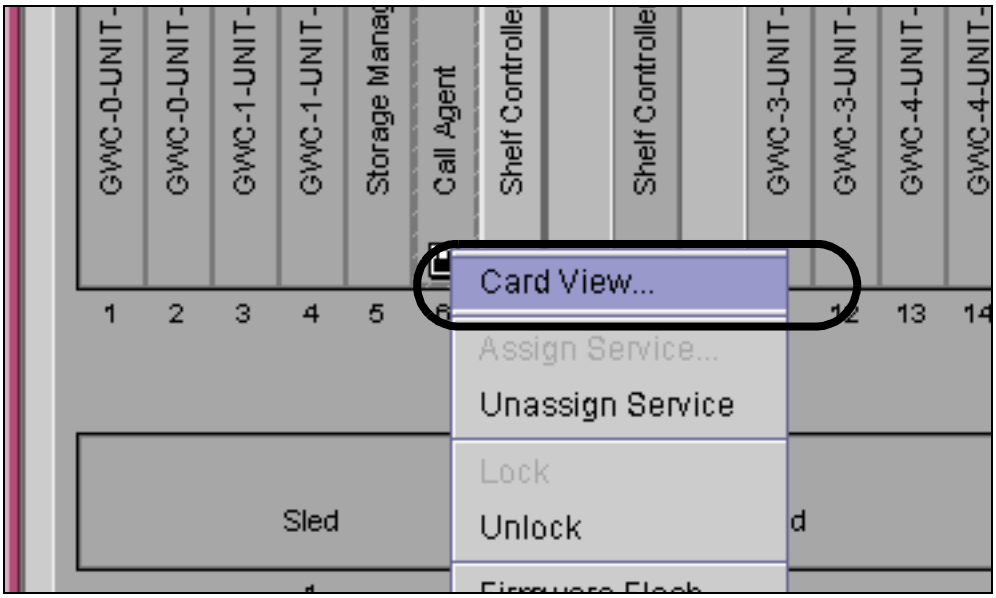
**3** This procedure is complete.

# ABORT: Provision previous software load

**ATTENTION**
Enter the software load from the previous release.

***At the CS 2000 SAM21 Manager client***

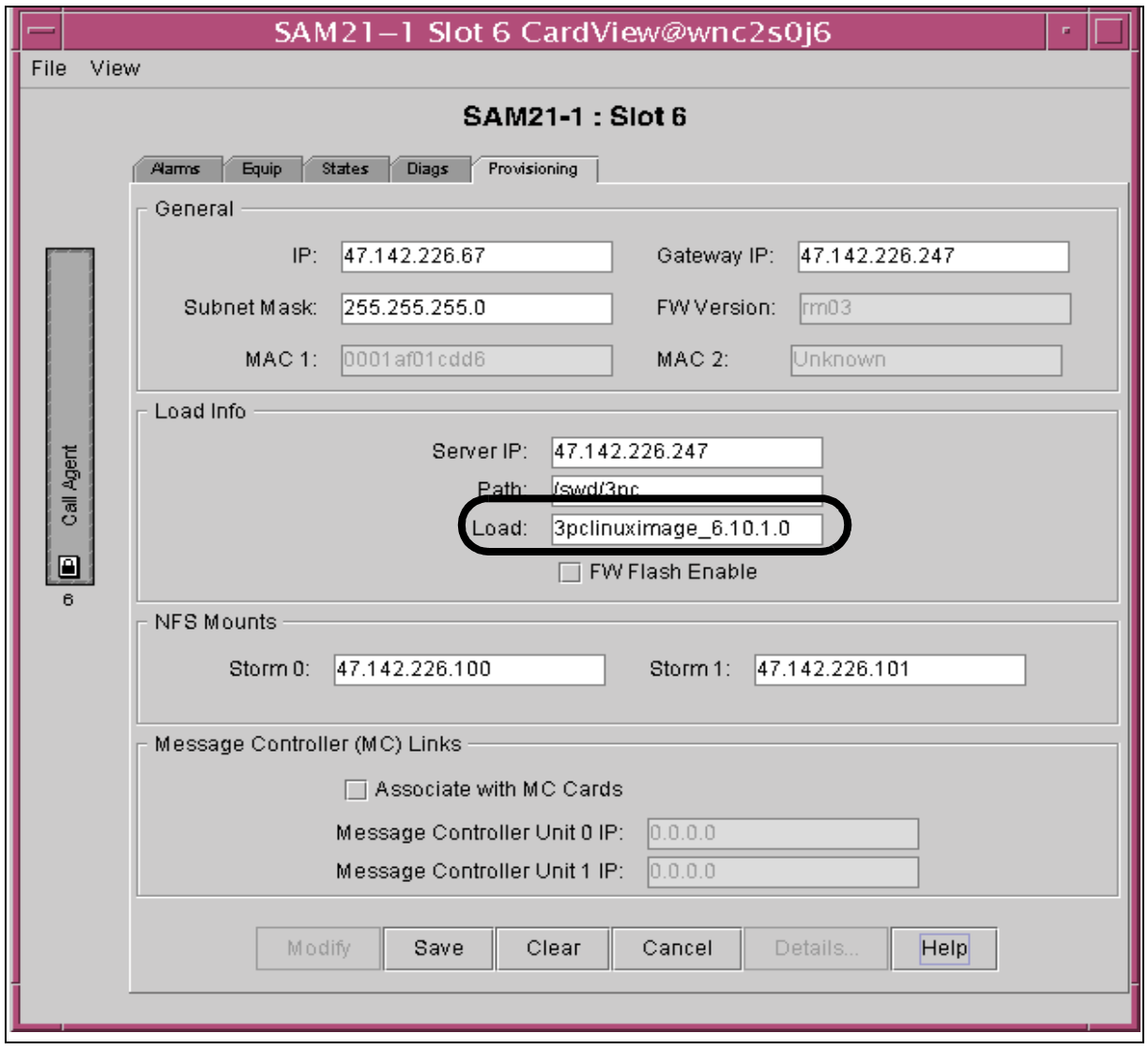
**1** From the Shelf View, right click on the card and select Card View from the context menu to open the Card View window.




**2** Click the Provisioning tab from the Card View window.

**3** Click the Modify button.

4 Enter the previous load file name in the load field.



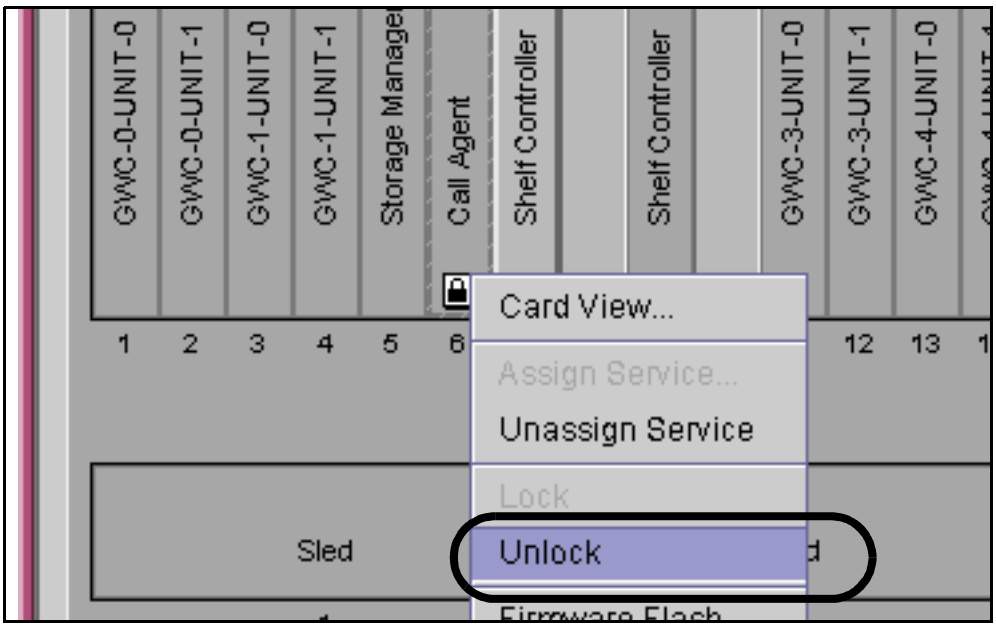

5 Click the Save button.

6 This procedure is complete.

# ABORT: Unlock the inactive Call Agent

***At the CS 2000 SAM21 Manager client***

**1** From the Shelf View, right click on the card and select Unlock from the context menu.




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

*The card resets, downloads software, and reboots. If platform patches were applied to the inactive Call Agent earlier in this upgrade, then the same patches are applied and automatically committed on this Call Agent unit as the card boots. No action is required for platform patching.*

**2** Wait for the lock icon to disappear.

**3** This procedure is complete.

Proceed to Execute POSTSWACT on page 204.

# Patching software

Platform and call processing application software is patchable. Platform patching does not patch the Linux kernel.

## What's new in platform software patching

### SN07

The format for the name of platform patch files has changed from `3pclinuxpatch_6.20.1.1` to `ncgl_cca_patch_5.15.1.1`. The procedure for applying patches remains unchanged.

### SN06

For the SN06 release, the command to start the Call Agent Manager has changed from **tpcmtc** to **ccamtc**. The patching procedure remains the same as the patching procedure for the SN05 release.

For customers registered with Regional Patch Selector (RPS), platform patches can be delivered directly from the RPS server to the `/swd/3pc/patch` directory on the CS 2000 Core Manager. If customers have platform patches delivered to an electronic dropbox, the customer is responsible for transferring the Call Agent platform patches to the `/swd/3pc/patch` directory on the CS 2000 Core Manager.

For Linux warranty patching visit Nortelnetworks.com to retrieve the patches:
Nortelnetworks.com
Select: Software Downloads
Select: Families *(top right under Find Products)*
Select: Succession Product Family
Select: Succession Communication Server 2000-Compact

### SN05

For the SN05 and ISN05 releases, platform patching offers greater robustness than earlier releases. Patch files are no longer cumulative and the Call Agent Manager enables validation of patch files for out of order application of patches.

If a patch fails to apply, the patching software automatically rolls back the patch. This feature enables the application of patches on the active Call Agent rather than patching the inactive Call Agent as required in earlier releases. A timer automatically commits patches after 10 minutes. Unless the user requests otherwise, patches are applied on

the active Call Agent, success is verified, and then the patching software begins applying the same patch on the inactive Call Agent.

## Platform patching

Patch files have the following identification scheme:

ncgl_cc_patch_r.w.c.v

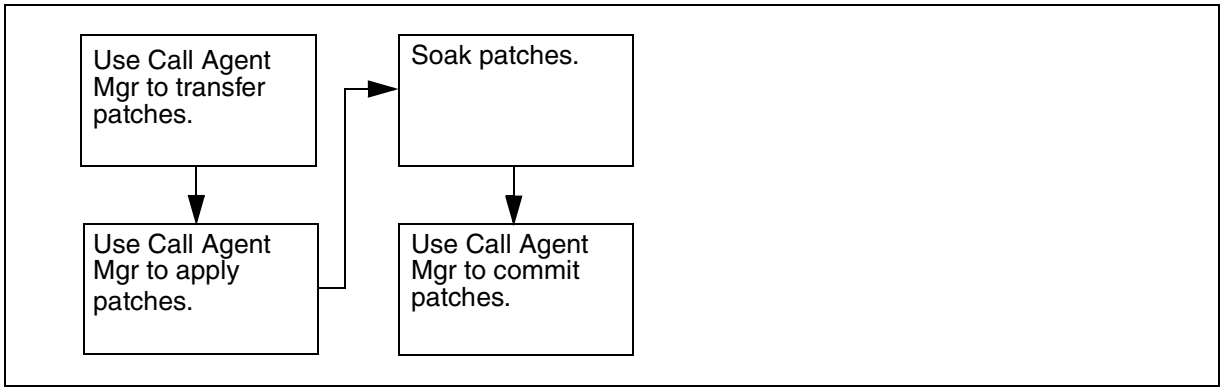
- **r** indicates the release. For example, 5.
- **w** indicates the week number of the load build. For example, 15.
- **c** indicates the compile. This value is equal to the fc value for an NCL or equal to (fc+i) for an MNCL. The patch is only applicable to a load that matches this number.
- **v** indicates the patch version.

***Note:*** Patches are only applicable to NCLs and MNCLs with matching r, w, and c values as the patch file.

Patching of the platform software is done through the Call Agent Manager.

Refer to the following flowchart for an overview of the platform patching procedure.

**Platform patching overview**




## Call processing application patching

Patching of the call processing application is done through Post-Release Software Manager (PRSM). This tool is available through the MAP.

Refer to *Post-Release Software Manager Reference Manual*, 297-8991-540, for information about patching the call processing application.

# Transfer platform patch files

Verify that patch files are installed on the CS 2000 Core Manager or CBM before completing this procedure. Platform software patch files are stored in `/swd/3pc/patch` for the Call Agent.

For Linux warranty patching visit Nortelnetworks.com to retrieve the patches:
Nortelnetworks.com
Select: Software Downloads
Select: Families *(top right under Find Products)*
Select: Succession Product Family
Select: Succession Communication Server 2000-Compact

This procedure requires root privilege.

### *At the Call Agent Manager*

**1** Enter the Transfer level:

```
> Admin
> SWIM
> Transfer
```

```
CallAgent       SYS       CON       APPL              Unit: 0
    .            .         .         .

Transfer     Current Load : 5.15.1.0
 0 Quit      Source       : /3pc/patch
 2 Select
 3 Fetch      # Patch Description                    Version
 4 Source     1 ncgl_cca_patch                      5.15.1.9
 5            2 ncgl_cca_patch                      5.15.1.8
 6            3 ncgl_cca_patch                      5.15.1.7
 7            4 ncgl_cca_patch                      5.15.1.6
 8
 9
10
11 Up
12 Down
13 LogQuery
14 Alarm                        Filesets on the source: 1 to 4 of 4
15
16
17 Help
18 Refresh
  mtc
Time  13:06  >
```

***Note 1:*** If patch files do not appear in the list, verify that the patch files are installed on the CS 2000 Core Manager or CBM in `/swd/3pc/patch` and have read permissions such as 777 or 755.

***Note 2:*** If patch files are stored in a different directory, use the SOURCE command to change the source directory. The CS 2000 Core Manager or CBM prepends `/swd` to all values.

2 Use the Select command to select the patch file to transfer from the CS 2000 Core Manager or CBM:

```
> Select num
```

**num**
is the decimal value that indicates the fileset

3 Use the Fetch command to retrieve the selected patch file:

```
> Fetch
```

***Note 1:*** If the FETCH command fails, verify that the patch files are installed and applied on the CS 2000 Core Manager or CBM and that the files have read permission set such as 777 or 755.

***Note 2:*** The fetch command retrieves the patch file and stores it on the active and inactive Call Agent cards by default. ACTIVE and INACTIVE options enable storage to a specific Call Agent card.

***Note 3:*** If the patch fileset already exists, the Call Agent prompts to determine if the existing file should be overwritten. Patch filesets can be overwritten.

```
Fileset already present. Overwrite?
Please confirm ("YES", "Y", "NO", "N"):
```

4 This procedure is complete.

# Apply platform software patch

**CAUTION**
**Possible service interruption**
Do not perform any patching activity within the first ten minutes following a Call Agent unlock.

***At the Call Agent Manager***

**1** Enter the Patch level:

```
> Admin
> SWIM
> Patch
```

```
CallAgent       SYS       CON       APPL              Unit: 0
   .             .         .         .

Patch         Current Load : 5.15.1.0
 0 Quit       Filter       : ALL
 2 Select
 3 Apply       # Patch Description              Version         Status
 4 Delete      1 ncgl_cca_patch                 5.15.1.9        NEW
 5 Commit      2 ncgl_cca_patch                 5.15.1.8        VALIDATED
 6             3 ncgl_cca_patch                 5.15.1.7        VALIDATED
 7             4 ncgl_cca_patch                 5.15.1.6        VALIDATED
 8
 9
10
11
12
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
  mtc
Time  14:14  >
```

2 Use the Select command to select the patch file to apply:

```
> Select <num>
```

**num**
is the integer value that indicates the patch

3 Use the Disadmin command to display any warnings or special application instructions. Perform any special application instructions:

```
> Disadmin
```

4 Reselect the patch and use the Validate command to verify that all dependencies are met:

```
> Select <num>
> Validate
```

| If | Do |
|---|---|
| dependencies are met and the patch validates successfully | step 5 |
| dependencies are not met and the validate fails | Fetch, select, and validate earlier patches before attempting to apply this patch. For example, if the current patch level is 5.26.1.10 and patch file 5.26.1.13 fails validation, attempt to validate and apply patches 5.26.1.11 and 5.26.1.12. |

5 Reselect the patch and use the Apply command to apply the patch file:

```
> Select <num>
> Apply
```

| If | Do |
|---|---|
| the patch applied successfully | step 6 |
| the patch fails to apply | Refer to Troubleshooting. |
| the patch is an older version or requires special application instructions | Refer to Additional information. |

**6**

**ATTENTION**

At this point, the patch is applied and is part of the running load. Soak the patch according to telephone operating company procedure before committing the patch. Patches are automatically committed 10 minutes after application unless manually committed earlier.

Reselect and use the Commit command to write the change to persistent storage. The committed load boots the next time the card is reset or rebooted:

```
> Select <num>
> Commit
```

***Note:*** If the ACTIVE or INACTIVE options are used, committing a patch on one card raises a C_MisM alarm. Committing the same patch on the second card clears the alarm. No alarms are raised or cleared if this is the first patch being committed.

**7** If additional patches need to be applied, repeat from step 2. Otherwise, this procedure is complete.

## Troubleshooting

The following table describes causes of possible problems, and what actions are required.

| Problem | Possible cause | Action |
|---|---|---|
| SWACT while running patch commands | The patch could be the cause of the SWACT. | Patching does not continue and patches are rolled back on the formerly active Call Agent. Contact Nortel Networks support personnel. |
| loss of mate communication while running patch commands | • link failures at router<br>• link pulls<br>• abnormal software process termination | Patching completes for the Call Agent on which patching was executing and looks for patch mismatch between the Call Agent cards.<br>If communication fails during inactive Call Agent patching, patching completes successfully because the active is already patched. |
| patch files available to only one Call Agent | • STORM failure<br>• failure to retrieve patch files and write them to storage | Correct STORM failure. Use the **TRANSFER** command to retrieve the files again. Attempt patch application again. |
| patch levels out of synchronization between active and inactive Call Agent cards | A previous attempt to apply patches failed. | Contact Nortel Networks support personnel for assistance with synchronizing the patch database files and determining the cause of failure. |

## Additional information

This section contains information about reverting to older patch levels and patch scenarios that require a platform upgrade.

### Reverting patches

Uncommit a patch from the running load with the **UNCOMMIT** command. Unless specified with the ACTIVE or INACTIVE options, the patch is uncommitted from the active Call Agent and then from the inactive Call Agent.

### Non-patchable versions

Non-patchable version patch files require a newer maintenance release than the currently running release.

Upgrade the platform software load first, then apply the patch file. Refer to the Upgrade strategy on page 8 procedure in this document.

### Special application instructions

If the patch file contains special application instructions, use the **DISADMIN** to display the instructions. Execute the required instructions.

### PATCH level command reference

The following list of commands are available from the PATCH level.

**SELECT**

This command selects a patch file by integer value from the list of fetched patches for validation, display of administrative information, application, commit, or uncommit. For example, SELECT 5.

**APPLY**

This command applies a selected patch file to the running load. Unless specified with the ACTIVE or INACTIVE options, the selected patch is applied on the active Call Agent and then applied on the inactive Call Agent.

**DELETE**

This command deletes the selected patch file from storage. The patches cannot be in the APPLIED or COMMITTED state. Deleting patches in the APPLIED or COMMITTED state causes problems during booting and future attempts to remove the patches fail.

**COMMIT**

This command commits the selected patch file to the running load. The patch must be in the APPLIED state and when the card is reset or reboots, the patch is re-applied. This command accepts ACTIVE and INACTIVE options, though the options are expected to be used during platform and call processing application upgrades only.

**UNCOMMIT**

This command uncommits the selected patch file from the running load. The patch file remains in storage and remains applied, but will not be re-applied after reset or a reboot. If other applied patch files depend on the selected patch file, a warning message is generated. Uncommit is permitted, but the dependencies are broken. Nortel Networks does not recommend uncommitting patches that break dependencies. Use the **REMOVE** command to un-apply a patch from the running load.

**FILTER**

This command alters the list of patch files to show only the patch files that are in a specified state. The list of available states is ALL, NEW, VALIDATED, APPLIED, COMMITTED, and REMOVED.

**REMOVE**

This command un-applies the selected patch file from the running load. The patch file must not be in the COMMITTED state. The removed patch files are not deleted from storage. If other applied patches depend on the selected patch file, removal is refused. Remove uncommit and remove the patches that depend on the selected patch file first.

**VALIDATE**

This command validates that the selected patch file can be successfully applied to the running load. This command accepts ACTIVE and INACTIVE options though the options are only useful if the two Call Agent cards are running different patch levels.

**DISADMIN**

This command displays administrative data about the selected patch file.

**UP**

This command scrolls up the list of patch files.

**DOWN**

This command scrolls down the list of patch files.

# Upgrading firmware on the occasion of a software upgrade

## Application

If firmware is available for the Call Agent card, it is delivered as part of the SAM21 Shelf Controller software load.

## Interval

Perform this procedure when the *SAM21 Platform Release Notes* indicate that a firmware upgrade is available. This procedure is not a standard part of upgrading the Call Agent.

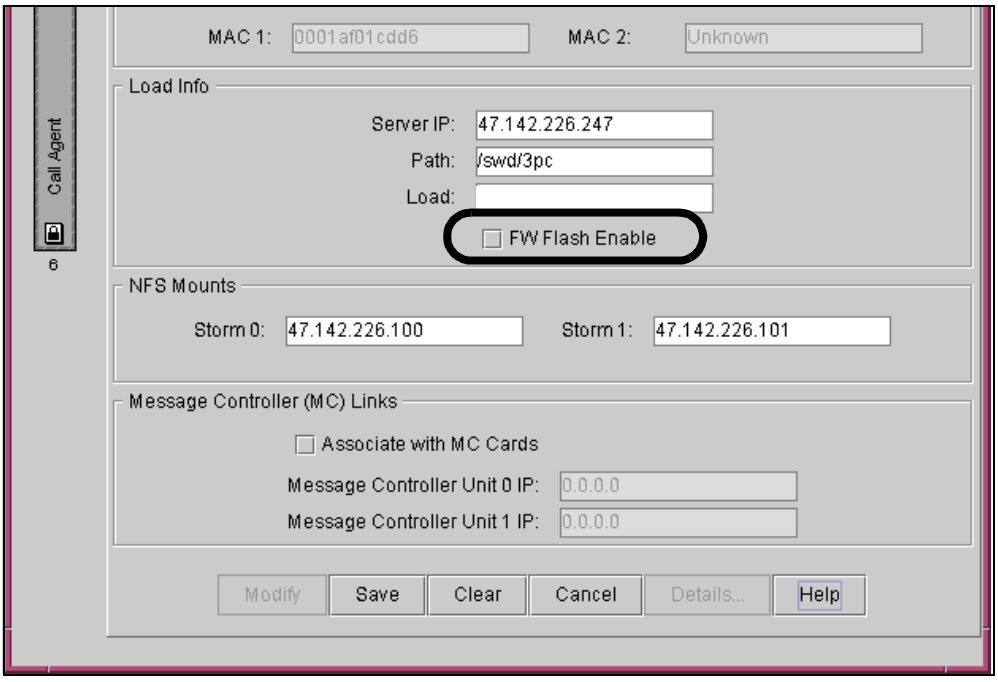
## Common procedures

There are no common procedures.

## Action

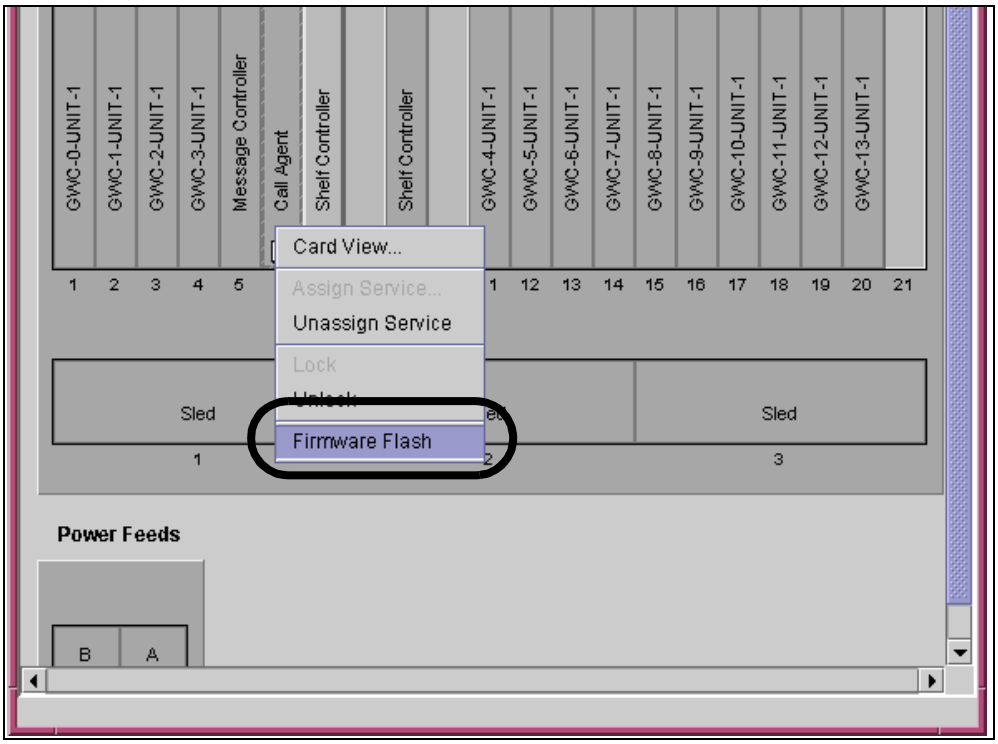
If the FW Flash enable checkbox is selected on the Provisioning panel of the Card View window at the CS 2000 SAM21 Manager client, firmware is automatically applied during an unlock request.

**Provisioning tab of the Call Agent Card View window**




Manual firmware upgrade is also available at the CS 2000 SAM21 Manger client by selecting Firmware Flash from the card context menu at the Shelf View window.

## Manual firmware flash from Shelf View




***Note:*** The Call Agent must be locked, and the FW Flash Enable checkbox on the Provisioning tab of the Card View window must be disabled to allow manual firmware flashing.